UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria
Corso di Laurea in Ingegneria Informatica e dell'Automazione

Analisi e simulazione dell'efficacia di uno CSIRT sulla propagazione di minacce cyber nelle reti

Analysis and simulation of the effectiveness of a CSIRT on the propagation of cyber threats in networks

Candidato:
Simone ONORI

Relatore:
Prof. Marco BALDI

Correlatore:
Prof. Luca Spalazzi

Anno Accademico 2022-2023

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria
Corso di Laurea in Ingegneria Informatica e dell'Automazione

Analisi e simulazione dell'efficacia di uno CSIRT sulla propagazione di minacce cyber nelle reti

Analysis and simulation of the effectiveness of a CSIRT on the propagation of cyber threats in networks

Candidato:
Simone ONORI

Relatore:
Prof. Marco BALDI

Correlatore:
Prof. Luca Spalazzi

Anno Accademico 2022-2023

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Informatica e dell'Automazione
Via Brecce Bianche – 60131 Ancona (AN), Italy

A mia madre Mirella
a mio padre Mauro
a mio fratello Davide
alla mia famiglia
alla mia ragazza Aurora
a tutti quelli che mi hanno accompagnato in questo mio percorso

Sommario

Un "Computer Security Incident Response Team" (Team di Risposta agli Incidenti di Sicurezza Informatica), o più semplicemente CSIRT, consiste in un gruppo di professionisti incaricato di gestire e rispondere agli incidenti di sicurezza informatica in un'organizzazione. Questo team è responsabile di monitorare, rilevare, rispondere e risolvere gli incidenti di sicurezza informatica, come violazioni della sicurezza, attacchi informatici, malware, perdite di dati e altre minacce alla sicurezza delle informazioni.
Nell'attuale panorama digitale, la crescente complessità delle minacce informatiche ha generato una domanda sempre più urgente di misure di sicurezza efficaci per proteggere le reti e i sistemi informatici dalle intrusioni. In questo contesto, il ruolo cruciale svolto dai Computer Security Incident Response Team (CSIRT) è emerso come un fattore determinante nella gestione degli incidenti di sicurezza informatica e nella limitazione della diffusione delle minacce cyber. La presente tesi si propone di condurre un'analisi approfondita e simulazioni dettagliate sull'efficacia di quattro livelli distinti di un CSIRT: assente, poco efficace, moderatamente efficace e altamente efficace, nella prevenzione e nel contrasto della propagazione delle minacce cyber all'interno delle reti.
Il titolo stesso della ricerca riflette l'obiettivo principale di valutare e comparare l'impatto di diverse capacità di risposta agli incidenti di sicurezza informatica sullo sviluppo e la diffusione di minacce nel contesto delle reti digitali.
La mancanza di un CSIRT o la presenza di un team con una capacità limitata di risposta agli incidenti potrebbe esporre le reti e i sistemi informatici a rischi significativi, consentendo alle minacce di diffondersi senza un'adeguata mitigazione. Al contrario, un CSIRT altamente efficace potrebbe fungere da baluardo contro queste minacce, impedendone la diffusione e limitandone l'impatto sui sistemi digitali.
In questo elaborato viene utilizzato il software *Microsoft CyberBattleSim* [1], un ambiente di simulazione che modella attacchi e difese informatiche su una rete. L'applicativo utilizza agenti di apprendimento automatico per simulare interazioni attacco-difesa, fornendo un ambiente per valutare strategie di sicurezza informatica. In particolare, è stato scelto e analizzato come caso di studio la diffusione di una minaccia cyber attraverso l'infrastruttura critica di una regione, simile, nel nostro caso, alla regione Marche.
Attraverso l'utilizzo di simulazioni e analisi approfondite, questa ricerca mira a fornire una valutazione comparativa dei diversi livelli di efficienza di un CSIRT nell'affrontare e contenere le minacce cyber, con l'obiettivo di fornire linee guida

pratiche per migliorare le strategie di difesa informatica e la gestione degli incidenti di sicurezza a livello organizzativo e aziendale.
La valutazione dettagliata di questi quattro livelli di efficacia di un CSIRT è fondamentale per comprendere il ruolo determinante che esso svolge nel contrastare le minacce cyber e nella protezione delle reti digitali, offrendo spunti preziosi per l'implementazione di pratiche e politiche più robuste in materia di sicurezza informatica. Attraverso un'analisi empirica e simulazioni accuratamente strutturate, questa ricerca si propone di contribuire significativamente alla comprensione delle dinamiche di risposta agli incidenti di sicurezza informatica e all'ottimizzazione delle strategie difensive nelle organizzazioni digitali.

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

Un CSIRT (*Computer Security Incident Response Team*) è la struttura che ha la responsabilità di monitorare, intercettare, analizzare e rispondere alle minacce cyber. È evidente, dunque, quanto il suo compito sia essenziale per la protezione di aziende e organizzazioni di ogni tipo dai sempre più micidiali attacchi informatici.
La genesi dei moderni CSIRT parte da lontano. È il 2 novembre 1988 quando alle otto e trenta del mattino Robert Tappan Morris, fresco di diploma ad Harvard, si siede davanti a un computer del MIT e lancia sulla "Internet" il suo codice, con l'obiettivo di dimostrare l'inadeguatezza delle misure di sicurezza a protezione della rete.
In meno di ventiquattro ore, 6.000 dei 60.000 computer connessi tra università, enti governativi e militari sono vittime di un *worm* che, pur non distruggendo i dati dei server, li rallenta fino a renderli inutilizzabili. Qualcuno prova a rimuovere il file dai sistemi, altri li sconnettono dalla rete, ma ormai la frittata è fatta: il rallentamento delle reti, il ritardo di giorni nella consegna delle e-mail, la disconnessione forzata di interi dipartimenti causano danni stimati nell'ordine di milioni di dollari.
Con lo scopo di porre rimedio al disastro, Robert abbozza un primitivo tentativo di *incident response* inviando anonimamente le istruzioni per la rimozione del *worm* e impedire una nuova infezione, ma sulla rete che lui ha paralizzato le informazioni non arrivano in tempo.
L'analisi a posteriori confermò che le contromisure in atto non sarebbero comunque state in grado di evitare i danni ingenti a causa di problemi di comunicazione e coordinamento strutturali alla rete.
Il *worm* di Morris fornì quindi lo spunto alla DARPA (*Defense Advanced Research Projects Agency*), l'agenzia USA che veicolava e che tuttora veicola cospicui finanziamenti verso i progetti di ricerca di sicurezza nazionale, per istituire velocemente il primo centro per la risposta coordinata agli incidenti presso il *Software Engineering Institute* (SEI) della *Carnegie Mellon University.* Nacque così il *Computer Emergency Response Team Coordination Center* (CERT/CC) con il compito di gestire le emergenze, l'incident response e costruire velocemente un robusto tessuto di consapevolezza all'interno della comunità Internet.
CSIRT, CERT e CIRT vengono spesso utilizzati in modo intercambiabile nel campo della sicurezza informatica. In realtà, CSIRT e CIRT sono quasi sempre equivalenti;

essenzialmente, sono sinonimi e un'organizzazione potrebbe preferire uno o l'altro in base a sottili differenze nel campo di competenza dell'organizzazione.
Per quanto riguarda il termine CERT, sebbene molte aziende lo utilizzino in modo generico, come detto in precedenza è un marchio registrato dell'Università di Carnegie Mellon dal 1997. Mentre, il fatto che due organizzazioni chiamino entrambe il loro team di risposta CSIRT, ad esempio, non significa che quei due team abbiano gli stessi obiettivi o metodi, o si conformino a una definizione idealizzata.
Parte della sfida con le organizzazioni che utilizzano il nome CERT è che può essere genuinamente confuso.
La designazione CERT di Carnegie Mellon ha un focus e una nicchia particolari; opera come un "partner con il governo, l'industria, le forze dell'ordine e l'ambiente accademico per migliorare la sicurezza e la resilienza dei sistemi e delle reti informatiche". Un CERT studia "problemi che hanno ampie implicazioni per la sicurezza informatica e sviluppa metodi e strumenti avanzati".
Alcune organizzazioni riflettono questi aspetti nell'uso del termine. In altre parole, utilizzano il CERT per indicare che il focus interno del loro team è leggermente diverso da quello di un tipico CSIRT. Ad esempio, il team potrebbe porre maggiore enfasi sulla collaborazione con altri team e organizzazioni interni o esterni, concentrarsi di più sulla metodologia e lo sviluppo di strumenti, o concentrarsi di più sulla ricerca delle minacce emergenti. Il termine CERT utilizzato in questo modo si concentra in modo più ampio sull'ottimizzazione della risposta agli incidenti come disciplina rispetto solo alla propria organizzazione.
Altre organizzazioni che utilizzano il termine CERT, in genere quelle che non sono consapevoli dello status di marchio registrato del CERT, utilizzano invece il termine come sinonimo di CIRT o CSIRT.
Sebbene CSIRT e CERT vengano spesso utilizzati in modo intercambiabile, nonostante le sottili differenze che esistano tra le due terminologie, esiste una differenza distintiva tra i due. Il termine CERT è di solito riservato alle principali organizzazioni di sicurezza informatica autorizzate dalle autorità governative, mentre un CSIRT può essere il team generale di risposta agli incidenti in una qualsiasi organizzazione.
Durante il proseguimento di questa trattazione, nonostante i due termini possano essere usati in modo quasi intercambiabile dal momento in cui in Italia esistono, come vedremo poi nei paragrafi successivi, tre enti che gestiscono a livello nazionale la risposta alla propagazione di possibili minacce cyber, faremo riferimento al solo CSIRT in quanto lo scopo della tesi è di analizzarne l'efficacia sulla propagazione di minacce cyber nelle reti.
Inoltre, le simulazioni in esame sono state eseguite tenendo in considerazione come ambiente un modello di rete e di infrastrutture critiche simile a quello che è possibile riscontrare all'interno della regione Marche, la quale in caso di attacco andrebbe a ricadere sotto la giurisdizione del CSIRT Italia.

1.1 CSIRT: significato e definizione

L'acronimo *CSIRT* è comunemente associato a un gruppo di esperti specializzati nella gestione degli incidenti di sicurezza informatica. Questi professionisti sono in grado di collaborare e coordinare gli interventi necessari per mitigare l'impatto di tali incidenti e ripristinare le normali condizioni operative dei servizi digitali. Oltre a rispondere agli incidenti, la maggior parte dei CSIRT fornisce servizi di prevenzione e offre programmi di formazione e sensibilizzazione per la propria comunità di riferimento.
Il funzionamento dei CSIRT si basa sulla gestione integrata dei flussi informativi provenienti dalla propria *constituency*[1] e da fonti esterne, svolgendo un ruolo cruciale come interfaccia operativa per le attività di *Information Sharing* per la sicurezza. Questi team sono in grado di raccogliere non solo segnalazioni di incidenti informatici, ma anche informazioni sulle vulnerabilità e potenziali minacce. Questa analisi consente loro di valutare gli impatti potenziali sugli asset informatici della comunità o dell'organizzazione e di identificare i rischi sottostanti, conducendo così all'implementazione delle contromisure più adeguate.
Nel contesto attuale, il focus dei CSIRT si sta spostando dalla semplice *Response* (risposta) agli incidenti alla *Readiness* (prontezza) preventiva. Questo cambiamento riflette l'evoluzione dei servizi informatici, la crescente sofisticazione delle minacce e la crescente importanza dei target che possono essere presi di mira. Pertanto, ogni organizzazione, in caso di incidente di sicurezza informatica, deve prepararsi in anticipo, sviluppando una cultura di sicurezza e attuando misure proattive atte a ridurre la probabilità e l'impatto degli incidenti. Questa preparazione significa sviluppare la capacità di adattare non solo gli aspetti tecnologici, ma anche quelli di processo e procedurali dei propri sistemi di difesa, in base all'evoluzione delle minacce, alla scoperta di nuove vulnerabilità e all'esperienza di incidenti sia avvenuti internamente che subiti da altre organizzazioni.
Alcuni elementi fondamentali per garantire questa "preparazione" includono la capacità di rilevare e rispondere agli incidenti, la comprensione approfondita degli asset informatici, inclusa la loro configurazione e vulnerabilità, la capacità di identificare minacce esterne e i modi in cui potrebbero colpire i sistemi e i servizi informatici, nonché la capacità di condividere informazioni in modo efficiente. Questo permette alle organizzazioni, alle amministrazioni, alle istituzioni e alle infrastrutture critiche di collaborare e scambiare conoscenze per anticipare attacchi, innalzando in questo modo il proprio livello di protezione.

[1] Comunità di utenti ed entità, sia interne che esterne all'organizzazione a cui il CSIRT appartiene e verso cui fornisce i propri servizi.

1.2 Evoluzione del CSIRT

L'evoluzione di CERT e CSIRT riflette la crescente complessità delle minacce informatiche ed è una storia di adattamento alle mutevoli sfide della sicurezza informatica e di crescita. Originariamente concepiti nei primi anni '80 con la creazione del CERT/CC (*Computer Emergency Response Team Coordination Center*) presso la *Carnegie Mellon University*, questi team hanno risposto principalmente a incidenti tecnici e problemi di sicurezza informatica di portata limitata.
Negli anni '90 e nel 2000, la loro funzione è cresciuta in complessità e portata, spaziando dalla gestione di incidenti tecnici alla risposta a violazioni della sicurezza di ampia portata. Questa evoluzione ha segnato un passaggio fondamentale, trasformando i CERT in entità multidisciplinari che non solo rispondono agli incidenti, ma li prevedono, li analizzano e adottano misure preventive. Cosi facendo nei primi anni 2000 e nel ventennio successivo, i CERT si sono diffusi a livello mondiale, dando origine a una vasta rete di organizzazioni governative, accademiche e aziendali. Questo sviluppo è stato guidato dall'aumento esponenziale delle minacce informatiche e dalla necessità di una risposta coordinata ai problemi di natura cibernetica.
L'evoluzione dei CSIRT ha seguito un percorso simile a quello dei CERT, ma con sfumature specifiche. Emergenti negli anni '90, i CSIRT hanno inizialmente affrontato principalmente sfide tecniche e problemi di sicurezza informatica. Tuttavia, la loro evoluzione è stata rapida, spinti dall'aumento della complessità delle minacce e dalla necessità di affrontare violazioni della sicurezza di ampia portata, anche i CSIRT hanno dovuto adattarsi evolvendosi rapidamente in entità multidisciplinari, in grado di rispondere non solo a incidenti di sicurezza informatica di vasta portata, ma anche di prevenirli e di adottare misure proattive.
Questa crescita parallela alla complessità delle minacce riflette la loro importanza nell'ecosistema della sicurezza informatica.
Man mano che le aziende creavano i propri Response Team, questi nuclei specializzati hanno iniziato a fare rete, adottando un approccio organizzato alla difesa e cooperando per proteggere le infrastrutture comuni. Con la vertiginosa crescita di Internet (più della metà della popolazione mondiale è connessa al web) la protezione della rete è diventata un tema geopolitico; gli Stati hanno cominciato a istituire gruppi di difesa cyber a livello civile e militare e i CSIRT governativi sono diventati componente imprescindibile delle strategie nazionali di cybersecurity.
I Team possono essere strutturati in modi differenti, in funzione della *constituency* di riferimento e degli assetti interni; ci sono gruppi impegnati a tempo pieno nella gestione degli incidenti così come possono esserci figure specializzate, impiegate nelle *operations* di sicurezza, che vengono chiamate a raccolta nel caso si verifichi un allarme.
Al di là di forma e struttura, un CSIRT ha il compito di assegnare risorse esperte nella gestione degli incidenti che, oltre le immancabili *skill* verticali su tecnologie e strumenti, siano in grado di comprendere i processi aziendali funzionali all'organizzazione

così come il bacino di utenza verso il quale erogano i propri servizi.

1.3 Quadro di riferimento nazionale

Negli ultimi anni, l'architettura nazionale per la sicurezza cibernetica ha subito significative modifiche volte a razionalizzare e migliorare gradualmente le capacità di difesa del paese nel campo della cybersecurity. Nel 2013, conosciuto come il "*Decreto Monti*" [2], l'Italia ha delineato per la prima volta la sua struttura di sicurezza cibernetica, cercando di coordinare le diverse competenze del settore tra diverse autorità governative. Questo ha portato a un notevole potenziamento delle capacità di cybersecurity a livello nazionale, guidate da direttive della Presidenza del Consiglio dei Ministri, sia a livello strategico con il "*Quadro strategico nazionale per la protezione dello spazio cibernetico*" che a livello operativo con il "*Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*".
Il 17 febbraio 2017 è stato adottato il Decreto del Presidente del Consiglio dei Ministri "*Direttiva recante gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*" (cd."Decreto Gentiloni") [3], che ha sostituito il decreto del 2013 e ha posizionato il *Dipartimento Informazioni per la Sicurezza* (DIS) al centro della governance nazionale per la cybersecurity. Il DIS ora presiede il *Nucleo per la Sicurezza Cibernetica* (NSC), responsabile della gestione di incidenti cibernetici di particolare rilevanza e della dichiarazione di crisi cibernetica nazionale, tenendo costantemente informato il Presidente del Consiglio dei Ministri in caso di situazioni critiche.
Di seguito, sono descritte le principali strutture organizzative che compongono l'architettura nazionale per la sicurezza cibernetica, fungendo da punti di riferimento essenziali per un CERT (*Computer Emergency Response Team*) che opera in Italia.

CISR (*Comitato Interministeriale per la Sicurezza della Repubblica*) [4] è un organo istituzionale di raccordo politico-strategico sul tema della sicurezza nazionale, con compiti di consulenza, proposta e deliberazione. È presieduto dal Presidente del Consiglio dei Ministri e composto, oltre che dall'Autorità delegata, ove istituita, dai Ministri degli Affari Esteri e Cooperazione Internazionale, dell'Interno, della Giustizia, della Difesa, dell'Economia e delle Finanze, dello Sviluppo Economico. Il Direttore Generale del DIS svolge le funzioni di segretario del Comitato. Il CISR svolge, inoltre, compiti di supporto al Presidente del Consiglio in caso di situazioni di crisi, anche per la sicurezza cibernetica.

DIS (*Dipartimento Informazioni per la Sicurezza*) [5] è un organismo di cui si avvalgono il Presidente del Consiglio dei Ministri e l'Autorità delegata, ove istituita, per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza. Nell'architettura nazionale cyber, il DIS ha un ruolo centrale

ed è chiamato a definire e attuare la governance in materia, sia a livello nazionale (anche attraverso la presidenza del Nucleo per la Sicurezza Cibernetica), sia in ambito UE, NATO, OSCE e ONU. In coerenza con tale framework, il Decreto legislativo 18 maggio 2018, n. 65, di recepimento della Direttiva NIS (`si veda par. 1.1.2`) prevede che il Dipartimento assuma il ruolo di Punto di Contatto Unico NIS, con il compito di coordinare, a livello nazionale, le questioni relative alla sicurezza delle reti e dei sistemi informativi e di svolgere una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità competenti NIS con quelle degli altri Stati Membri nonché con il Gruppo di cooperazione, istituito presso la Commissione Europea.

NCS (*Nucleo per la CyberSicurezza*) [6] è un organo costituito presso l'ACN, a supporto del Presidente del Consiglio dei Ministri e del CISR, nella materia dello spazio cibernetico, per gli aspetti relativi alla prevenzione e preparazione a eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento, svolgendo funzioni di raccordo tra le diverse componenti dell'architettura istituzionale cyber. Il Nucleo per la cybersicurezza è presieduto dal Direttore Generale dell'Agenzia o, per sua delega, dal Vice Direttore Generale, ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del *Dipartimento delle informazioni per la sicurezza* (DIS), dell'*Agenzia informazioni e sicurezza esterna* (AISE), dell'*Agenzia informazioni e sicurezza interna* (AISI), del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri (PCM), del Ministero degli esteri e della cooperazione internazionale (MAECI), del Ministero dell'interno, del Ministero della giustizia, del Ministero della difesa, del Ministero dell'economia e delle finanze (MEF), del Ministero delle imprese e del made in Italy (MIMIT), del Ministero dell'ambiente e della sicurezza energetica (MASE), del Ministero dell'università e della ricerca (MUR), del Ministero delle infrastrutture e dei trasporti (MIT) e del Dipartimento della protezione civile della PCM; in situazioni di crisi di natura cibernetica il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del Ministero della salute e del Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile.

CNAIPIC (*Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche*) [7] è incaricato della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale. Si avvale di tecnologie di elevato livello e di personale altamente qualificato, specializzato nel contrasto del cybercrime, che ha maturato concreta esperienza anche nei settori del cyber terrorismo e dello spionaggio industriale. L'operatività del CNAIPIC è soddisfatta attraverso l'esercizio di un Settore Operativo e di un Settore Tecnico. Il Settore Operativo supporta le funzioni di:

Sala Operativa, Intelligence e Analisi. Il Settore Tecnico è invece deputato alla gestione e all'esercizio dell'infrastruttura tecnologica del CNAIPIC e dei collegamenti telematici con le Infrastrutture Critiche convenzionate, ai processi di individuazione, testing e acquisizione di risorse strumentali e alla pianificazione di cicli di formazione e aggiornamento del personale.

COR (*Comando per le Operazioni in Rete*) [8] è responsabile della condotta delle operazioni nel dominio cibernetico, nonché della gestione tecnico-operativa in sicurezza di tutti i Sistemi di Information & Communications Tecnology/C4 della Difesa, al fine di armonizzare e distribuire tempestivamente le informazioni prodotte dai sistemi di comando e controllo, computing, Intelligence Surveillance & Reconnaissance necessarie ad abilitare le funzioni del Capo di Stato Maggiore della Difesa, nella sua funzione di Comandante in Capo delle Forze, e dei Comandi interessati.
Nato nel 2018 su ordine del Capo di Stato Maggiore della Difesa dalle risultanze del lavoro svolto dal GdP (*Gruppo di Progetto denominato "Riorganizzazione e razionalizzazione del settore Cyber"*), è emersa la necessità di costituire un comando capace di riunire le competenze di diversi attori operanti in ambito Difesa.
La soluzione ordinativo-organica rispondente a tale esigenza è stata individuata aggregando due comandi preesistenti: il Comando C4 Difesa (C4D) e il Comando Interforze per le Operazioni Cibernetiche (CIOC).
Il 9 marzo 2020, è stato costituito il *Comando per le Operazioni in Rete della Difesa* (CORDIFESA), soluzione rispondente a criteri di efficienza ed efficacia, che si pone quale ente attraverso il quale la Difesa ha inteso razionalizzare il citato settore per eliminare le preesistenti criticità.
Il CORDIFESA ha assunto il ruolo di responsabile della Rete, dei Sistemi, dei Servizi, degli Applicativi e dei Portali Web della Difesa, consentendo pertanto l'accentramento, a connotazione Interforze, di quelle funzioni comuni tra le Forze Armate e l'Area Interforze.

CERT-Difesa [9] costituito all'interno del COR, il CERT della Difesa italiana si articola su due pilastri fondamentali. Il primo è denominato Cert Coordination Center ed è realizzato in seno al II Reparto dello Stato maggiore della Difesa, il Reparto informazioni e sicurezza, mentre la componente tecnico-operativa, che prende il nome di Cert Technical Center, è realizzata in seno al Comando C4 Difesa, dipendente dal VI Reparto dello Stato maggiore della Difesa. Il Comando C4 Difesa in particolare è l'organo preposto alla gestione tecnico-operativa di tutti gli assetti e di tutti i sistemi di Information and Communication Technology del comparto Difesa e, quindi, del Dipartimento.
Queste due anime svolgono congiuntamente attività di indirizzo, coordinamento e informazione verso gli analoghi organi costituiti presso le Forze armate. Infatti ogni singola Forza armata ha un suo CERT che lavora in maniera coordinata

con il CERT Difesa, sovrapposto agli altri non in termini organici, ma funzionali. Infatti, in caso di situazioni di crisi, il CERT Difesa assume il coordinamento delle attività da porre in essere.
Compito del Cert Difesa è quello di prevenire la minaccia cibernetica, rilevare le attività di natura malevola e reagire agli incidenti informatici. Più nello specifico, il Cert Coordination Center svolge attività di informazione e di allertamento anche a scopo di prevenzione e collabora e condivide informazioni con i corrispondenti Cert nazionali e internazionali. In particolare, il Cert internazionale con cui si relaziona la Difesa italiana è quello della Nato, che va sotto il nome di Nato Computer Incident Response Capability (NCIRC). L'ultima funzione è quella di supportare il Cert Technical Center con attività di analisi in caso di evento cibernetico.
Il Cert Technical Center è, invece, preposto a prevenire, rilevare e contenere sul piano tecnico-operativo gli incidenti informatici. Tale centro, peraltro, coordina e supporta l'azione dei Cert di Forza armata in caso di emergenza cibernetica.

Autorità competente NIS [10] è l'autorità incaricata di attuare il decreto di recepimento della Direttiva NIS, vigilando sulla sua applicazione nel settore di competenza ed esercitando le relative potestà ispettive e sanzionatorie.
Nell'ordinamento nazionale le autorità coinvolte sono:

- il Ministero dello Sviluppo Economico per il settore energetico (sottosettori energia elettrica, gas e petrolio), per le infrastrutture di scambio del traffico telematico (le cosiddette infrastrutture digitali, sottosettori IXP, DNS, TLD) e per i servizi digitali;
- il Ministero dei Trasporti e delle infrastrutture per il settore dei trasporti (sottosettori aereo, ferroviario, per vie d'acqua e su strada);
- il Ministero dell'Economia e delle Finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con in collaborazione con le autorità di vigilanza di settore, la Banca d'Italia e con la *Commissione Nazionale per le Società e la Borsa* (CONSOB);
- il Ministero della Salute e, per quanto di competenza, le Regioni e le Province autonome di Trento e Bolzano per l'attività di assistenza sanitaria;
- il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

CERT-AGID [11] Sulla base delle esperienze e delle conoscenze maturate nell'ambito delle funzioni svolte dal CERT-PA fino al termine della sua vita operativa, l'Agenzia per l'Italia Digitale ha voluto creare una sua nuova struttura, denominata CERT-AGID, nella quale confluiscono il team e le infrastrutture che

costituivano la parte fondante del CERT-PA. Il CERT-PA, attivo dal mese di marzo 2014 fino al 6 maggio 2020, ha operato all'interno di AGID con il compito di supportare le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica.
Il CERT-AGID è stato censito presso ENISA (*European Network and Information Security Agency*), l'agenzia dell'Unione Europea che supporta la creazione della rete Europea dei CERT e dal 19 Luglio 2016 ha ottenuto lo status di "Team accreditato" presso Trusted Introducer, la rete di fiducia dei CERT mondiali fondata in Europa nel 2000. Dal 6 maggio 2020, recependo il DPCM 8 agosto 2019, "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano" [12], il CERT-PA termina l'erogazione di servizi reattivi e di risposta agli incidenti informatici dedicati alla PA, confluisce nel CERT-AGID e si predispone per supportare AGID su tutti i temi riguardanti trasversalmente gli aspetti di sicurezza informatica relativi ai progetti interni ed esterni a cui AGID partecipa in maniera diretta o indiretta.

CSIRT Italia [10] il D.lgs. 65/2018 di recepimento all'interno dell'ordinamento nazionale italiano della Direttiva NIS ha previsto l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico *Computer Security Incident Response Team*, detto "CSIRT Italia", che svolgerà i compiti e le funzioni degli attuali CERT-PA e CERT-N. Il CSIRT Italia, sulla base di un modello cooperativo pubblico-privato, avrà compiti di natura tecnica finalizzati a supportare la PA, i cittadini e le imprese attraverso azioni di sensibilizzazione, prevenzione e coordinamento della risposta a eventi cibernetici su vasta scala, anche in cooperazione con gli altri CERT europei. In particolare, secondo quanto disposto dal decreto di recepimento, avrà i seguenti compiti:

- definire le procedure per la prevenzione e la gestione degli incidenti informatici;
- ricevere le notifiche di incidente, informandone il DIS, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al NSC;
- fornire al soggetto che ha effettuato la notifica le informazioni che possono facilitare la gestione efficace dell'evento;
- informare gli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali o del fornitore di servizi digitali nonché la riservatezza delle informazioni fornite;
- garantire la collaborazione nella rete di CSIRT, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la

condivisione di best practices.

La rilevanza dei CERT e dei servizi che questi possono fornire, è evidenziata anche a livello di strategia nazionale. In quest'ottica, il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica rimarca le esigenze di potenziamento degli attuali CERT e la necessità di istituirne di nuovi. In particolare, si sottolinea come l'approntamento di capacità di prevenzione e reazione a eventi cibernetici richieda lo sviluppo dei CERT quali soggetti erogatori di servizi di assistenza tecnica, ricerca e sviluppo, formazione e informazione per i rispettivi utenti, pubblici e privati. Organismi, dunque, che siano in grado di assicurare un'effettiva capacità di assistenza e supporto attivo alla propria constituency in caso di evento cibernetico.

Queste strutture sono fondamentali per la sicurezza cibernetica in Italia, svolgendo ruoli chiave nella prevenzione, rilevazione e risposta agli incidenti cibernetici.

1.4 Directive on Security of Network and Information Systems

La creazione del CSIRT costituisce una delle misure, adottate dall'Italia, volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno. La direttiva europea 2016/1148 (*Direttiva NIS*) [13] è, in questo senso, di primaria importanza, in quanto fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi e crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (*rete CSIRT*).
La Direttiva, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea, rappresenta il primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza cibernetica e delinea le azioni in capo agli Stati membri volte a migliorare le capacità di sicurezza dei singoli Paesi dell'Unione Europea.
La Direttiva ambisce inoltre ad aumentare il livello di collaborazione nella prevenzione delle minacce cibernetiche e nell'implementazione di misure di risposta agli attacchi cyber. All'interno della Direttiva ampia rilevanza è assegnata al ruolo esercitato dai CERT, già esistenti o che verranno istituiti dagli Stati membri, cui saranno affidate funzioni di responsabilità del monitoraggio degli incidenti a livello nazionale.
Come si è visto, attraverso il D. Lgs. 65/2018 [10], che ha recepito la Direttiva NIS all'interno dell'ordinamento nazionale italiano, è stato istituito il CSIRT Italia. Il CSIRT è parte integrante del processo di innovazione che l'Italia sta portando avanti nel settore della cyber security. In questo contesto si inserisce anche il Perimetro di sicurezza nazionale cibernetica, istituito dal Decreto-legge 105/2019 [14] per "innalzare la resilienza di reti, sistemi informativi e servizi informatici degli attori nazionali, tanto pubblici quanto privati, che esercitano una funzione essenziale dello

Stato". Il decreto, tra le altre disposizioni, prevede che gli attori notifichino gli incidenti alle strutture deputate alla prevenzione, preparazione e gestione degli eventi cyber, in particolare al NSC e al CSIRT.
La normativa che regola il funzionamento del CSIRT prevede un alto livello di cooperazione, sia a livello nazionale che europeo. Il team farà, infatti, affidamento sull'Agenzia per l'Italia digitale (AgID) e in particolare sul CERT-AGID che ha sostituito il CERT-PA, con il compito di definire raccomandazioni e strategie per sensibilizzare e informare le amministrazioni sui temi della sicurezza informatica.
A livello europeo, il CSIRT, attraverso il punto di contatto (il DIS), collabora con i suoi omologhi presenti negli altri stati membri, con la Commissione Europea e con l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). Questa collaborazione permette la creazione di una cornice di sicurezza europea e l'adozione di politiche comuni sulla sicurezza informatica. La creazione di un unico centro di gestione degli incidenti, attraverso una più ampia condivisione di informazioni, permette di acquisire una maggiore consapevolezza dei rischi e delle minacce a livello nazionale, tanto nel settore pubblico quanto in quello privato. La costituzione dello stesso in seno al DIS significa dare maggiore centralità al governo, a capo del dipartimento, e garantire una maggiore capacità di risposta, assicurata dalla sinergia di capacità di cui il dipartimento già dispone.
Infine, la creazione del CSIRT vuole essere un incentivo per i soggetti interessati a comunicare gli incidenti avvenuti. Sebbene la segnalazione sia in molti casi un'ammissione di colpa, ovvero di mancata prevenzione, la sua tempestività potrebbe determinare una risposta efficace al fine di tutelare i cittadini e la sicurezza nazionale.
Con la Direttiva NIS il legislatore europeo ha altresì previsto che gli Stati membri si dotino di un'organizzazione in grado di vincolare gli operatori di servizi ritenuti essenziali e i fornitori di servizi digitali per l'economia all'adozione di stringenti misure di protezione. Come precedentemente illustrato, nel modello istituzionale scelto dal governo italiano, sono state designati 5 Ministeri quali Autorità Competenti NIS (Sviluppo Economico, Infrastrutture e Trasporti, Economia, Salute e Ambiente) ciascuno responsabile di specificare per uno o più settori rientrati nelle proprie aree di competenza gli operatori di servizi essenziali, definire le misure di sicurezza minime, vigilare sulla loro applicazione anche mediante ispezioni, comminare sanzioni.

Tutti i paesi europei, chi più chi meno, hanno provveduto all'implementazione di CSIRT nazionali affiancati a CSIRT privati in linea appunto con la direttiva NIS. Nella figura 1.2 è presente il numero di CSIRT europei pubblicato dal sito di ENISA [15] l'European Union Agency for Cybersecurity unitamente, in figura 1.1 all'inventario delle differenti tipologie di CSIRT nei differenti settori economici (PA e Difesa, Utilities, Energia, Finanza, Industria, Trasporti ecc.).

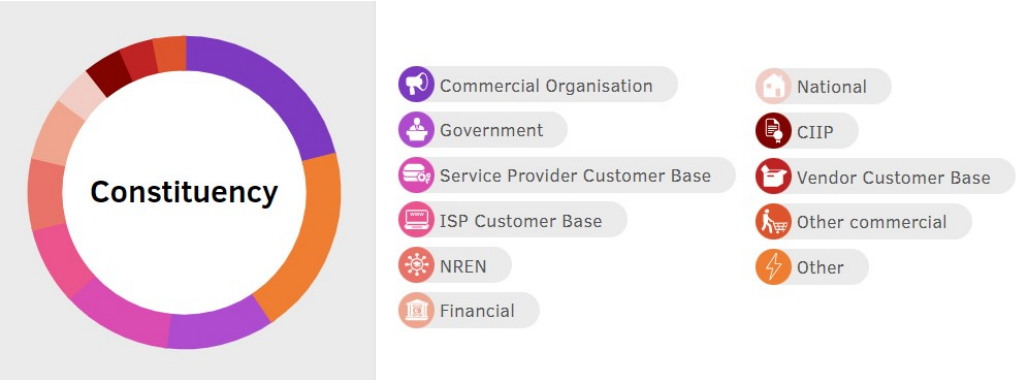

Figura 1.1: Costituency degli CSIRT presenti nei paesi dell'Unione Europea

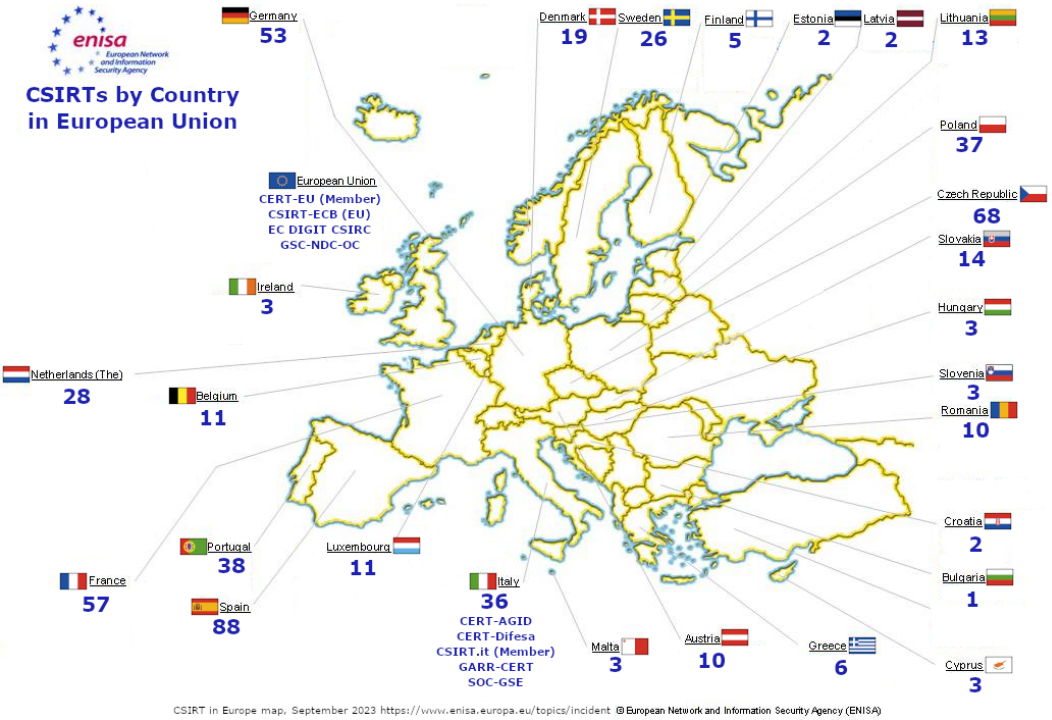

Figura 1.2: Numero di CSIRT presenti nei paesi dell'Unione Europea

Capitolo 2

Requisiti e caratteristiche di un CSIRT

Nel panorama in costante mutamento della sicurezza informatica, i CERT (Computer Emergency Response Team) e i CSIRT (Computer Security Incident Response Team) sono una componente vitale nella gestione delle minacce e degli incidenti di sicurezza informatica all'interno delle organizzazioni e giocano un ruolo cruciale nella difesa delle infrastrutture digitali.
L'evoluzione dei CSIRT ha seguito un percorso simile a quello dei CERT, ma con sfumature specifiche. Emergenti negli anni '90, i CSIRT hanno inizialmente affrontato principalmente sfide tecniche e problemi di sicurezza informatica. Tuttavia, la loro evoluzione è stata rapida, spinta dall'aumento della complessità delle minacce e dalla necessità di affrontare violazioni della sicurezza di ampia portata. In questa evoluzione, i CSIRT hanno ampliato le loro competenze per diventare entità multifunzionali, capaci non solo di rispondere agli incidenti, ma anche di prevenirli e di adottare misure proattive.
Questo capitolo si propone di esplorare in dettaglio lo stato dell'arte dei CSIRT, analizzando la loro evoluzione storica, le funzioni chiave, le sfide affrontate e le tendenze emergenti che delineano il loro ruolo nel contesto della sicurezza informatica.

2.1 Missione di un CSIRT

La missione di un CSIRT (Computer Security Incident Response Team) comprende una serie di attività fondamentali:

Fornire Supporto Specializzato : Il CSIRT è dedicato a fornire supporto e assistenza specialistica alla sua comunità di riferimento. Questo supporto si estende all'analisi dei dati relativi alle minacce informatiche emergenti e alla risoluzione degli incidenti di sicurezza informatica.

Diffondere Informazioni Tempestive : Un importante compito del CSIRT è la diffusione di informazioni tempestive e utili. Queste informazioni riguardano nuovi scenari di rischio, attacchi in corso e tendenze nei fenomeni cibernetici. Tale diffusione è cruciale per mantenere la comunità informata e preparata.

Promuovere le Best Practices : Il CSIRT lavora per promuovere l'adozione di processi di gestione della sicurezza, metodologie e metriche valutative. Questi

strumenti sono essenziali per il governo efficace della sicurezza cibernetica e contribuiscono a una maggiore resilienza.

Supportare la Prevenzione e il Monitoraggio : Il CSIRT facilita le attività di prevenzione e monitoraggio degli eventi cibernetici nella sua area di competenza. Questo può includere un controllo più diretto a livello locale, contribuendo così a garantire la sicurezza delle reti e dei sistemi informatici.

Collaborare a livello Nazionale e Internazionale : Il CSIRT lavora in collaborazione e cooperazione con altre organizzazioni a livello nazionale e internazionale. Questa cooperazione mira a potenziare e migliorare le capacità difensive delle organizzazioni in materia di sicurezza informatica, creando una rete di difesa più robusta.

Sviluppare Competenze e Sensibilizzare : Il CSIRT si impegna a sviluppare le competenze specialistiche del personale coinvolto nella sicurezza informatica. Inoltre, promuove attivamente la sensibilizzazione su questi temi a livello locale, contribuendo a una maggiore consapevolezza riguardo alla sicurezza cibernetica.

Queste attività rappresentano il fulcro della missione di un CSIRT, che lavora costantemente per migliorare la sicurezza informatica, rispondere agli incidenti e preparare la comunità per affrontare le sfide emergenti nel mondo digitale.

2.2 Identificazione della constituency

Nel contesto del proprio funzionamento, ogni CSIRT è coinvolto in una vasta gamma di interazioni con diverse entità e soggetti. La comunità più significativa tra queste è la constituency, ossia la comunità di utenti ed entità, sia interne che esterne all'organizzazione a cui il CSIRT appartiene e verso cui fornisce i propri servizi. La composizione di questa constituency può variare, a seconda delle circostanze:

- **Estensione Illimitata**: Un CSIRT potrebbe offrire servizi a un'ampia varietà di utenti, senza restrizioni. In questo caso, il CSIRT è disponibile per chiunque richieda assistenza.
- **Vincoli Finanziari**: Alcuni CSIRT potrebbero avere limitazioni finanziarie legate ai finanziamenti iniziali ottenuti per la loro creazione e avvio delle attività. Questi vincoli possono influenzare la portata dei servizi offerti.
- **Vincoli Geografici o Politici**: In alcune situazioni, gli CSIRT possono essere vincolati da considerazioni geografiche o politiche. Ad esempio, potrebbero essere incaricati di supportare una constituency nazionale o organizzazioni specifiche all'interno di un apparato governativo o amministrativo.

- **Vincoli Tecnico-Organizzativi**: Altri CSIRT potrebbero essere creati all'interno di organizzazioni specifiche o indirizzati a una clientela di mercato particolare.

Oltre alla constituency principale, un CSIRT potrebbe anche collaborare con altre entità al di fuori della sua comunità di riferimento. Questi rapporti possono essere parte di community informali, più o meno strutturate, che si occupano di scambio di informazioni e possono coinvolgere accordi specifici o regolamenti definiti all'interno di tali comunità.
L'identificazione e la definizione della constituency rappresentano un passo critico per il successo di un CSIRT. A seconda dei servizi offerti e delle loro caratteristiche, un CSIRT potrebbe dover definire più di una constituency. In alcuni casi, potrebbero verificarsi sovrapposizioni tra le constituency servite da uno o più CSIRT, il che richiede un coordinamento efficace per evitare duplicazioni e conflitti che potrebbero portare all'erogazione di servizi inefficaci e/o in reciproco contrasto (si pensi ad esempio alla sovrapposizione di un CSIRT privato con uno governativo nell'ambito degli stessi servizi).
Con riferimento alle diverse tipologie di CSIRT individuati in Tabella 2.1, è possibile individuare specifiche constituency.
Infine, anche se una constituency è limitata nel suo ambito, un CSIRT potrebbe

CATEGORIA DI CSIRT	**CONSTITUENCY DI RIFERIMENTO**
Nazionale	Cittadini e organizzazioni pubbliche e private appartenenti aduna specifica nazione.
Governativo	Cittadini, agenzie governative e altre organizzazioni pubbliche.
Settoriale	Utenti e organizzazioni operanti in specifici settori.
Militare	Personale appartenente a corpi militari/difesa o di entità organizzative strettamente correlate.
Privato o interno	Personale interno e dipartimenti/funzioni dell'organizzazione ospitante.
Commerciale	Clienti pubblici o privati che si avvalgono di un fornitore esterno.

Tabella 2.1: Constituency di riferimento per tipologia di CSIRT

necessitare di interagire con entità esterne per raccogliere informazioni rilevanti per il suo operato. Alcuni CSIRT svolgono il ruolo di coordinatori tra la loro constituency e altre entità esterne, come altri CSIRT, forze dell'ordine, fornitori, media, promuovendo la condivisione delle informazioni e la collaborazione.
Promuovere i servizi dello CSIRT sia all'interno della sua constituency che oltre richiede una comunicazione efficace attraverso vari canali, tra cui siti web istituzionali, workshop e iniziative di sensibilizzazione, al fine di garantire una comprensione chiara

del ruolo dello stesso e dei servizi che offre, ottenendo riconoscimento anche nella più ampia comunità di CSIRT.

2.3 Modello Organizzativo

La struttura organizzativa di un CSIRT è un elemento cruciale per sostenere operazioni efficaci e proattive nei confronti della propria constituency. In termini di responsabilità e coordinamento, un CSIRT può adottare diverse modalità organizzative.
Nel primo scenario abbiamo un livello di autorità **Completo**, ovvero il CSIRT opera con piena autorità, guidando la sua constituency nell'attuazione di azioni necessarie per migliorare la postura di sicurezza dell'organizzazione o per affrontare un incidente. Ha il potere di prendere decisioni e imporre direttive.
Nel secondo scenario abbiamo un livello di autorità **Condiviso**, in questo caso il CSIRT collabora con la sua constituency per influenzare il processo decisionale relativo alle azioni da intraprendere. Tuttavia, non ha il potere di imporre decisioni unilaterali, ma lavora in collaborazione.
Infine, nel terzo scenario abbiamo un livello di autorità **Assente**, a differenza dei precedenti, in alcuni casi, un CSIRT potrebbe adottare un modello che non conferisce autorità al CSIRT stesso. In questo scenario, il CSIRT fornisce consulenza e supporto alla constituency ma non ha poteri decisionali diretti.
Va notato che alcuni servizi tipicamente offerti da un CSIRT (e presentati più avanti in dettaglio nel paragrafo 2.5), come il tracciamento degli incidenti o il monitoraggio e il rilevamento degli intrusi, potrebbero essere erogati solo se esiste un livello di autorità completo o parziale nei confronti della constituency. Questi servizi possono essere resi disponibili attraverso specifici accordi contrattuali tra il CSIRT e i membri della constituency interessati.
Il modello organizzativo del CSIRT può variare da distribuito a centralizzato o coordinato, a seconda della missione, dei servizi offerti e delle esigenze della constituency. In letteratura [16], sono stati identificati tre modelli operativi di CSIRT:

Indipendente : Un CSIRT indipendente opera come un'entità separata, fornendo servizi di sicurezza informatica in modo autonomo (Figura 2.1).

Incorporato : Un CSIRT incorporato è parte di un'organizzazione più ampia, come un'azienda o un'istituzione governativa, e fornisce servizi di sicurezza informatica all'interno di quella struttura (Figura 2.2).

Campus : Un CSIRT di tipo campus è specificamente dedicato a un'organizzazione accademica o a una comunità di campus e offre servizi di sicurezza informatica per quei contesti (Figura 2.3).

La scelta del modello strutturale del CSIRT dipende dalla missione, dai servizi offerti e dalla natura della constituency servita.

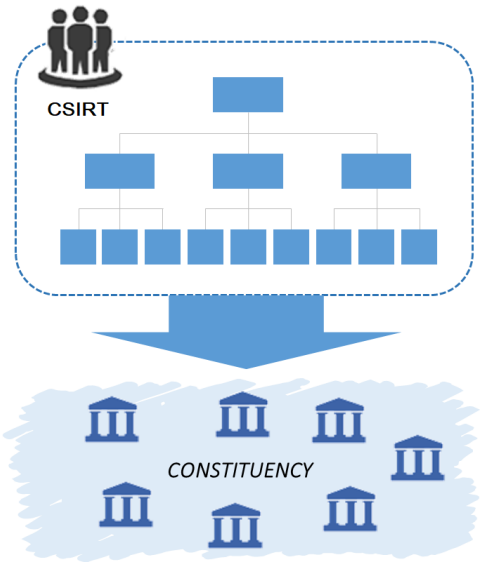

Figura 2.1: Modello indipendente

Nel `Modello Indipendente` il CSIRT viene istituito come un'organizzazione indipendente con una propria direzione e risorse dedicate, anche se può essere collocato all'interno di un'entità più ampia che potrebbe a sua volta far parte della constituency. Il modello indipendente si basa su un CSIRT dedicato e centralizzato che assume la piena responsabilità e autorità per tutte le attività di analisi, gestione e risposta agli incidenti. Il personale operativo è formalmente assegnato al CSIRT e riporta direttamente al responsabile del CSIRT (noto come Responsabile CSIRT, paragrafo 2.6.1).

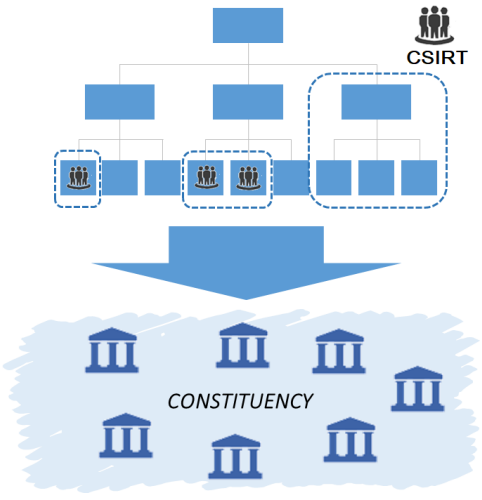

Figura 2.2: Modello Incorporato

Il `Modello Incorporato` viene adottato quando si decide di creare un CSIRT all'interno di un'organizzazione esistente, facendo leva sulle risorse già operative e allocate presso altre strutture organizzative, come ad esempio la Funzione IT e di

Sicurezza. Il CSIRT è guidato da un responsabile che è responsabile delle attività complessive del CSIRT. Questo responsabile riunisce gli specialisti necessari per affrontare gli incidenti o svolgere le attività del CSIRT e può richiedere assistenza all'interno dell'organizzazione per ottenere supporto.

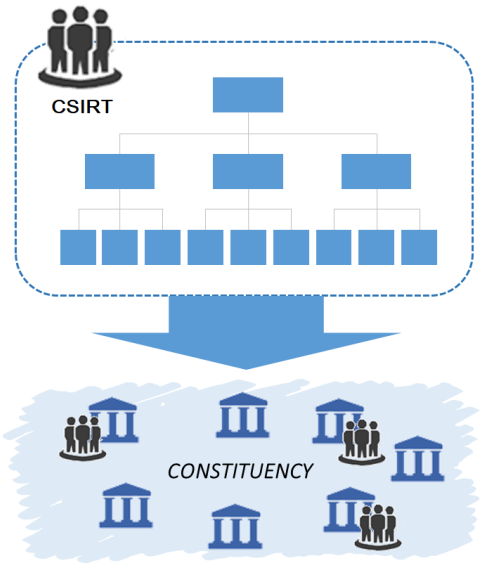

Figura 2.3: Modello Campus

Infine, nel `Modello Campus`, ogni entità all'interno della constituency è autonoma rispetto al CSIRT e alle altre entità che compongono la stessa constituency. In questo scenario, il CSIRT, anche se è una struttura separata, utilizza le risorse messe a disposizione dalle altre organizzazioni all'interno della constituency (ad esempio, se dispongono di un proprio Security Operations Center - SOC). Il CSIRT offre i suoi servizi sia alle entità che forniscono risorse sia a tutti gli altri membri della constituency.
Il modello campus è comunemente adottato nei CSIRT di settore, tra cui rientrano anche i CSIRT accademici/di ricerca e quelli militari, poiché consente di bilanciare le esigenze di coordinamento centrale con quelle di autorità locale. Questo è particolarmente utile quando si tratta di utenti singoli o consorziati appartenenti allo stesso settore professionale o con interessi comuni, come ad esempio la sanità o i trasporti. D'altro canto, i modelli indipendente e incorporato sono più adatti per i CSIRT territoriali, specialmente quando la constituency è caratterizzata da una distribuzione geografica estesa, consentendo loro di operare efficacemente sotto la supervisione dell'ente che li ha istituiti.

2.4 Modello Amministrativo

Dal punto di vista amministrativo, i CSIRT possono adottare diverse modalità amministrative, a seconda dei seguenti fattori.

Organizzazione Interna : Alcuni CSIRT possono essere una parte integrante dell'organizzazione ospitante, come una funzione o un dipartimento dedicato alla sicurezza informatica. In questo caso, le responsabilità del CSIRT possono estendersi oltre alla risposta agli incidenti, includendo altre funzioni. Questo modello semplifica l'avvio e può sfruttare sinergie con altre parti dell'organizzazione. Tuttavia, è essenziale stabilire pratiche e processi per garantire una chiara separazione dei ruoli e delle responsabilità al fine di evitare sovrapposizioni con le attività dell'organizzazione ospitante.

Società In-House : Alcuni CSIRT possono essere incorporati in una società in-house, che può essere una nuova entità giuridica o già esistente. Questa società è di proprietà totale o parziale, diretta o indiretta, di un'organizzazione che richiede i servizi del CSIRT. Sebbene questo possa garantire un chiaro focus e autonomia gestionale, può comportare una maggiore complessità amministrativa, tempi di avvio più lunghi e costi operativi più elevati, inclusi duplicati di posizioni apicali.]

Outsourcing : In alternativa, un'organizzazione può affidarsi a un fornitore esterno per i servizi del CSIRT, attraverso meccanismi di outsourcing. Questo approccio può essere vantaggioso per ridurre i costi e ottenere l'accesso a competenze specialistiche. Tuttavia, richiede contratti chiari e potrebbe comportare la perdita di alcune competenze interne.

Una soluzione efficace per i CSIRT di una rete nazionale o territoriale è la creazione di gruppi di lavoro estesi, che coinvolgono rappresentanti delle diverse entità della constituency (aziende, enti governativi, società in-house, ecc.). Questa collaborazione offre diversi vantaggi come la riduzione dei costi, la condivisione delle competenze e la possibilità di una risposta coordinata. Il primo lo si ottiene semplicemente coinvolgendo più entità, in modo tale da condividere i costi fissi, riducendo il carico finanziario su ciascuna entità, risultando particolarmente vantaggioso quando si gestiscono entità eterogenee. Tramite il secondo vantaggio competenze locali diventano un patrimonio comune, riducendo il rischio di perdita di competenze tra i diversi CSIRT. Il patrimonio informativo viene condiviso, consentendo una risposta più rapida agli incidenti. E, infine, la collaborazione permette una risposta più coordinata agli incidenti, con una regia centralizzata che coordina tutte le entità coinvolte.
Un'altra opzione per aumentare le capacità di un CSIRT è ricorrere a competenze esterne, specializzate in determinati settori o aree di competenza. Questo può comportare vantaggi come la riduzione dei costi tramite l'`outsourcing` a fornitori specializzati si può ridurre i costi rispetto alla formazione e alla gestione di personale interno; una risposta più rapida all'innovazione, poiché i fornitori specializzati possono adattarsi rapidamente all'evoluzione delle minacce e delle tecnologie, offrendo un vantaggio competitivo; contratti vincolanti, ovvero gli accordi contrattuali possono essere basati su risultati o prestazioni, garantendo un livello di servizio definito;

possibilità di confronto e `benchmarking` dal momento in cui collaborare con fornitori esterni può portare a nuove idee e pratiche di successo che possono essere adottate internamente.
In generale, la scelta della modalità amministrativa dipenderà dalle esigenze specifiche del CSIRT, dalla sua constituency e dalle risorse disponibili. La collaborazione tra entità e il ricorso a competenze esterne possono essere soluzioni efficaci per affrontare le sfide della sicurezza informatica in modo efficiente ed efficace.

2.5 Servizi

Secondo fonti autorevoli nel campo della sicurezza informatica [16, 17, 18](ENISA, "Un approccio graduale alla creazione di un CSIRT" del 2006, CMU-SEI "Handbook for Computer Security Incident Response Teams" del 2003, CMU-SEI "Organizational Models for Computer Security Incident Response Teams (CSIRTs)" del 2003), i servizi forniti da un CSIRT possono essere suddivisi in quattro categorie principali:

1. **Servizi Reattivi**: Questi servizi sono orientati alla gestione degli incidenti una volta che si sono verificati. L'obiettivo principale è ridurre al minimo il danno derivante dagli incidenti e rispondere alle richieste di assistenza provenienti dalla constituency. Questi incidenti possono essere notificati da terzi o rilevati internamente o tramite monitoraggio delle minacce.

2. **Servizi Proattivi**: Questi servizi sono mirati alla prevenzione degli incidenti. L'obiettivo è condividere informazioni e utilizzare strumenti specifici per migliorare la sicurezza delle infrastrutture e dei processi nella comunità di riferimento prima che si verifichi un incidente o che venga rilevata una minaccia. Questi servizi possono anche includere attività di gestione e condivisione delle informazioni provenienti da fornitori e altre comunità, allo scopo di limitare la diffusione di attacchi futuri o simili.

3. **Servizi di Gestione della Qualità della Sicurezza**: Questi servizi riguardano le pratiche per migliorare la sicurezza generale dei membri della constituency. Sono progettati per incorporare le lezioni apprese dalle esperienze di risposta a incidenti, vulnerabilità e attacchi al fine di migliorare continuamente la sicurezza.

4. **Gestione degli Artefatti**: Questo servizio coinvolge la raccolta e l'analisi di elementi o prove (come file, codici malevoli o tracce in memoria) che sono coinvolti in azioni malevole o incidenti.

Queste categorie di servizi offerti da un CSIRT sono essenziali per garantire la sicurezza delle infrastrutture informatiche e la risposta efficace agli incidenti.
La Tabella 2.2 offre una possibile suddivisione dei servizi all'interno di queste categorie.

SERVIZI REATTIVI	**SERVIZI PROATTIVI**
Allarmi e avvisi	Annunci
Gestione degli incidenti	Controllo tecnologico
Analisi degli incidenti	Revisioni e valutazioni della sicurezza
Sostegno della risposta agli incidenti	Configurazione e mantenimento della sicurezza
Coordinamento della risposta agli incidenti	Sviluppo di strumenti di sicurezza
Risposta agli incidenti in loco	Servizi di rilevamento intrusioni
Gestione delle vulnerabilità	
Analisi delle vulnerabilità	
Risposta alle vulnerabilità	
Coordinamento della risposta alle vulnerabilità	

GESTIONE DELLA QUALITÀ DELLA SICUREZZA	**GESTIONE DEGLI ARTEFATTI**
Analisi dei rischi	Analisi degli artefatti
Continuità operativa e ripristino in caso di disastro	Risposta agli artefatti
Consulenza sulla sicurezza	Coordinamento della risposta agli artefatti
Sensibilizzazione	
Istruzione/formazione	
Valutazione o certificazione dei prodotti	
Divulgazione di informazioni relative alla sicurezza	

Tabella 2.2: Elenco dei servizi CSIRT (fonte: CERT/CC, ENISA)

Nel contesto della trattazione, si propone l'adozione di un modello alternativo per la definizione del catalogo dei servizi essenziali offerti da un CSIRT Regionale chiamato il modello IRPA (*Incident Response Public Administration*), in uso presso il CERT-AGID. Questa scelta mira a sfruttare sinergie e definire un insieme di servizi aggiuntivi per gli CSIRT Regionali rispetto a quelli forniti dal CERT-AGID alla sua constituency.

Il modello IRPA, all'interno del contesto della pubblica amministrazione italiana, si prefigge diversi obiettivi di fondamentale importanza.

Innanzitutto, mira a prevenire e mitigare gli impatti derivanti dagli incidenti sulla sicurezza delle informazioni. Questo obiettivo principale pone l'accento sulla necessità di evitare che incidenti informatici possano danneggiare o compromettere la sicurezza dei dati e dei sistemi.

Un secondo aspetto cruciale riguarda l'istituzione di un modello strategico che definisca chiaramente i ruoli e le responsabilità dei vari attori coinvolti nella gestione degli

incidenti di sicurezza informatica. Questo assicura che ci sia una chiara comprensione di chi deve fare cosa in situazioni di emergenza.
Il modello IRPA mira anche all'unificazione delle politiche esistenti, cercando di armonizzare le diverse linee guida in un piano strategico coerente e adeguato al contesto specifico della pubblica amministrazione.
Promuovere la consapevolezza, la condivisione delle informazioni e il coordinamento, sia durante la gestione quotidiana che in situazioni di crisi, è un altro obiettivo chiave. Questo garantisce che le informazioni rilevanti vengano scambiate in modo efficiente e che le risposte agli incidenti siano coordinate.
Un altro punto importante è stabilire quando e come le attività operative dovrebbero essere integrate in una risposta coordinata a livello di pubblica amministrazione o nazionale. Questo assicura che, in situazioni di emergenza, le azioni siano sincronizzate per massimizzare l'efficacia.
Infine, il modello IRPA si concentra sugli incidenti che potrebbero avere un impatto significativo sulla sicurezza, la salute, l'economia dei cittadini e la credibilità della pubblica amministrazione. Questa focalizzazione consente di indirizzare le risorse e le attenzioni verso le minacce più rilevanti e di maggiore impatto.
A questo scopo, il modello IRPA ha l'obiettivo di coordinare e fornire una struttura chiara per affrontare le sfide della sicurezza informatica nella pubblica amministrazione italiana. Questo modello si articola in cinque fasi chiave.
La fase di "`Preparazione e Prevenzione`" è fondamentale. In questa fase, vengono stabilite regole di sicurezza nazionali basate sull'esperienza pregressa e si diffondono informazioni cruciali sulla sicurezza. Questo processo mira a migliorare la consapevolezza verso le tematiche di cybersicurezza all'interno della pubblica amministrazione.
La "`Rilevazione`" è la seconda fase, e coinvolge il monitoraggio costante della sicurezza, la condivisione delle informazioni e l'uso di fonti di intelligence sia *open* che *closed-source* per individuare incidenti o minacce in modo tempestivo.
La fase successiva è la fase di "`Analisi`". Qui, gli incidenti segnalati dalle pubbliche amministrazioni vengono analizzati in dettaglio. Questa fase implica la raccolta e l'analisi approfondita delle prove per comprendere appieno la natura e la portata dell'incidente.
La "`Risposta`" è una fase critica in cui si definiscono e coordinano le azioni necessarie per affrontare l'incidente. Questa coordinazione coinvolge sia le pubbliche amministrazioni coinvolte che altre parti come i fornitori di servizi Internet (ISP), lo *CSIRT-Nazionale* e i media. Si valutano e applicano le normative pertinenti, ad esempio coinvolgendo le autorità competenti in caso di frodi o crimini informatici.
Infine, la "`Fase di Ripristino`" è dedicata a pianificare come ripristinare i servizi una volta che la minaccia è stata affrontata con successo. In altre parole, si tratta di ritornare alla normalità una volta che la minaccia è stata eliminata.
In sintesi, il modello IRPA mira a supportare una vasta gamma di entità, comprese la pubblica amministrazione, le infrastrutture critiche e le organizzazioni private, nell'affrontare le sfide della sicurezza informatica. Il suo obiettivo è garantire che

la società, la salute, la sicurezza, l'economia e il benessere dei cittadini non siano compromessi dagli incidenti informatici.
I servizi proposti dal modello IRPA sono illustrati nella Tabella 2.3 che possiamo vedere qui di seguito.

FASE MODELLO IRPA	**SERVIZI**
Preparazione e prevenzione	Accreditamento e linee guida Informative Formazione e awareness Supporto al risk mapping Security assessment e consulenza
Rilevazione	Ticketing Threat intelligence
Analisi	Correlazione Analisi incidente Triage & escalation
Risposta	Coordinamento della risposta Supporto alle azioni di risposta Monitoraggio della risposta
Ripristino	Analisi post-incidente e coordinamento Monitoraggio del ripristino
Tutte le fasi	Information Sharing

Tabella 2.3: Modello dei servizi basato su IRPA

2.5.1 Servizi offerti dai CSIRT Regionali

L'offerta dei servizi da parte di un CSIRT Regionale è un passaggio critico che richiede attenta pianificazione e adattamento alle specifiche esigenze della comunità da servire. La selezione dei servizi deve iniziare con un'analisi approfondita delle necessità della constituency, ponendo particolare enfasi sui servizi minimi ed essenziali, nonché quelli di maggiore rilevanza per le pubbliche amministrazioni locali coinvolte. È fondamentale evitare un approccio eccessivamente ambizioso, che potrebbe sovraccaricare il CSIRT Regionale con un numero eccessivo di servizi rispetto alle risorse disponibili e alle reali necessità della comunità. Questo potrebbe comprometterne la fattibilità e la sostenibilità nel lungo termine. La decisione di attivare specifici servizi dovrebbe essere graduale, e l'espansione del portafoglio di servizi dovrebbe essere basata sul feedback e le esigenze della comunità di riferimento.
In secondo luogo, il modello di servizio del CSIRT Regionale dovrebbe essere complementare a quello offerto dal CERT-AGID. Inizialmente, il focus dovrebbe essere sui servizi di base ed essenziali, dove la vicinanza al territorio può portare a miglioramenti significativi nell'efficacia del supporto fornito alla constituency locale, rispetto a un approccio centralizzato da parte del CERT-AGID.

Tuttavia, con il tempo e un maggiore livello di maturità, il CSIRT Regionale potrebbe valutare l'offerta di servizi più complessi e tecnologicamente avanzati, in base alle risorse disponibili e alle priorità identificate attraverso una valutazione dei rischi. La selezione dei servizi essenziali si basa su due fattori chiave: il grado di complessità operativa e la rilevanza del servizio per la comunità servita.
Nelle sezioni successive, verranno delineati i servizi di base che un CSIRT Regionale dovrebbe fornire alla propria constituency, tenendo conto delle risorse necessarie per erogarli in modo efficace.

Accreditamento

L'accreditamento è un servizio cruciale offerto da un CSIRT Regionale, che si sviluppa in due aspetti distinti. In primo luogo, il CSIRT Regionale si accredita presso il CERT-AGID, diventando parte della sua constituency. In questa fase, il CERT-AGID fornisce un portale dedicato attraverso il quale il CSIRT Regionale riceve aggiornamenti su nuove vulnerabilità e minacce. Questi aggiornamenti possono essere ricevuti manualmente, ad esempio sotto forma di news, bollettini e liste nere, o in modalità automatica, attraverso sistemi come `STIX/TAXII` e `MISP`. Inoltre, il portale fornisce l'accesso a risorse riservate, quali indicatori di compromissione (IOC), dati sulle violazioni e altro materiale informativo. Questa fase permette anche di partecipare a eventi di formazione organizzati dal CERT-AGID e di ricevere assistenza consulenziale dedicata.
Il secondo aspetto riguarda l'accreditamento delle singole PAL (*Pubbliche Amministrazioni Locali*) nei confronti del CSIRT Regionale, consentendo loro di entrare a far parte della sua constituency. Per richiedere l'accreditamento, una PAL che soddisfi i requisiti necessari per farne parte contatta il CSIRT Regionale attraverso i canali appropriati. Il Responsabile della Sicurezza Informatica della PAL deve fornire prova della propria identità e del ruolo all'interno dell'ente. Inoltre, si impegna a fornire al CSIRT tutte le informazioni necessarie per una corretta gestione degli incidenti di sicurezza.
Queste informazioni includono:

- *Identificazione delle persone dell'ente in grado di intervenire in caso di incidente informatico e comunicazione delle relative modalità di contatto.* Queste figure devono essere preparate per affrontare una crisi informatica in tutti i suoi aspetti, compreso il trattamento di informazioni sensibili potenzialmente esfiltrate durante un attacco cibernetico. Queste persone svolgono un ruolo critico nella gestione dell'incidente, compresi aspetti come la comunicazione sia interna che esterna all'organizzazione, il coordinamento delle diverse aree coinvolte nel contenimento e nel ripristino delle operazioni e la raccolta di prove per eventuali procedimenti legali. Inoltre, è fondamentale fornire informazioni dettagliate su queste figure, compresi i loro nomi, il ruolo aziendale, i numeri di contatto (telefono fisso, cellulare, e-mail e altre modalità di comunicazione), le

fasce orarie di contatto e la disponibilità di sostituti al di fuori di queste fasce. Mantenere queste informazioni aggiornate nel tempo è di vitale importanza, tenendo traccia di cambi di ruolo, dimissioni, pensionamenti o spostamenti in altre sedi.

- *La presenza o meno di una procedura documentata per la gestione di incidenti di sicurezza.* Questo aiuta il CSIRT a valutare il livello di preparazione dell'ente per affrontare incidenti, se ha adottato le migliori pratiche in questo campo e se è in grado di raccogliere le informazioni necessarie per trattare gli incidenti in modo efficace.

- *La presenza o meno di una documentazione di analisi del rischio e della classificazione di informazioni.* Analogamente, la presenza di questa documentazione è un indicatore della consapevolezza dell'ente riguardo agli effetti potenziali di un incidente di sicurezza, permettendo di valutare l'impatto dell'incidente e di pianificare una risposta adeguata.

- *L'elenco dei domini e degli indirizzi di rete che afferiscono all'ente, un elenco dell'hardware e del software utilizzato.* Questo consente al CSIRT di comunicare in modo mirato informazioni sulle vulnerabilità scoperte, riducendo al minimo le informazioni non necessarie. Questo processo di scrematura contribuisce a una comunicazione più efficace e orientata alle esigenze specifiche dell'ente accreditato.

Questi passaggi sono fondamentali per garantire che il CSIRT Regionale sia in grado di fornire un supporto efficace in caso di incidenti di sicurezza. Il CSIRT deve essere visto come un partner prezioso, pronto a fornire assistenza e consigli, ma non può sostituire le best practice interne dell'ente. La cooperazione e la condivisione delle informazioni sono fondamentali per affrontare le sfide legate alla sicurezza informatica. Una volta completata la procedura di accreditamento con successo, l'ente potrà accedere a tutti i servizi che il CSIRT regionale mette a disposizione della propria constituency.

Informative

Il servizio di Informative rappresenta un mezzo essenziale attraverso il quale il CSIRT Regionale diffonde informazioni rilevanti alle PAL (*Pubbliche Amministrazioni Locali*) accreditate. Queste informazioni vengono trasmesse sotto forma di alert periodici, bollettini di sicurezza, comunicazioni generiche o segnalazioni specifiche di sicurezza. Questo servizio ha lo scopo di informare le PAL su diversi aspetti:

- **Nuovi Scenari di Rischio**: Vengono condivise informazioni riguardo a scenari di rischio emergenti di natura tecnologica, normativa e organizzativa che potrebbero avere un impatto significativo sulle PAL all'interno della constituency.

- **Nuove Minacce e Vulnerabilità**: Vengono segnalate nuove minacce o vulnerabilità che potrebbero influenzare i sistemi e le applicazioni in uso presso le PAL.
- **Attacchi in Corso**: Si fornisce notizia di attacchi attualmente in corso contro le PAL, identificando il potenziale impatto sulla loro infrastruttura tecnologica.
- **Azioni della Comunità**: Si informa sulle azioni intraprese da altri soggetti all'interno della comunità delle PAL in risposta a eventi o incidenti di sicurezza.

Questo servizio è progettato per agevolare la diffusione di informazioni tempestive e direttamente applicabili riguardo a scenari di rischio emergenti, attacchi in corso, tendenze nei fenomeni cyber che interessano settori specifici e potenziali implicazioni per le pubbliche amministrazioni locali e le loro utenze. Inoltre, agevolando l'attività informativa preventiva a livello locale, gli CSIRT Regionali svolgono un ruolo chiave nell'esercitare un controllo diretto sulla loro constituency e nell'assicurare che le informazioni siano mirate ed efficaci per le esigenze locali.

Formazione e Awareness

Il servizio di Formazione e Awareness è progettato per incrementare la consapevolezza del personale delle PAL responsabile della gestione dei processi di sicurezza informatica. Questo servizio si focalizza su diversi aspetti, tra cui:

- **Principi di Gestione della Sicurezza delle Informazioni e della Cybersecurity**: Fornisce una formazione riguardo ai principi fondamentali della gestione della sicurezza delle informazioni e delle pratiche di sicurezza informatica.
- **Tematiche Specifiche**: Approfondisce argomenti specifici quali il risk management (gestione del rischio) e la gestione degli incidenti di sicurezza. Questa formazione aiuta il personale a comprendere e gestire meglio i rischi di sicurezza informatica.
- **Processi e Procedure nel dominio della PA**: Illustra i processi e le procedure adottate nel contesto della pubblica amministrazione per favorire la collaborazione e l'interazione tra le entità locali e gli CSIRT Regionali.

Questo servizio può essere attivato su richiesta delle PAL accreditate. Le modalità di formazione possono variare e includere corsi periodici in aula o in modalità remota tramite l'accesso a piattaforme di formazione online. Inoltre, possono essere organizzate iniziative di sensibilizzazione come workshop, eventi locali e campagne informative territoriali, mirate a evidenziare i rischi legati alla sicurezza informatica affrontati dalle entità locali.

Ticketing

Il servizio di Ticketing funge da punto di ingresso fondamentale per il processo di gestione degli incidenti. Questo servizio si basa su una sofisticata piattaforma di trouble ticketing che svolge un insieme di funzioni interconnesse.
All'interno di ciascuna PAL accreditata, gli utenti autorizzati hanno la possibilità di segnalare direttamente o richiedere l'apertura di un ticket presso il CSIRT Regionale al fine di notificare eventuali incidenti legati alla sicurezza informatica all'interno della propria organizzazione.
Gli analisti del CSIRT Regionale giocano un ruolo essenziale nell'aggiornamento e nell'analisi dei ticket. Mantengono costantemente aggiornate le informazioni contenute nei ticket, fornendo i risultati delle analisi compiute nelle varie fasi del processo di gestione degli incidenti. Inoltre, hanno la facoltà di allegare documentazione rilevante, come comunicazioni intercorse con fornitori, documenti sottoposti ad analisi e dettagli relativi a conversazioni verbali.
Un elemento cruciale è la possibilità, offerta dalla piattaforma di ticketing, di aprire ticket indirizzati ad altre entità coinvolte e di seguire da vicino lo sviluppo di ciascun evento segnalato. Questa capacità semplifica notevolmente il monitoraggio dei livelli di servizio e delle attività svolte da tutti i soggetti coinvolti.
Un altro aspetto significativo del servizio di Ticketing è la centralizzazione delle informazioni relative agli incidenti. Questa funzione consente di alimentare una knowledge base che fornisce al CSIRT Regionale gli strumenti per effettuare analisi approfondite e, allo stesso tempo, agevola il collegamento tra segnalazioni provenienti da diverse PAL. Questa sinergia contribuisce a individuare eventi sospetti e modelli di attacco che si ripetono nel tempo.

Correlazione

Il servizio di Correlazione consente al CERT Regionale di mettere in relazione le segnalazioni provenienti dal sistema di ticketing con le informazioni raccolte da altre fonti, tra cui il CERT-AGID, al fine di fornire al servizio di analisi degli incidenti una visione completa di ciascuna segnalazione.
Nello specifico, utilizzando la piattaforma di trouble ticketing e la *knowledge base* a essa collegata, si effettuano ricerche mirate per individuare connessioni tra ticket diversi. Questo processo mira a:

- Rilevare modelli di attacco che si ripetono nel tempo o che hanno come obiettivo diversi target.
- Individuare eventuali eventi con impatto sistemico o eventi che coinvolgono più PAL in maniera trasversale.

In questo modo, il servizio di Correlazione contribuisce in modo significativo a identificare pattern di minacce, tendenze e incidenti di ampia portata che richiedono

una risposta coordinata tra diverse entità all'interno della constituency del CSIRT Regionale.

Analisi degli incidenti

In risposta a un incidente che è stato segnalato e inizialmente classificato da una PAL, il team di analisti di sicurezza del CSIRT Regionale attiva il servizio di Analisi Incidente. Questo servizio ha l'obiettivo di:

- Verificare e analizzare le informazioni inviate dalla PAL e allegare al ticket dell'incidente.
- Riesaminare la classificazione effettuata dalla PAL e, se necessario, riclassificare l'evento. Questa revisione tiene conto dell'impatto dell'incidente da una prospettiva sistemica e comporta l'incrocio delle informazioni ricevute con eventuali indicazioni correlate, pervenute da altre PAL.

In questo modo, il servizio di Analisi Incidente contribuisce a garantire che gli incidenti siano correttamente valutati e classificati, tenendo conto delle loro implicazioni a livello sistemico e consentendo una visione più completa e approfondita delle minacce alla sicurezza.

Triage & escalation

Attraverso il servizio di Triage ed Escalation, il CSIRT Regionale esegue una valutazione standardizzata degli incidenti segnalati, esprimendo il livello di criticità dell'incidente su una scala ordinale con vari livelli di impatto (si consiglia una scala a cinque livelli simile a quella utilizzata dal CERT-AGID).
Al termine della fase di triage, il CSIRT Regionale può intraprendere le seguenti azioni:

- **Declassificazione dell'incidente**: Se si determina che si trattava di un falso positivo, il CSIRT Regionale invia una comunicazione alla PAL coinvolta, chiude il ticket e allega i risultati delle analisi condotte.
- **Modifica della classificazione precedente**: Se necessario, il CSIRT Regionale può modificare il livello di classificazione precedentemente assegnato e comunicato dalla PAL che ha segnalato l'incidente.
- **Avvio delle attività di gestione dell'incidente**: Se si ritiene che l'incidente richieda interventi specifici, il CSIRT Regionale avvia le attività di trattamento seguendo le procedure condivise con le PAL durante la fase di accreditamento.

Nel caso di incidenti distribuiti che coinvolgono diverse PAL all'interno della sua constituency, il CSIRT Regionale invia segnalazioni urgenti alle PA coinvolte e coordina tutte le attività di gestione dell'incidente.

Se si verifica un incidente di livello massimo (ad esempio, livello 4 secondo una scala da definire), il CSIRT Regionale deve dichiarare lo stato di emergenza e attivare un'escalation verso il CERT-AGID o il CSIRT-Italia, collaborando con quest'ultimo per tutte le attività successive di gestione dell'incidente.

Supporto alle azioni di risposta

Nella fase di Supporto alle Azioni di Risposta, il CSIRT Regionale fornisce assistenza alle PAL all'interno della sua constituency, offrendo soluzioni potenziali per la gestione degli incidenti. Questa assistenza può includere procedure, modalità di risposta e competenze specifiche relative a un particolare tipo di attacco, nel caso in cui l'Ente non le possieda.
In particolare, il CSIRT Regionale collabora con le PAL nella definizione del piano di trattamento dell'incidente. Questo piano comprende:

- Identificazione dei servizi e dei sistemi coinvolti nell'attacco, con la relativa classificazione in base alla criticità.
- Definizione delle misure di contrasto e contenimento progettate per affrontare l'incidente e riportare la situazione a uno stato ordinario.
- Specifica degli obiettivi attesi dall'implementazione delle misure di sicurezza sopra menzionate.

Nel caso di incidenti di rilevanza sistemica che coinvolgono più PAL, il CSIRT Regionale coordina il coinvolgimento delle PAL interessate, fornendo loro tutte le informazioni necessarie per affrontare l'incidente in corso.

Information Sharing

L'Information Sharing rappresenta il fondamento dei processi degli CSIRT e della rete di entità a livello nazionale e internazionale con cui collaborano. Questo sistema stabilisce le regole e le modalità per la condivisione delle informazioni in entrata e in uscita con tutti gli attori coinvolti. La condivisione di informazioni deve garantire una comunicazione tempestiva a tutte le parti interessate, mantenendo i livelli di classificazione previsti.
La condivisione efficace delle informazioni permette agli CSIRT di raccogliere input, elaborare dati e condividere conoscenze, aumentando la capacità reattiva e proattiva degli attori coinvolti. Questa condivisione arricchisce le informazioni originali, consentendo valutazioni più precise. Per massimizzare l'utilità delle informazioni condivise, queste devono essere "*actionable*", cioè immediatamente utilizzabili in azioni operative. Le informazioni condivise possono riguardare minacce, campagne, vulnerabilità, exploit [1] e indicatori di compromissione (IOC).

[1] Ovvero programmi dannosi che contengono dati o codici eseguibili in grado di sfruttare una o più vulnerabilità di un software presente su un sistema.

Alcuni principi fondamentali della condivisione delle informazioni includono la fiducia tra gli attori coinvolti, l'adozione di schemi di classificazione standard, la definizione del livello di accuratezza richiesto, la tempestività delle comunicazioni e la possibilità di anonimizzare le fonti delle informazioni.
Le modalità di attuazione dell'Information Sharing possono includere la raccolta di informazioni da diverse fonti, la distribuzione di alert, bollettini e informative, nonché comunicazioni periodiche attraverso incontri o workshop. Inoltre, è essenziale stabilire strumenti e metodologie standard per la trasmissione automatizzata delle informazioni, specialmente per la condivisione di liste di IOC.
L'obiettivo finale è creare una rete di CSIRT collegati tra loro in grado di scambiare informazioni in tempo reale usando standard comuni e una tassonomia condivisa. Questo consentirà una risposta più efficace alle minacce cibernetiche. CERT-AGID, ad esempio, sta lavorando su una sperimentazione che coinvolge un gruppo di attori pubblici e privati per definire regole di trasmissione utilizzando *MISP*, *CNTI* e *EasyList* per il trasporto. Questo approccio consente la condivisione automatizzata delle informazioni tra nodi della rete CERT/CSIRT.

2.6 Struttura organizzativa e risorse umane

Per realizzare gli obiettivi stabiliti nella strategia del CSIRT, è fondamentale definire una struttura organizzativa adeguata e in grado di adattarsi all'evoluzione dei processi e dei servizi forniti nel tempo. Questa struttura organizzativa dovrebbe specificare i ruoli chiave, le relative competenze e responsabilità. L'organizzazione interna deve essere periodicamente riesaminata per assicurare un dimensionamento adeguato in base al volume e al tipo di eventi e incidenti gestiti, alle fonti informative analizzate e alle relazioni di condivisione delle informazioni con la comunità di riferimento.
La struttura organizzativa di un CSIRT dipende innanzitutto dalla struttura esistente nell'organizzazione ospitante e dalle caratteristiche della comunità di riferimento, nonché dalla possibilità, e relativa facilità, di potersi avvalere, in modo permanente o per esigenze specifiche, delle competenze di professionisti esterni. Indipendentemente da queste considerazioni, per avviare le attività di un CSIRT è consigliabile definire una struttura organizzativa che copra le seguenti aree:

Management : questa area è responsabile della pianificazione strategica, direzione e leadership del CSIRT. Gestisce le relazioni con la constituency e stabilisce collaborazioni con altre organizzazioni pubbliche e private.

Operations : quest'area è responsabile della gestione generale e dell'operatività dei servizi forniti alla constituency. Include operatori e analisti, supportati da team di esperti specializzati in aree specifiche.

Processi di supporto : questi processi consentono il funzionamento generale del CSIRT. Includono attività come amministrazione e controllo, gestione delle infrastrutture IT, gestione del personale e comunicazione interna ed esterna.

Durante la fase iniziale di avvio del CSIRT, potrebbe non essere possibile assegnare formalmente tutti i ruoli. Tuttavia, è essenziale identificare le figure che assumeranno temporaneamente le relative responsabilità. Una struttura organizzativa potrebbe essere rappresentata in questo modo (Figura 2.4), considerando le aree e i profili necessari per gestire i servizi principali.

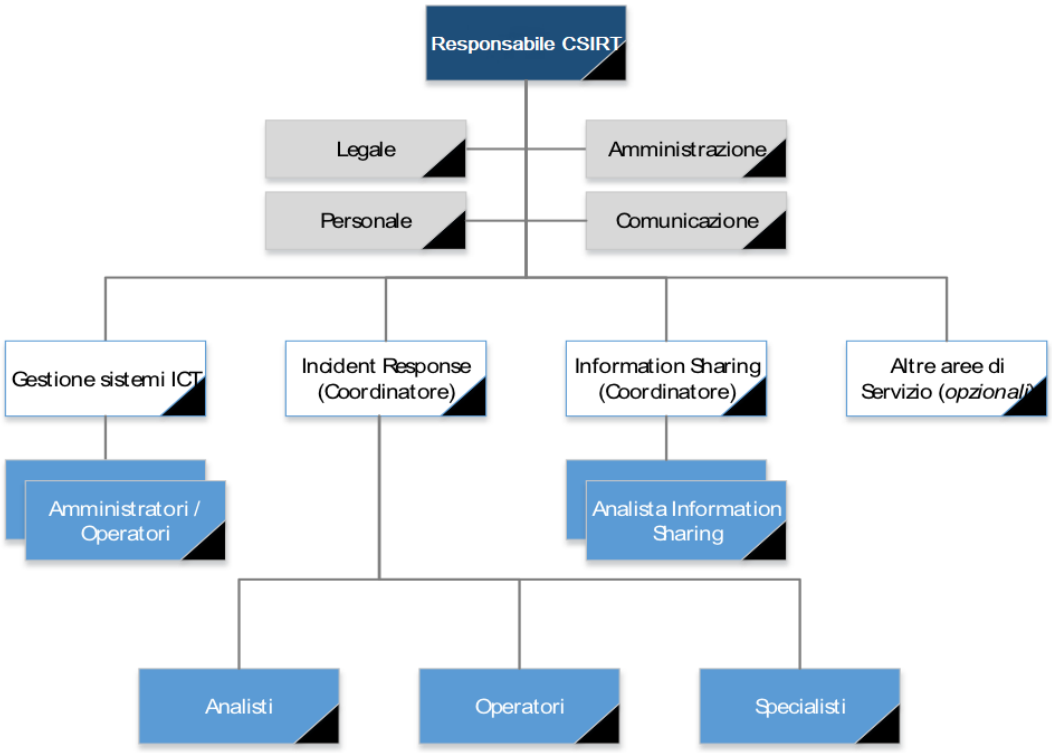

Figura 2.4: Esempio di struttura organizzativa

Si noti che durante la fase di avvio del CSIRT, non tutti i ruoli potrebbero essere pienamente attivati. Alcuni profili possono essere considerati opzionali inizialmente, specialmente in relazione ai servizi aggiuntivi offerti alla constituency.
I ruoli chiave da definire in questo modello di CSIRT, insieme alle principali responsabilità e competenze richieste, sono delineati nei paragrafi seguenti. Per ciascun ruolo, viene proposta una possibile corrispondenza con alcuni dei profili descritti nel modello dell'*European e-Competency Framework* (e-CF) [19].

2.6.1 Management

Il Responsabile CSIRT è una figura chiave all'interno del Management in quanto responsabile dell'identificazione, definizione e progettazione dei servizi del CSIRT

stesso, basandosi sui requisiti della constituency e sulle esigenze di protezione. Il Responsabile CSIRT svolge un ruolo fondamentale nello sviluppo, nell'implementazione e nella manutenzione dei processi, delle politiche e delle procedure del CSIRT, oltre a definire linee guida per il miglioramento continuo del team.
Con riferimento alla figura del *Information Security Manager*, illustrata all'interno del *European e-Competency Framework* [19], possiamo delineare alcune delle responsabilità e delle competenze richieste a chi necessita di ricoprire il ruolo di responsabile di un CSIRT.
`Responsabilità`:

- Identificare, definire e progettare i servizi CSIRT in base ai requisiti della constituency e alle esigenze di protezione.
- Sviluppare, implementare e mantenere processi, politiche e procedure, nonché definire linee guida per il miglioramento continuo del team.
- Allocare le risorse necessarie per garantire il corretto funzionamento del CSIRT.
- Definire il piano di sviluppo e potenziamento per processi, risorse e tecnologie.
- Gestire e organizzare il team del CSIRT, inclusi aspetti come formazione e assegnazione dei ruoli.
- Rappresentare il punto di contatto con la constituency, la comunità di riferimento e le istituzioni per quanto riguarda l'esecuzione dei servizi. Definire e gestire le comunicazioni verso l'esterno e supervisionare i processi di escalation.
- Definire e riesaminare gli indicatori chiave delle prestazioni e della qualità.
- Assicurare la conformità alle politiche e alle procedure del CSIRT.

`Competenze`:

- Comprensione approfondita delle esigenze della constituency.
- Capacità di esercitare una presenza autorevole e di comando, come esperto in materia, durante le situazioni di crisi per gestire le comunicazioni relative agli incidenti di sicurezza.
- Capacità di gestire e allocare le risorse del team, assegnando diverse priorità per ottenere risultati misurabili nel corso del programma.
- Forti capacità decisionali, con la capacità di valutare costi e benefici delle possibili azioni e identificare le azioni più appropriate.
- Forti abilità comunicative nei confronti di diversi tipi di interlocutori.

Inoltre, il Responsabile CSIRT deve designare un delegato all'interno del team che possa sostituirlo e/o agire al suo posto in casi di assenza o indisponibilità temporanea o prolungata.

2.6.2 Operations

Coordinatori (Incident Response / Information Sharing)

Con riferimento alla figura del *Service Manager*, illustrata all'interno del *European e-Competency Framework* [19], questi possono essere definiti come professionisti "con compiti di indirizzo e coordinamento dei team di rispettiva competenza, necessarie a guidare l'efficacia e l'efficienza dei servizi e processi gestiti, dei quali monitorano le prestazioni, valutando e suggerendo raccomandazioni per il miglioramento continuo".

Analista Incident Response

Con riferimento alle figure del *Systems Analyst, Systems Architect, Technical Specialist*, illustrate all'interno del *European e-Competency Framework* [19], possiamo identificare le responsabilità e le competenze richieste a un analista di Incident Response.
`Responsabilità`:

- Analizzare e gestire i ticket relativi agli incidenti di sicurezza e documentare le azioni intraprese.
- Applicare la classificazione degli incidenti in base ai livelli di classificazione previsti dalla metodologia adottata.
- Analizzare e riportare gli incidenti rilevanti al Team Leader, definendo con questi un piano di risposta agli incidenti per gestire tutte le attività richieste.
- Fornire supporto nell'identificazione degli step di ripristino.
- Aggiornare la Knowledge Base con i risultati dell'analisi post-mortem sugli incidenti, al fine di sviluppare/aggiornare le procedure di risposta agli incidenti.
- Fornire i dati di input per il monitoraggio delle prestazioni dei processi di gestione degli incidenti.

`Competenze`:

- Capacità di eseguire analisi sugli allarmi e sulle segnalazioni di incidenti di sicurezza.
- Conoscenza delle tecniche di analisi degli incidenti e di analisi del malware e dei casi di utilizzo.
- Capacità di comprendere e implementare soluzioni per la correzione e risoluzione di vulnerabilità tecniche.
- Conoscenza dei sistemi operativi e delle tecnologie in uso presso la constituency di riferimento.

In funzione del livello di specializzazione richiesta e dei servizi attivati, l'analista potrebbe presentare livelli di seniority differente e/o ambiti di competenza specifici. Ad esempio, potrebbero essere reclutati analisti dei malware con competenze specifiche sull'analisi del codice eseguibile, sia in modalità statica che dinamica, così come analisti forensi, dedicati a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni, documentando il tutto in modo che sia correttamente presentabile in sede processuale [20].

Operatore Incident Response

Con riferimento alla figura del *Technical Specialist*, illustrata all'interno del *European e-Competency Framework* [19], si possono individuare le seguenti responsabilità e competenze richieste a tale figura.
`Responsabilità`:

- Monitorare i dispositivi e l'infrastruttura in tempo reale, analizzando i log degli eventi e tutti gli altri input ricevuti.
- Rappresentare il punto di contatto verso gli utenti.
- Aprire ticket per tutte le segnalazioni interne ed esterne, richieste di lavoro e di informazioni.
- Eseguire una prima analisi dell'incidente ed effettuare il triage.
- Definire la strategia di risposta iniziale agli incidenti.
- Gestire l'escalation verso le altre entità coinvolte secondo le procedure stabilite.
- Fornire i dati di input per il monitoraggio delle prestazioni dei processi di gestione degli incidenti.

`Competenze`:

- Capacità di comprendere e riconoscere vulnerabilità tecniche.
- Conoscenza e capacità di utilizzo e amministrazione di strumenti di trouble ticketing.
- Conoscenza dei sistemi operativi e delle tecnologie in uso presso la constituency di riferimento.

Specialista Incident Response

Con riferimento alla figura del *Service Support*, illustrata all'interno del *European e-Competency Framework* [19], essi "detengono una ampia conoscenza delle tecnologie che degli strumenti utilizzati per esaminare la sicurezza di sistemi e reti e competenze

estese all'ingegneria e sviluppo del software, alla programmazione e ai linguaggi di scripting".

`Responsabilità`:

- Gestire e monitorare eventi di sicurezza e il comportamento dei prodotti di sicurezza.
- Fornire supporto nell'aggiornamento della Knowledge Base.
- Monitorare e misurare le metriche associate ai controlli di sicurezza.
- Lavorare a stretto contatto con altri analisti per identificare e affrontare le minacce in modo tempestivo.
- Gestire e risolvere i problemi operativi che coinvolgono i controlli di sicurezza.

`Competenze`:

- Capacità di eseguire analisi sugli allarmi e sulle segnalazioni di incidenti di sicurezza.
- Conoscenza dei sistemi operativi e delle tecnologie in uso presso la constituency di riferimento.
- Capacità di analizzare i flussi di pacchetti per identificare le anomalie.
- Esperienza nell'implementazione e nell'aggiornamento dei controlli di sicurezza e delle best practices.

Analista Information Sharing

Con riferimento alla figura del *Information Security Specialist*, illustrata all'interno del *European e-Competency Framework* [19], si possono individuare le seguenti responsabilità e competenze richieste a tale figura.

`Responsabilità`:

- Supportare il Team Leader nella definizione della strategia di comunicazione in caso di minacce e/o attacchi in corso.
- Selezionare i contenuti da diffondere all'esterno in base ai livelli di confidenzialità delle informazioni.
- Identificare e gestire i canali per la diffusione e la comunicazione delle informazioni verso l'esterno.

`Competenze`:

- Conoscenza delle tecniche di comunicazione e gestione dei rapporti con i media.
- Esperienza nella redazione e pubblicazione di contenuti tematici.
- Conoscenza delle caratteristiche e dei servizi offerti dal CSIRT.

2.6.3 Personale di Supporto

L'operatività del CSIRT dipende anche dalla presenza e dalle attività condotte da personale di supporto ai processi operativi, quali:

- personale dell'area Information Technology[2], che ha la responsabilità di implementare, gestire e mantenere aggiornati i sistemi e le infrastrutture informatiche in dotazione al CSIRT – sia di funzionamento che a supporto dell'erogazione dei servizi alla constituency;
- personale dell'area Amministrazione e Finanza, con responsabilità di gestire le risorse contabili al fine di garantire un adeguato controllo amministrativo, fiscale e finanziario dell'organizzazione, oltre a consentire la gestione del personale sotto il profilo amministrativo;
- personale dell'area Comunicazione, con il compito di supportare il management nella gestione delle comunicazioni con gli stakeholder del CSIRT e di mantenere costantemente aggiornati i contatti all'interno e all'esterno dell'organizzazione, ad esempio attraverso la preparazione e distribuzione di news e bollettini e la gestione dei canali di comunicazione attivati dal CSIRT;
- personale dell'area Legale, che fornisce un supporto specialistico in materia normative e in merito alla possibilità di divulgare le informazioni in accordo con le policy del CSIRT, le leggi e i regolamenti applicabili.

Pur riconoscendo la centralità delle attività di formazione del personale interno, la velocità di cambiamento degli scenari di rischio potrebbe richiedere talvolta l'intervento di figure esterne specializzate, in grado di fornire supporto mirato, nonché le linee guida per l'internalizzazione di competenze specifiche sulla base dei progetti svolti in collaborazione con figure consulenziali esterne.
È difficile fornire requisiti ragionevoli per un dimensionamento iniziale di un CSIRT regionale, poiché vari fattori influenzano il numero di risorse necessarie. Prendendo in considerazione le esperienze di CSIRT di tipo nazionale/governativo [21, 22, 23], un dimensionamento adeguato da cui partire è compreso tra 3 e 5 *Full-Time Equivalent*[3] (FTE), quando i servizi sono forniti solo durante l'orario d'ufficio, fino ad arrivare a 6-8 FTE nel caso di realtà amministrative più complesse.
Al fine di fornire livelli di servizio sostenibili, indipendentemente dalla posizione per cui sono stati assunti, le risorse dovrebbero detenere un'ampia gamma di competenze per poter ricoprire più ruoli in una fase di avvio dei servizi. L'ipotesi di operatività 24/7/365 nell'ambito della constituency dovrà essere valutata in ragione del portafoglio di servizi, della struttura e delle responsabilità del team, considerando anche

[2] Le competenze richieste a tali figure possono essere individuate nei seguenti profili proposti dall'e-CF: ICT Operations Manager; Network Specialist, Systems Administrator; Data Administrator.
[3] Rappresenta l'unità di misura che indica la quantità di lavoro a tempo pieno impiegata in un'organizzazione o azienda.

opzioni di reperibilità da remoto, al fine di garantire comunque tempi di risposta rapidi, specialmente per i rapporti sugli incidenti.

2.7 Modello dati e informazioni

Un CSIRT gestisce dati che seguono un ciclo di vita composto da cinque fasi:

1. **Raccolta**: durante questa fase, il CSIRT acquisisce informazioni e dati relative a violazioni e minacce informatiche provenienti da varie fonti.

2. **Conservazione**: le informazioni raccolte sono archiviate in un'apposita banca dati amministrata dal CSIRT. Questo database registra sia le violazioni riscontrate che le minacce previste, basandosi sulle segnalazioni degli utenti.

3. **Utilizzo**: il CSIRT utilizza queste informazioni per valutare minacce e violazioni ed eseguire azioni preventive o reattive per mitigare tali situazioni. Questa fase è fondamentale per garantire una risposta efficace alle minacce.

4. **Diffusione**:le informazioni raccolte e analizzate dal CSIRT possono essere condivise con i membri della constituency al fine di diffondere la conoscenza sulle minacce informatiche e le violazioni. Tuttavia, potrebbero essere applicate regole di confidenzialità che limitano la divulgazione di informazioni sensibili.

5. **Distruzione**: con il passare degli anni, i dati obsoleti o non più rilevanti devono essere eliminati in modo sicuro per evitare utilizzi impropri.

L'obiettivo principale della creazione di un CSIRT è consentire ai membri della constituency di rispondere in modo efficace alle minacce informatiche, sia in termini preventivi che reattivi. Poiché le informazioni fornite dai segnalanti spesso contengono dati sensibili e riservati, è fondamentale rispettare rigorose regole di confidenzialità. Si potrebbe considerare un diverso grado di trasparenza nell'ambito dei flussi informativi. Le informazioni fornite dai segnalanti al CSIRT potrebbero essere condivise in modo completo, consentendo a quest'ultimo di eseguire valutazioni accurate. Diversamente, quando le informazioni vengono diffuse dalla banca dati del CSIRT alla constituency, le informazioni identificative del segnalante potrebbero essere oscurate per proteggere la sua riservatezza.
In generale, le regole di confidenzialità imporrebbero il divieto di divulgare le informazioni del CSIRT a terzi non autorizzati, di utilizzare queste informazioni per scopi diversi da quelli previsti e di garantire una custodia sicura delle informazioni per prevenirne l'accesso non autorizzato.
In linea di principio, i flussi informativi del servizio CSIRT dovrebbero riguardare principalmente organizzazioni e altre entità, senza includere dati personali o informazioni che potrebbero identificare direttamente o indirettamente individui. In questo modo, si preserva la riservatezza e la sicurezza delle informazioni gestite dal CSIRT.

2.7.1 Tipologie di dati trattati

I *dati in movimento* fanno riferimento a tutti i dati che viaggiano da un punto all'altro attraverso una rete. Questi dati sono suscettibili di vulnerabilità, rendendo la loro protezione cruciale. D'altro canto, i *dati statici* sono dati conservati su dispositivi o archiviati. Sebbene si tenda a ritenere i dati statici meno vulnerabili, gli attaccanti spesso concentrano i loro sforzi su di essi. Il livello di rischio associato ai dati, sia in movimento che statici, dipende dalle misure di sicurezza adottate per proteggerli. Proteggere questi dati è imperativo poiché gli attacchi che mirano a rubare o compromettere dati sensibili stanno diventando sempre più sofisticati.
La cifratura svolge un ruolo fondamentale nella protezione dei dati, indipendentemente dal fatto che siano in movimento o statici. Per i dati in movimento, la cifratura viene applicata prima della trasmissione per proteggerli. Per i dati statici, vengono cifrati prima dell'archiviazione o, in alternativa, si può cifrare il dispositivo di archiviazione stesso.
Oltre alla cifratura, le best practices per la protezione dei dati includono:

- **Controlli di sicurezza di rete robusti**: Firewall e sistemi di controllo degli accessi rendono la rete più sicura proteggendola da intrusioni e attacchi.
- **Sicurezza proattiva**: Non ci si dovrebbe basare esclusivamente su misure di sicurezza reattiva. La sicurezza proattiva identifica in modo preventivo i dati potenzialmente a rischio e mette in atto un sistema di sicurezza adeguato.
- **Soluzioni di protezione dati avanzate**: Utilizzare soluzioni che consentono agli utenti di richiedere, bloccare o cifrare automaticamente i dati sensibili in movimento, ad esempio, quando vengono inviati via e-mail o spostati su cloud.
- **Classificazione dei dati**: Categorizzare e classificare in modo sistematico tutti i dati dell'organizzazione, indipendentemente dalla loro posizione, per garantire protezione continua.

Sebbene i dati in movimento e i dati statici possano presentare profili di rischio diversi, il rischio intrinseco è principalmente legato alla sensibilità e al valore stesso dei dati. Gli attaccanti cercheranno di accedere a informazioni sensibili, sia in movimento che statici, in base a quale sia più vulnerabile. Pertanto, un approccio proattivo che includa la categorizzazione e la classificazione dei dati sensibili rappresenta il metodo più efficace per proteggere entrambe le categorie di dati.
Oltre alla distinzione tra dati in movimento e dati statici, un CERT può trattare diverse tipologie di dati, ciascuna con contenuti, fonti e destinazioni differenti. Queste categorie comprendono:

- **Dati di Accreditamento dei Membri della Constituency**: dati riguardanti i membri della constituency e raccolti durante il processo di accreditamento. Essi possono includere informazioni sull'organizzazione e, in alcuni casi, dati personali.

- **Dati delle Segnalazioni di Incidenti**: sono dati trasmessi dai membri della constituency e includono informazioni relative agli incidenti, come registri, file, asset, indirizzi IP, timestamp e altro ancora.
- **Dati di Threat Intelligence**: dati raccolti attraverso il processo di threat intelligence, che può essere gestito internamente o esternalizzato. Questi dati possono essere in vari formati, come STIX, TAXII, JSON, e possono includere informazioni su minacce specifiche, come domini, indirizzi IP, URL, hash di file e stringhe, che contribuiscono all'identificazione delle minacce.
- **Dati sulle Vulnerabilità**: dati riguardanti nuove vulnerabilità e provengono da altri CERT/CSIRT e da *vendors*.
- **Dati sulle Minacce Emergenti**: dati che riguardano minacce emergenti e provengono da entità di livello superiore.

Il modello dati di un CSIRT è fortemente influenzato dai servizi offerti e dalle interazioni con altre parti. La gestione di queste diverse tipologie di dati richiede una pianificazione e misure di sicurezza adeguate per garantire la riservatezza, l'integrità e la disponibilità delle informazioni, nonché il rispetto delle normative sulla privacy e della legislazione applicabile.
In funzione dei servizi attivati e delle parti con cui un CSIRT interagisce, è possibile definire un modello dati come quello rappresentato nella figura sottostante (Figura 2.5).

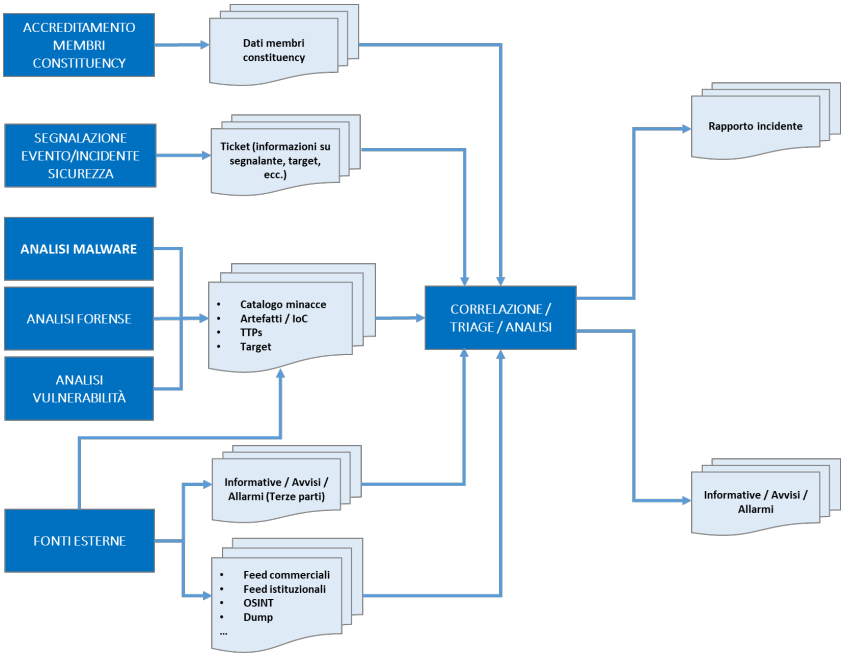

Figura 2.5: Modello dati di un CSIRT

Nell'ambito della gestione delle informazioni, è fondamentale classificare i dati in base al loro livello di riservatezza. La classificazione determina chi ha il permesso di

accedere e modificare le informazioni e stabilisce le misure di protezione necessarie, sia fisiche che logiche, dall'origine dei dati fino alla loro distruzione o declassificazione. Nel contesto civile, solitamente, le informazioni vengono classificate in tre livelli principali: *informazione pubblica*, *informazione a uso interno dell'organizzazione* e *informazione a uso ristretto*. Altri livelli possono basarsi sulla normativa Privacy, ad esempio, la normativa italiana distingue tra dati personali, personali sensibili e personali giudiziari, per i quali sono da applicare diverse misure di sicurezza.
La classificazione delle informazioni è cruciale per garantire la sicurezza e il rispetto delle normative sulla privacy. Determina come le informazioni devono essere gestite e chi può accedervi, contribuendo a proteggere la riservatezza e l'integrità dei dati sensibili.

2.8 Modelli tecnologici e applicativi

Per garantire che il CSIRT possa svolgere le sue funzioni in modo efficace, è fondamentale individuare e implementare le tecnologie necessarie che supportino le attività di analisi e risposta agli incidenti, nonché la comunicazione con tutte le parti coinvolte.
Un requisito essenziale è la creazione di un ambiente completamente isolato e autonomo rispetto alle altre infrastrutture ICT esistenti. In altre parole, il CSIRT deve operare su sistemi, applicazioni e reti indipendenti e separati dalle infrastrutture IT preesistenti.
Per fornire un quadro più completo degli argomenti trattati in seguito e per un ulteriore approfondimento, si consiglia di far riferimento alle schede di approfondimento relative alle tecnologie open source attualmente adottate dai principali CERT/CSIRT a livello internazionale.

2.8.1 Infrastruttura di rete

L'infrastruttura di rete del CSIRT deve essere progettata attentamente per garantire sia la fornitura dei servizi richiesti che la sicurezza dei dati e delle informazioni trattate. Questo richiede un'infrastruttura di rete che soddisfi i requisiti operativi, di protezione e di continuità dei servizi offerti alla constituency. Inoltre, è importante identificare gli strumenti di comunicazione e le piattaforme applicative necessarie.
Dal punto di vista logico, è consigliabile utilizzare uno o più firewall per segmentare la rete in diverse aree indipendenti (VLAN) in base ai servizi che offrono. Eccone una possibile configurazione:

- segmento di rete (DMZ esterna) utilizzato esclusivamente per ospitare i servizi pubblici (web, mail, portale, ecc.) esposti su Internet. Questi possono essere mirati per la propria constituency o comprendere altre attività (es. bollettini, linee guida) volte a una diffusione più ampia.

- la rete interna (CSIRT LAN), dedicata allo svolgimento delle attività di amministrazione e gestione e di operatività del CSIRT. In questo caso è auspicabile definire un'ulteriore segregazione tra la LAN destinata a ospitare le postazioni e le dotazioni assegnate al personale del CSIRT e un segmento di DMZ interna per ospitare i file server, i sistemi di ticketing e i server a supporto degli strumenti per l'erogazione dei servizi alla constituency. In questo modo è possibile definire un'area sicura per la conservazione, l'accesso e il trasferimento di dati da e verso il CSIRT, nonché per una gestione interna allo stesso, secondo il principio di *need-to-know*[4]. Le informazioni legate a incidenti rilevati all'interno della propria constituency dovrebbero infatti essere mantenute con la massima riservatezza su server (fisici/virtuali) dedicati, non raggiungibili dall'esterno.

- segmento di rete dedicato a un'area di test (laboratorio), essenziale nel caso in cui il CSIRT eroghi servizi di analisi degli artefatti o di investigazione forense. Tale area non solo deve permettere la gestione in sicurezza di artefatti malevoli, ma comprendere un'architettura (fisica/logica) isolata (sandbox), che può includere macchine virtuali e device dedicati, dove riprodurre, in ambiente controllato, situazioni di compromissione di sistemi per analizzarne il comportamento e valutare possibili contromisure. La segregazione di tale rete è essenziale per la protezione dei dati custoditi dal CSIRT e per preservare l'operatività e l'integrità di tutti i servizi offerti. L'ambiente di test, infine, deve poter essere ripulito e ripristinato rapidamente dopo un'investigazione.

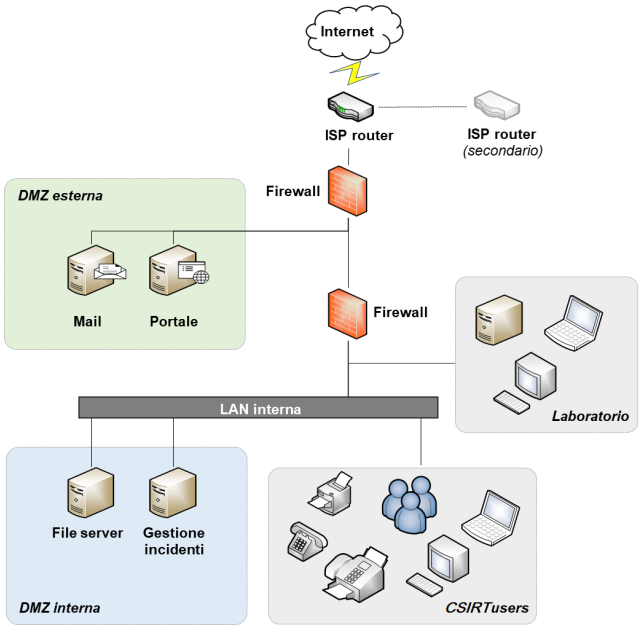

Figura 2.6: Infrastruttura di rete

[4] Definizione di regole e policy di sicurezza che specificano chi ha diritto di accesso a quali informazioni e sotto quali circostanze.

Il CSIRT deve essere connesso a Internet per erogare i suoi servizi pubblici, e questa connessione dovrebbe coinvolgere due ISP (Internet Service Provider) diversi per garantire la continuità operativa in caso di guasto sulla linea principale. Inoltre, una connessione telefonica dedicata, fissa o mobile, consente di mantenere il CSIRT raggiungibile tramite chiamate o fax, garantendo comunicazioni in situazioni di emergenza.
I server utilizzati dal CSIRT per i servizi interni ed esterni possono essere fisicamente separati o virtualizzati in un cluster unico per ottimizzare l'uso delle risorse e migliorare la resilienza. L'immagine seguente (Figura 2.6) mostra una possibile configurazione dell'architettura di rete descritta in precedenza.

2.8.2 Strumenti

I servizi erogati dal CERT verso la propria constituency dovranno essere supportati da strumenti specializzati per area di servizio, che possono tuttavia essere impiegati anche per più aree funzionali:

Strumenti di correlazione (crawling/mining/correlation), ovvero tecnologie che abilitano attività di threat intelligence in termini di raccolta, ricerca e analisi dei dati su minacce, violazioni, ecc, costituendo di fatto un input per il processo di Incident Response. In particolare, favoriscono la conduzione di analisi su specifiche minacce e dunque l'individuazione di linee guida e indicazioni per le successive attività investigative e rendendo possibile la condivisione con gli altri soggetti coinvolti per le azioni di prevenzione e monitoraggio.

Piattaforme per l'information sharing ovvero tecnologie che consentono la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di compromissione e minacce relative all'analisi degli incidenti di sicurezza informatica e all'analisi di malware. Attraverso l'utilizzo di tali piattaforme è possibile condividere informazioni in forma strutturata all'interno della propria comunità o anche all'esterno, favorendo l'adozione di approcci comuni per la risoluzione degli incidenti. Questo processo permette infatti agli stakeholder lo scambio di informazioni delicate e privilegiate mantenendo la confidenzialità e la fiducia nella comunicazione e mantenendo la sicurezza delle informazioni.monitoraggio.

Strumenti per l'analisi malware volti all'esecuzione di analisi statica e dinamica di codice eseguibile

Strumenti per l'investigazione e l'analisi forense strumenti volti all'acquisizione e analisi di tutti i dati necessari che riguardano un attacco subito da sistemi informatici.

Strumenti di comunicazione sicura per coordinare e consentire lo scambio di informazioni con la constituency e la comunità di riferimento sulla base dei livelli

di protezione e sicurezza richiesti (es. meccanismi di autenticazione, cifratura delle comunicazioni). L'utilizzo di cifratura a chiave pubblica (es. PGP, GPG), di certificati digitali (X.509) e di protocolli di comunicazione sicura (es. HTTPS), risulta indispensabile per mitigare il rischio di attacchi di tipo *man-in-the-middle* e *spoofing* e per garantire adeguati livelli di sicurezza (es. comunicazioni autenticate/cifrate) sui canali di scambio.

Knowledge Base ovvero un ambiente volto a facilitare la raccolta, l'organizzazione e la distribuzione della conoscenza sulle modalità di analisi e risoluzione degli incidenti con l'obiettivo di favorire la definizione di modus operandi standardizzati.

Strumenti di ticketing ovvero tecnologie per favorire l'automazione dei workflow autorizzativi e la tracciatura delle attività effettuate per l'analisi e la risoluzione degli incidenti. In particolare, consentono di gestire il processo di risoluzione dell'incidente in maniera automatizzata, dalla registrazione della segnalazione fino alla soluzione. In questo modo, è possibile avere una visione completa del processo seguito, visualizzando l'avanzamento della soluzione passo dopo passo e con la possibilità di allegare, e utilizzare successivamente, ampia documentazione correlata all'evento.

Strumenti per la conduzione di simulazioni/formazione che comprendono le piattaforme applicative di *e-learning* (Learning Management System) che permettono l'erogazione dei corsi online e quelle destinate alla progettazione di scenari simulati per la conduzione di esercitazioni pratiche su vari argomenti di cybersecurity, anche in stile «*Capture the Flag*" e impiegando sistemi reali e interattivi da attaccare.

2.9 Facilities

Infine, le facilities sono un sottoinsieme del patrimonio fisico dell'organizzazione che viene utilizzato per eseguire i servizi. Sono centri di attività in cui si intersecano molti servizi dell'organizzazione, come edifici per uffici e locali tecnici. Possono essere di proprietà dell'organizzazione ma spesso vengono noleggiate da un fornitore esterno. Le persone, le informazioni e le risorse tecnologiche «*vivono*» all'interno delle facilities: forniscono lo spazio fisico per le azioni delle persone (le persone lavorano negli uffici), l'uso e la memorizzazione delle informazioni (file, server) e l'operazione di componenti tecnologici (come nei data center e nelle server farm). Proprio per tale ragione è cruciale l'adozione di requisiti di sicurezza fisica e ambientale idonei a consentire la protezione delle informazioni.

2.10 Sicurezza fisica

La gestione della sicurezza fisica è fondamentale per garantire la protezione delle aree, dei sistemi e delle informazioni gestite da un CSIRT. Questa gestione richiede l'identificazione e l'implementazione di adeguate misure di sicurezza per preservare la riservatezza e l'integrità delle informazioni.
Alcuni punti rilevanti da considerare includono la creazione di spazi dedicati per le diverse funzioni all'interno del CSIRT, l'istituzione di aree sicure per i server e i dati, l'utilizzo di casseforti o armadi blindati per proteggere informazioni fisiche e non elettroniche, nonché la creazione di comunicazioni interne ed esterne sicure e crittografate tramite telefono, fax, email e schemi crittografici. Queste misure sono essenziali per prevenire l'accesso non autorizzato, danni o interferenze. Inoltre, la sicurezza delle aree fisiche deve essere progettata per impedire l'accesso non autorizzato, danni alle informazioni e interruzioni nei servizi e nei processi informatici.
È importante sottolineare che alcune misure minime di sicurezza fisica sono necessarie per ottenere l'accreditamento e l'affiliazione da parte di organizzazioni e associazioni autorevoli come ENISA, Carnegie Mellon, FIRST e Trusted Introducer.
In particolare sono di seguito riportate alcune delle misure minime da implementare, ovvero:

- Stabilire un luogo specifico per ogni locale del CSIRT, con in aggiunta una struttura protetta per le riunioni (*war room*).
- Assicurare la chiusura delle porte di accesso ai locali del CSIRT.
- Rafforzare i controlli fisici di accesso (badge, chiavi) al fine di impedire accessi non autorizzati alle strutture del CSIRT.
- Rendere disponibile in ogni locale del CSIRT un deposito sicuro (armadio chiuso a chiave, cassaforte) per archiviare la documentazione riservata e il disco di backup.
- Dotare i locali di distruggi documenti.
- Adottare, in conformità con i termini di legge, sistemi di videosorveglianza per proteggere i perimetri esterni e registrare gli accessi alle aree riservate.
- Attivare all'interno dei locali sistemi di allarme con sensori di movimento quando personale del CSIRT o altro personale autorizzato (vigilanza, servizi di pulizia, ecc.) non sono presenti.
- Adottare le dovute contromisure per proteggere le conversazioni telefoniche confidenziali, per non renderle accessibili a terzi non autorizzati.

Alcune misure aggiuntive, sebbene altamente consigliate per elevare il livello di sicurezza, possono essere considerate opzionali a causa della loro complessità e dei

costi associati.
Un'ulteriore area di sicurezza fisica riguarda le apparecchiature, che includono misure atte a proteggere le risorse ICT e i supporti da danni accidentali o intenzionali, nonché la sicurezza ambientale, particolarmente rilevante quando il CERT ha il controllo esclusivo del data center e delle attrezzature informatiche. Alcuni fattori da considerare in questo contesto includono:

Posizionamento delle apparecchiature : Le apparecchiature devono essere collocate su pavimenti rialzati, a una distanza sicura dalle tubature che potrebbero causare danni da liquidi. Inoltre, i server e le attrezzature di rete dovrebbero essere sistemati in appositi armadi rack per una maggiore protezione.

Sistemi di climatizzazione : È essenziale implementare un sistema di controllo delle temperature ambientali e dell'umidità, specialmente nelle aree che ospitano i server, per garantire le condizioni ambientali ottimali.

Sistemi di rilevamento degli allarmi ambientali : Questi includono sistemi di rilevamento fumo e antincendio, con attivazione di dispositivi di spegnimento degli incendi in conformità alle normative di settore. Inoltre, è consigliabile utilizzare sistemi di allarme contro gli allagamenti situati sotto il pavimento rialzato.

Impianti di alimentazione elettrica : È cruciale garantire un'alimentazione elettrica affidabile per le apparecchiature e i sistemi. Questo può essere ottenuto attraverso linee di alimentazione separate, l'uso di *UPS* (Uninterruptible Power Supply) e batterie di backup per protezione contro blackout brevi o interruzioni di corrente e generatori di emergenza per protezione in caso di blackout prolungati, a condizione che sia garantito un rifornimento di carburante adeguato. UPS, batterie e generatori devono essere dimensionati per sostenere tutte le apparecchiature collegate durante interruzioni di corrente.

Cablaggi : I cavi di alimentazione e di telecomunicazione dovrebbero essere collocati in canaline sottopavimento o canalette aeree per evitare danni accidentali. È fondamentale separare chiaramente i cavi di alimentazione da quelli di telecomunicazione per evitare interferenze. Inoltre, è consigliabile etichettare chiaramente l'inizio e la fine di ciascuna canalina per agevolarne il riconoscimento. Se possibile, è opportuno proteggere le canaline che attraversano ambienti esterni per prevenire danneggiamenti accidentali o vandalismo durante lavori di costruzione o scavi.

Queste misure supplementari possono migliorare la sicurezza fisica delle apparecchiature e degli ambienti del CSIRT, anche se possono essere considerate opzionali a causa della loro complessità e dei costi associati.

2.10.1 Archivi fisici

Gli archivi fisici possono servire alla conservazione di documenti in formati non digitali, come carta e fotografie, ma anche di supporti digitali come hard disk, nastri, CD, DVD, e così via. Per garantire la sicurezza e il controllo dell'accesso a tali archivi fisici, sono necessarie specifiche autorizzazioni e metodi di controllo degli accessi. Questi metodi possono includere chiavi tradizionali o combinazioni, oppure approcci personali basati su tessere magnetiche, smart card o caratteristiche biometriche. Inoltre, è essenziale monitorare costantemente la temperatura e l'umidità degli archivi per evitare danni ai documenti o ai supporti.
All'interno degli uffici e delle aree sensibili, è fondamentale mantenere tutti i documenti archiviati in un apposito spazio archivio, limitando sulla scrivania la presenza solo dei documenti strettamente necessari. Questa pratica, nota come *clear desk policy*, è finalizzata a impedire a persone non autorizzate di accedere o leggere documenti sensibili che potrebbero essere lasciati incustoditi sulle scrivanie.

2.11 Sicurezza logica

Mentre la sicurezza fisica fornisce un primo livello di protezione per i dati, la sicurezza logica costituisce un elemento essenziale per difendere i sistemi e le reti informatiche. Date la natura delle informazioni trattate da un CSIRT e la possibilità di vulnerabilità e incidenti, è fondamentale implementare controlli di sicurezza logica. Questi controlli mirano a preservare la riservatezza e l'integrità delle informazioni.
Nel contesto nazionale italiano, un punto di partenza adeguato è costituito dalle "Misure minime di Sicurezza ICT per la PA" [24]. Queste misure rappresentano un insieme di controlli mirati a fornire un livello base di sicurezza per tutte le organizzazioni che devono affrontare minacce di tipo cibernetico.
I suddetti controlli possono essere raccolti nei seguenti ambiti di sicurezza:

Inventario dispositivi e software : individuare i sistemi (hardware, software), i servizi e le risorse che gestiscono i dati informatici trattati da proteggere.

Governance : identificare e rispettare le leggi e/o i regolamenti con rilevanza in tema di cybersecurity applicabili al contesto.

Protezione da malware : i dispositivi in perimetro quando possibile devono utilizzare software di protezione, ad esempio antivirus/anti-malware, regolarmente aggiornato.

Gestione password e account : assicurare una complessità adeguata delle password e gestire le utenze secondo i principi di *need to know* e least privilege.

Formazione e consapevolezza : sensibilizzare il personale sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali.

Protezione dei dati : i sistemi devono essere configurati tramite procedure di hardening e backup periodici devono essere effettuati.

Protezione delle reti : le reti e i sistemi devono essere protetti da accessi non autorizzati attraverso componenti hardware/software.

Prevenzione e mitigazione : i software utilizzati vanno mantenuti aggiornati o dismessi in caso risultino obsoleti e non più aggiornabili. Nel caso di un incidente informatico devono essere informati i responsabili di sicurezza che seguiranno il processo di gestione degli incidenti interno.

Capitolo 3

Strumenti per la simulazione di efficienza di un CSIRT

CyberBattleSim è una piattaforma di ricerca sperimentale progettata per condurre esperimenti e simulazioni nel campo della sicurezza informatica e della cibernetica volti a studiare l'interazione di agenti automatizzati che operano in un ambiente di rete aziendale astratto simulato. È stata sviluppata per scopi di ricerca e formazione e fornisce agli esperti di sicurezza informatica e agli studenti un ambiente sicuro per testare e valutare strategie di difesa e attacco in un contesto simulato. Le caratteristiche di CyberBattleSim includono la simulazione di reti informatiche, nodi e agenti malevoli, consentendo agli utenti di eseguire scenari di attacco e difesa per valutare la resilienza delle infrastrutture informatiche e sviluppare strategie di mitigazione delle minacce. L'ambiente di simulazione supporta anche la personalizzazione e l'estensione il che lo rende un'utile risorsa per la ricerca accademica e industriale nel campo della sicurezza cibernetica. È possibile utilizzare CyberBattleSim per eseguire esperimenti di sicurezza informatica, addestrare personale alla sicurezza cibernetica e sviluppare nuove tecniche di difesa cibernetica. CyberBattleSim utilizza un modello parametrizzabile di alto livello di reti aziendali che simula l'esecuzione di attacchi e difese da parte di cyber-agent. Una topologia di rete fissa e una serie di vulnerabilità predefinite definiscono l'arena in cui si effettua la simulazione. L'obiettivo dell'aggressore è appropriarsi di una porzione della rete evolvendosi nella rete tramite movimenti laterali sfruttando le vulnerabilità presenti nei nodi del computer. Mentre l'aggressore tenta di diffondersi nella rete, un agente difensore osserva l'attività della rete e cerca di rilevare eventuali attacchi in atto e mitigare l'impatto sul sistema tentando di contenere l'aggressore e di rimuoverlo dalla rete.
Il simulatore fornisce un difensore stocastico di base che rileva e attenua gli attacchi in corso basati su probabilità predefinite di successo. La mitigazione è implementata semplicemente reimpostando le macchine infette, un processo modellato astrattamente come un'operazione che si estende su più passi di simulazione.
Per poter confrontare le prestazioni degli agenti, vengono fornite due metriche da analizzare: il numero di passi di simulazione necessari per raggiungere l'obiettivo (del difendente) e le ricompense cumulative nel corso dei passi di simulazione durante le fasi di addestramento. Il termine si riferisce al numero di volte che un algoritmo

di apprendimento automatico esamina l'intero set di dati di addestramento durante il processo di apprendimento, al fine di regolare i pesi e i parametri del modello per migliorare le prestazioni.
CyberBattleSim offre anche un'interfaccia OpenAI Gym per le sue simulazioni in modo da facilitare la sperimentazione con algoritmi di Reinforcement Learning.

3.1 Motivazioni sull'utilizzo di un ambiente di simulazione

Gli ambienti runtime di emulazione forniscono alta fedeltà e controllo: è possibile prendere codice o file binari esistenti ed eseguirli direttamente in macchine virtuali che eseguono sistemi operativi completi e connesse su una rete virtualizzata, dando accesso allo stato completo del sistema. Ciò, tuttavia, ha un costo in termini di prestazioni. Sebbene gli ambienti simulati soffrano di mancanza di realismo, tendono a essere leggeri, veloci, astratti e più controllabili il che li rende più suscettibili alle sperimentazioni con Reinforcement Learning.
La natura altamente astratta del simulatore ne impedisce l'applicazione diretta ai sistemi del mondo reale, garantendo così una salvaguardia contro il potenziale uso pericoloso di agenti automatizzati addestrati con esso. Allo stesso tempo, la sua semplicità consente di concentrarci su aspetti di sicurezza specifici che intendiamo studiare e sperimentare rapidamente con i recenti algoritmi di Machine Learning e intelligenza artificiale. I vantaggi della simulazione includono:

- Astrazione di livello superiore: possiamo modellare aspetti del sistema che contano per noi, come la comunicazione di rete a livello di applicazione rispetto alla simulazione di rete a livello di pacchetto. Possiamo ignorare i dettagli di basso livello se ritenuti non necessari (ad esempio, file system, registro).

- Flessibilità: la definizione di nuovi sensori della macchina è semplice (ad esempio, non richiede modifiche di basso livello/codice driver); possiamo restringere lo spazio d'azione a un sottoinsieme gestibile e rilevante.

- Acquisizione dello stato globale in modo efficiente semplificando il debug e la diagnosi.

- Ingombro a runtime leggero: esecuzione in memoria su una singola macchina/-processo.

Un principio di progettazione adottato prevede che la simulazione modelli la complessità appena sufficiente per rappresentare le tecniche di attacco dalla matrice MITRE pur mantenendo la semplicità richiesta per addestrare in modo efficiente un agente utilizzando tecniche di Reinforcement Learning. Dal lato dell'attacco, l'attuale simulazione si concentra più in particolare sulla tecnica del movimento laterale che è intrinseca a tutti gli attacchi post-violazione.

3.2 Funzionamento della simulazione

Vediamolo attraverso un esempio e introduciamo il funzionamento della simulazione utilizzando il linguaggio del Reinforcement Learning (Apprendimento per Rinforzo). Il nostro ambiente di rete è rappresentato da un grafo diretto annotato, in cui i nodi rappresentano computer e gli archi rappresentano la conoscenza degli altri nodi o la comunicazione che avviene tra i nodi.

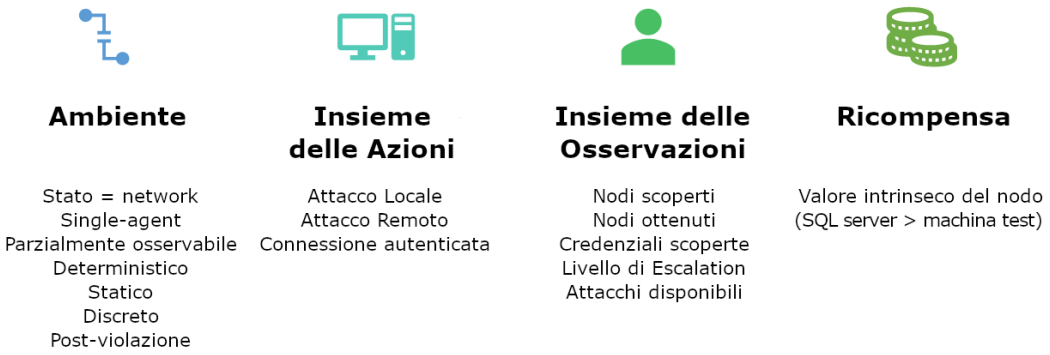

Figura 3.1: Agenti della simulazione

In figura 3.2 è possibile vedere un esempio di rete simulata con computer che eseguono sistemi operativi e software diversi. Ogni computer ha delle proprietà, un valore, ed è vulnerabile a predefinite vulnerabilità. Gli archi blu del grafo rappresentano il traffico che si verifica tra i nodi e sono etichettati con il protocollo di comunicazione.

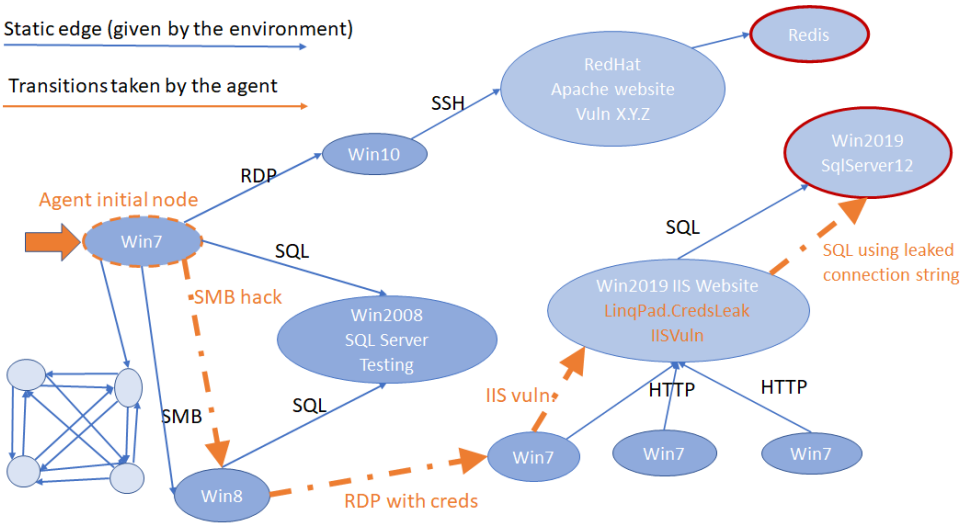

Figura 3.2: Funzionamento della simulazione

C'è un unico agente: definito come attaccante e inizialmente, un nodo è posto come infetto (ipotesi dopo una violazione). L'obiettivo dell'attaccante è massimizzare la ricompensa scoprendo e 'possedendo' i nodi nella rete. L'ambiente è parzialmente osservabile: l'agente non può vedere in anticipo tutti i nodi e gli archi del grafo di rete. Pertanto, l'attaccante esegue azioni per osservare gradualmente l'ambiente. Ci sono tre tipi di azioni che offrono una combinazione di capacità di sfruttamento ed esplorazione all'agente:

1. effettuare un attacco locale,
2. effettuare un attacco remoto,
3. connettersi ad altri nodi.

La ricompensa è un valore numerico che rappresenta il valore intrinseco di un nodo (ad esempio, un server SQL ha un valore maggiore rispetto a una macchina di test). Nell'esempio precedente (Figura 3.2), l'attaccante irrompe nella rete dal nodo Win7 a sinistra, indicato dalla grossa freccia arancione, poi procede con un movimento laterale verso il nodo Win8 sfruttando una vulnerabilità in SMB, poi utilizza alcune credenziali memorizzate per accedere a una macchina Win7, sfrutta una vulnerabilità remota di IIS per prendere il controllo del server IIS, e infine utilizza stringhe di connessione divulgate per accedere al database SQL.
L'ambiente di simulazione è parametrizzato dalla definizione della rete, che consiste nel grafo di rete insieme alla descrizione delle vulnerabilità supportate e ai nodi in cui sono presenti. Poiché la simulazione non esegue alcun codice, non esiste un modo per implementare effettivamente vulnerabilità ed exploit. Pertanto, modelliamo ogni vulnerabilità in modo astratto definendo: una precondizione che determina se la vulnerabilità è attiva su un dato nodo; la probabilità che possa essere sfruttata con successo da un attaccante; e gli effetti collaterali di un exploit riuscito.
Ogni nodo ha un insieme di proprietà denominate e assegnate. La precondizione viene quindi espressa come un'espressione booleana sull'insieme delle possibili proprietà del nodo (o flag).

3.2.1 Esiti delle vulnerabilità

Ogni vulnerabilità ha un esito predefinito che può includere:

- Un insieme di credenziali divulgate;
- Un riferimento divulgato a un altro nodo nella rete;
- Informazioni divulgate su un nodo (proprietà del nodo);
- Proprietà di un nodo;
- Escalation dei privilegi su un nodo.

Esempi di vulnerabilità remote includono:

- Un sito SharePoint che espone credenziali SSH (ma non necessariamente l'ID della macchina remota);
- Una vulnerabilità SSH che concede l'accesso alla macchina;
- Un progetto GitHub che divulga credenziali nella cronologia dei commit;
- Un sito SharePoint con un file contenente un token SAS per l'account di archiviazione.

Esempi di vulnerabilità locali sono:

- Estrazione di token di autenticazione o credenziali da una cache di sistema;
- Escalation a privilegi SYSTEM;
- Escalation a privilegi di amministratore.

Le vulnerabilità possono essere definite a livello di nodo o possono essere definite globalmente e attivate dalla precondizione espressa come espressione booleana.

3.3 Scenari Simulabili

CyberBattleSim è uno strumento di simulazione che mira a consentire la simulazione di una varietà di scenari legati alla sicurezza informatica e alla cybersicurezza. Alcuni degli scenari simulabili con CyberBattleSim includono:

- Simulazione di attacchi e difese informatiche: gli utenti possono simulare attacchi informatici contro una rete o un sistema cercando di scoprire vulnerabilità e sfruttarle. Dall'altra parte, possono anche simulare difese informatiche per proteggere la rete e rispondere agli attacchi.
- Rilevamento delle minacce: CyberBattleSim può essere utilizzato per simulare scenari di rilevamento delle minacce, dove gli utenti cercano di identificare attività sospette o comportamenti maligni all'interno di una rete.
- Analisi delle vulnerabilità: gli utenti possono eseguire simulazioni per valutare la presenza di vulnerabilità all'interno di un sistema o di una rete e valutare il loro impatto sulla sicurezza.
- Valutazione della risposta agli incidenti: la simulazione può essere utilizzata per valutare la capacità di un'organizzazione o di un sistema di rispondere agli incidenti di sicurezza informatica, compresa la gestione delle violazioni.
- Test di strategie di difesa: gli utenti possono testare diverse strategie di difesa informatica per valutare l'efficacia delle misure di sicurezza e la resilienza della rete.

- Valutazione delle politiche di sicurezza: CyberBattleSim può essere utilizzato per valutare l'impatto delle politiche di sicurezza informatica e delle decisioni sulla sicurezza su una rete o un sistema.
- Addestramento e formazione: è possibile utilizzare la simulazione per addestrare e formare professionisti della sicurezza informatica e per testare la preparazione del personale di sicurezza in scenari di attacco e difesa.
- Valutazione delle tecnologie di sicurezza: gli utenti possono simulare l'implementazione di diverse tecnologie di sicurezza informatica per valutare la loro efficacia nella protezione dei sistemi e delle reti.

In generale, CyberBattleSim offre la flessibilità per configurare una vasta gamma di scenari di cybersicurezza, consentendo agli utenti di esplorare, addestrare e valutare aspetti critici della sicurezza informatica in un ambiente simulato controllato. Notebooks disponibili dell'ambiente "Capture The Flag" (Cattura la Bandiera):

- **Random Agent**: Notebook interattivo per sperimentare con un agente casuale nell'ambiente "Capture The Flag".
- **Sessione interattiva per un attaccante umano**: Notebook interattivo che consente a un player umano di partecipare in modo interattivo all'ambiente "Capture The Flag".
- **Sessione interattiva - completamente risolta**: Notebook interattivo che mostra una soluzione completa per l'ambiente "Capture The Flag".

Notebook disponibili dell'ambiente "Chain" (Catena):

- **Random Agent**: Notebook interattivo per sperimentare con un agente casuale nell'ambiente "Chain".

Altri ambienti:

- **Sessione interattiva con un ambiente generato casualmente**: Notebook interattivo che consente di esplorare un ambiente generato casualmente e interagire con esso.
- **Random Agent che gioca su reti generate casualmente**: Notebook interattivo che mostra un agente casuale in azione su reti generate casualmente.

Benchmark (Valutazioni di prestazioni):

- **Valutazione delle prestazioni su un ambiente specifico**: Notebook che mostrano la valutazione delle prestazioni degli agenti di base su vari ambienti.
- **Valutazione delle prestazioni su ambienti "Chain" con un difensore di base**: Notebook che mostrano la valutazione delle prestazioni degli agenti di base su ambienti "Chain" con un difensore di base.

- **Valutazione del trasferimento dell'apprendimento con DQL**: Notebook che mostrano la valutazione dell'apprendimento con trasferimento utilizzando Deep Q-Learning (DQL).
- **Epsilon Greedy con ricerche di credenziali**: Notebook che mostrano l'uso di una strategia epsilon-greedy con ricerche di credenziali in ambienti specifici.
- **Tabular Q Learning**: Quaderni che mostrano l'apprendimento tabulare Q in un determinato ambiente.

Per tutti i casi precedenti sono disponibili sia il codice sorgente *.py* che il notebook completo *.ipynb* con output e grafici. Questi notebook e valutazioni sono utili per esplorare, testare e valutare le prestazioni degli agenti nell'ambito della cybersecurity e degli ambienti simulati forniti da CyberBattleSim.

3.4 Scenari Simulati

Per la prima simulazione sono stati utilizzati i parametri standard definiti all interno della prova di esempio del simulatore, contenente una battaglia preimpostata di test. Il tipo di scenario simulato è un ambiente di sicurezza informatica in cui un agente attaccante utilizza l'algoritmo DQL (Deep Q-Learning) per prendere decisioni su come interagire con una rete di nodi ognuno dei quali ha determinate proprietà e vulnerabilità. Alcuni aspetti chiave del tipo di scenario simulato includono:

1. **Agenti di attacco e difesa**: nella simulazione, c'è un agente che agisce come attaccante e cerca di ottenere il controllo dei nodi nella rete, e un agente di difesa che cerca di proteggere questi nodi o di ripristinarli in caso siano già stati compromessi.
2. **Ambiente di rete**: l'ambiente simulato è composto da nodi di rete ognuno dei quali ha diverse proprietà e stato (ad esempio, sistema operativo, software installato, vulnerabilità).
3. **Azione dell'agente**: l'agente DQL prende decisioni su quale azione intraprendere in base all'ambiente circostante. Queste azioni possono includere esplorare nodi, tentare attacchi locali o remoti e altro ancora.
4. **Ricompensa**: l'agente DQL riceve una ricompensa in base alle azioni intraprese. La simulazione tiene traccia delle ricompense cumulative ottenute durante l'episodio.
5. **Obiettivo**: l'obiettivo dell'agente attaccante è massimizzare la ricompensa scoprendo e possedendo nodi all'interno della rete. L'agente cerca di apprendere una strategia efficace per raggiungere questo obiettivo. In contrapposizione

all'obiettivo dell'attaccante, il difendente ha come scopo quello di mantenere un determinato livello di SLA (`Service Level Availability`) oppure di ripristinare tutte le macchine compromesse ed eradicare la minaccia.

6. **Esplorazione e sfruttamento**: l'attaccante utilizza una strategia epsilon-greedy, con un valore iniziale di epsilon elevato che viene gradualmente ridotto durante l'addestramento. Questo indica una combinazione di esplorazione (tentando azioni casuali) e sfruttamento (sfruttando le conoscenze acquisite).

7. **Statistiche di episodio**: alla fine di ogni episodio, la simulazione fornisce statistiche sull'episodio, comprese le azioni eseguite, le ricompense ottenute e altre informazioni.

Codice utilizzato

Listing 3.1: Chain environments with a basic defender

```
import sys
import logging
import gym
import importlib
import cyberbattle.agents.baseline.learner as learner
import cyberbattle.agents.baseline.plotting as p
import cyberbattle.agents.baseline.agent_wrapper as w
import cyberbattle.agents.baseline.agent_dql as dqla
import cyberbattle.agents.baseline.agent_randomcredlookup
    as rca
from cyberbattle.agents.baseline.agent_wrapper import
    Verbosity
from cyberbattle._env.defender import
    ScanAndReimageCompromisedMachines
from cyberbattle._env.cyberbattle_env import AttackerGoal
    , DefenderConstraint
importlib.reload(learner)
importlib.reload(p)
logging.basicConfig(stream=sys.stdout, level=logging.
    ERROR, format="%(levelname)s: %(message)s")
cyberbattlechain_defender = gym.make(
    'CyberBattleChain-v0',
    size=10,
    attacker_goal=AttackerGoal(own_atleast=0,
        own_atleast_percent=1.0),
    defender_constraint=DefenderConstraint(maintain_sla
        =0.80),
    defender_agent=ScanAndReimageCompromisedMachines(
```

```
                                        probability=0.6,
                                        scan_capacity=2,
                                        scan_frequency=5)
)
ep = w.EnvironmentBounds.of_identifiers(
    maximum_total_credentials=22,
    maximum_node_count=22,
    identifiers=cyberbattlechain_defender.identifiers
)
iteration_count = 600
training_episode_count = 10
dqn_with_defender = learner.epsilon_greedy_search(
    cyberbattle_gym_env=cyberbattlechain_defender,
    environment_properties=ep,
    learner=dqla.DeepQLearnerPolicy(
        ep=ep,
        gamma=0.15,
        replay_memory_size=10000,
        target_update=5,
        batch_size=256,
        learning_rate=0.01),
    episode_count=training_episode_count,
    iteration_count=iteration_count,
    epsilon=0.90,
    render=False,
    epsilon_exponential_decay=5000,
    epsilon_minimum=0.10,
    verbosity=Verbosity.Quiet,
    title="DQL"
)
dql_exploit_run = learner.epsilon_greedy_search(
    cyberbattlechain_defender,
    ep,
    learner=dqn_with_defender['learner'],
    episode_count=training_episode_count,
    iteration_count=iteration_count,
    epsilon=0.0,  # 0.35,
    render=False,
    # render_last_episode_rewards_to='images/chain10',
    verbosity=Verbosity.Quiet,
    title="Exploiting DQL"
)
```

```
credlookup_run = learner.epsilon_greedy_search(
    cyberbattlechain_defender,
    ep,
    learner=rca.CredentialCacheExploiter(),
    episode_count=10,
    iteration_count=iteration_count,
    epsilon=0.90,
    render=False,
    epsilon_exponential_decay=10000,
    epsilon_minimum=0.10,
    verbosity=Verbosity.Quiet,
    title="Credential lookups (epsilon-greedy)"
)
# Plots
all_runs = [
    credlookup_run,
    dqn_with_defender,
    dql_exploit_run
]
p.plot_averaged_cummulative_rewards(
    all_runs=all_runs,
    title=f"Attacker agents vs Basic Defender -- rewards\
        n env={cyberbattlechain_defender.name}, episodes
        ={training_episode_count}"
)
# p.plot_episodes_length(all_runs)
p.plot_averaged_availability(title=f"Attacker agents vs
    Basic Defender -- availability\n env={
    cyberbattlechain_defender.name}, episodes={
    training_episode_count}"
```

3.4.1 Input ricevuti e output prodotti

Il codice riceve i seguenti input e parametri di configurazione:

- **Configurazione dell'ambiente di simulazione**: Questo include parametri come la dimensione della rete (*size*), gli obiettivi dell'attaccante (*AttackerGoal*), e i vincoli del difensore (*DefenderConstraint*). Questi parametri definiscono l'ambiente di simulazione in cui gli agenti opereranno.
- **Proprietà dell'ambiente (EnvironmentBounds)**: Qui vengono definiti i dettagli relativi alle proprietà dell'ambiente simulato come il massimo numero

di credenziali totali e il massimo numero di nodi nella rete. Questi parametri definiscono le caratteristiche dell'ambiente in cui gli agenti agiranno.

- **Parametri di addestramento degli agenti**: Questi parametri includono il numero di episodi di addestramento (*training_episode_count*), il numero di iterazioni (*iteration_count*), il tasso di apprendimento (*learning_rate*), il tasso di esplorazione (epsilon), e altri parametri specifici dell'agente. Questi parametri influenzano il modo in cui gli agenti apprendono e prendono decisioni durante l'addestramento.

- **Metodi di addestramento degli agenti**: Il codice utilizza diverse funzioni e metodi per addestrare gli agenti di attacco. Ad esempio, vengono utilizzati il DQL (*Deep Q-Learning*) e l'esploratore di credenziali come agenti di attacco. Questi metodi ricevono input come l'ambiente di simulazione e i parametri di addestramento.

- **Configurazioni specifiche degli agenti**: Gli agenti possono avere configurazioni specifiche come il numero di episodi di addestramento, il tasso di apprendimento, il tasso di esplorazione e altri parametri che influenzano il loro comportamento durante l'addestramento.

Inoltre, il codice utilizza una serie di librerie Python, come Gym per la creazione dell'ambiente di simulazione e altre librerie per la gestione del logging e la creazione di grafici per visualizzare i risultati dell'addestramento. Il codice produce principalmente output sotto forma di grafici e informazioni di log. Ecco gli output principali prodotti da questo codice:

- **Grafici delle prestazioni degli agenti**: Alla fine dell'addestramento e della valutazione degli agenti vengono generati grafici che mostrano le prestazioni degli agenti in termini di ricompense cumulative medie ottenute in diversi episodi di addestramento. Questi grafici consentono di valutare le prestazioni relative degli agenti e l'efficacia delle strategie di addestramento.

- **Informazioni di log**: Il codice utilizza la libreria di logging per generare informazioni di log durante l'esecuzione. Questi includono informazioni sul livello di logging specificato, ad esempio errori o avvisi, e possono essere visualizzati nel terminale durante l'esecuzione del codice. Le informazioni di log possono essere utili per il debugging e il monitoraggio dell'esecuzione del codice.

- **Altri possibili output personalizzati**: A seconda della configurazione del codice, potrebbero essere presenti ulteriori output personalizzati o informazioni di debug, ad esempio la visualizzazione di episodi specifici o altre informazioni sul comportamento degli agenti durante l'addestramento.

In generale, gli output principali sono i grafici che consentono di valutare le prestazioni degli agenti di attacco in un ambiente di simulazione specifico. Questi grafici forniscono una rappresentazione visiva delle prestazioni degli agenti e dei risultati dell'addestramento. Spiegazione dei parametri di configurazione I principali parametri di configurazione utilizzati nel codice sono:

- **cyberbattlechain_defender**: Questo parametro rappresenta l'ambiente di simulazione CyberBattleChain in cui gli agenti opereranno. Vengono specificati vari dettagli dell'ambiente come la dimensione della rete, gli obiettivi dell'attaccante e i vincoli del difensore.

- **ep**: Questo parametro rappresenta le proprietà dell'ambiente come il massimo numero di credenziali totali e il massimo numero di nodi nella rete. Queste proprietà definiscono le caratteristiche dell'ambiente simulato in cui gli agenti opereranno.

- **iteration_count**: Questo parametro specifica il numero di iterazioni o passi di addestramento che gli agenti eseguiranno durante l'intero processo di addestramento.

- **training_episode_count**: Questo parametro indica il numero di episodi di addestramento che gli agenti completeranno durante l'addestramento. Un episodio rappresenta una serie di azioni compiute dagli agenti all'interno dell'ambiente di simulazione.

- **dqn_with_defender**: Questo parametro rappresenta l'agente di attacco DQL (Deep Q-Learning) e include diverse configurazioni specifiche dell'agente come il gamma (fattore di sconto), la dimensione della memoria di riproduzione, l'aggiornamento del target, la dimensione del batch, il tasso di apprendimento e altri.

- **credlookup_run**: Questo parametro rappresenta un altro agente di attacco chiamato "Credential Cache Exploiter". Anche questo agente include configurazioni specifiche come la probabilità di esplorazione epsilon, il numero di episodi di addestramento e altri.

- **all_runs**: Questo parametro è una lista che include tutti gli agenti di attacco addestrati. Viene utilizzato per generare grafici che confrontano le prestazioni degli agenti.

- **verbosity**: Questo parametro controlla il livello di verbosità o dettaglio delle informazioni di log durante l'esecuzione del codice. Può essere configurato per generare più o meno informazioni di log a seconda delle esigenze di debugging o monitoraggio.

- **title**: Questo parametro è utilizzato per fornire un titolo ai grafici generati, consentendo di identificarli in modo chiaro quando vengono visualizzati o salvati.

In generale, questi parametri di configurazione influenzano il modo in cui gli agenti di attacco vengono addestrati e valutati nell'ambiente di simulazione *CyberBattleChain* e come vengono presentati i risultati attraverso grafici e informazioni di log. Modificando questi parametri è possibile personalizzare l'addestramento e la valutazione degli agenti per adattarli alle specifiche esigenze della simulazione.

3.4.2 Spiegazione del funzionamento

Il Notebook eseguito è uno script Python utilizzato per addestrare e valutare agenti di attacco e difesa in un ambiente di simulazione denominato "*CyberBattleChain*". L'obiettivo è valutare le prestazioni degli agenti nell'affrontare un difensore di base all'interno dell'ambiente simulato. Di seguito possiamo trovare una spiegazione delle parti principali del codice:

1. **Importazioni**: Le prime righe del codice sono importazioni di librerie e moduli necessari per eseguire la simulazione, ad esempio librerie per la gestione del logging, la creazione di un ambiente di gym, e moduli specifici per la simulazione *CyberBattleChain*.

2. **Configurazione dell'ambiente di simulazione**: Viene creato un ambiente di simulazione *CyberBattleChain* con determinate configurazioni. L'ambiente viene configurato con le dimensioni della rete (*size*), gli obiettivi dell'attaccante (*AttackerGoal*) e i vincoli del difensore (*DefenderConstraint*).

3. **Definizione delle proprietà dell'ambiente (EnvironmentBounds)**: Vengono definite le proprietà dell'ambiente come il numero massimo di credenziali totali e il numero massimo di nodi nella rete.

4. **Addestramento degli agenti**: Vengono addestrati gli agenti di attacco utilizzando il metodo *epsilon_greedy_search*. Gli agenti utilizzati includono un agente DQL di addestramento (Deep Q-Learning), un agente per l'esplorazione delle credenziali (Credential lookups $\epsilon - greedy$) e un agente per l'exploiting il quale cerca di sfruttare le conoscenze acquisite attraverso l'algoritmo DQL (Exploiting DQL). Vengono specificate diverse configurazioni per gli agenti come il numero di episodi di addestramento, il numero di iterazioni e i parametri dell'agente, quali il tasso di apprendimento e la probabilità di esplorazione (epsilon).

5. **Stampa dei risultati**: Alla fine del codice vengono generati dei grafici per visualizzare le prestazioni degli agenti. In particolare viene creato un grafico delle ricompense cumulative medie ottenute dagli agenti in diversi episodi di addestramento.

In generale questo codice esegue una simulazione dell'addestramento e della valutazione degli agenti di attacco in un ambiente di sicurezza informatica simulato. Gli agenti vengono addestrati a prendere decisioni ottimali per massimizzare le loro ricompense in un ambiente di rete simulato con vulnerabilità e nodi. Gli obiettivi dell'attaccante includono la scoperta e il "possesso" di nodi nella rete. I risultati dell'addestramento vengono quindi visualizzati attraverso grafici.

Capitolo 4

Simulazione di un CSIRT

Per ottenere una comprensione completa degli effetti del CSIRT sulla propagazione delle minacce, è consigliabile eseguire un numero significativo di simulazioni con diverse configurazioni dei parametri. Tuttavia, il numero esatto dipende da vari fattori, tra cui la disponibilità di risorse computazionali e il tempo a disposizione. In linea di massima, si può considerare l'idea di eseguire almeno quattro categorie principali di simulazioni, ognuna con diverse configurazioni:

1. **CSIRT altamente capillare**: è stata eseguita una simulazione che implementi un CSIRT altamente capillare, con variazioni nelle probabilità di scansione, frequenza di scansione e altre configurazioni correlate.

2. **CSIRT moderatamente capillare**: è stata eseguita una seconda simulazione simile alla precedente per valutare l'efficacia di uno CSIRT con capillarità moderata, con variazioni nei parametri di probabilità di scansione, frequenza di scansione e altri correlati.

3. **CSIRT poco capillare**: è stata eseguita una terza simulazione, simile alle due precedenti, con capillarità minima, tramite delle variazioni nei parametri di probabilità di scansione, frequenza di scansione e altri correlati.

4. **CSIRT assente**: infine, per simulare la mancanza di un CSIRT, è stata eseguita una simulazione senza un difensore in modo da avere dei parametri di riferimento con cui poi confrontare le varie simulazioni aventi uno CSIRT a difesa della rete.

Così facendo è stato possibile valutare l'effetto di diversi livelli di capillarità del CSIRT sulla propagazione delle minacce.
In totale, ciò significa che sono state effettuate 4 simulazioni, ognuna delle quali avente un numero massimo di 1000 iterazioni, in modo da simulare l'avanzamento del tempo durante la fase di attacco, e 20 episodi durante i quali l'attaccante e il difendente si sono confrontati. Questo numero fornisce una base solida per analizzare gli effetti del CSIRT sulla propagazione delle minacce, tuttavia in futuro si potrebbe aumentare o ridurre il numero di simulazioni in base alle risorse a disposizione. La modifica di "*iteration_count*" e "*training_episode_count*" dipenderà dal livello di dettaglio e dalla precisione che si desidera ottenere dalle simulazioni. Questi parametri

controllano quanti passi di addestramento vengono effettuati e quante simulazioni vengono eseguite. Nel nostro caso sono state fatte le seguenti considerazioni:

- **iteration_count** (Numero di Iterazioni): Questo parametro controlla quante iterazioni vengono eseguite durante ciascun episodio di addestramento. Più iterazioni possono consentire un addestramento più approfondito, ma richiederanno anche più tempo di esecuzione. Nel nostro caso si è scelto un numero adeguato che non rendesse le simulazioni troppo lunghe ma che le rendesse al contempo il più possibile accurate e rappresentative. Se si volesse avere un addestramento più dettagliato, si potrebbe aumentare "*iteration_count*" al di sopra delle 1000 utilizzate nel nostro caso.

- **training_episode_count** (Numero di Episodi di Addestramento): Questo parametro controlla quante simulazioni complete vengono eseguite durante l'addestramento. Un numero maggiore di episodi può fornire una migliore generalizzazione, ma richiederà anche più tempo. Anche in questo caso si è scelto un numero che potesse bilanciare il tempo di esecuzione con la possibilità di ottenere risultati affidabili. Se si volesse avere una simulazione più accurata, si potrebbe aumentare "*training_episode_count*" al di sopra dei 20 episodi.

In generale, la modifica di questi parametri deve bilanciare la precisione desiderata con il tempo di esecuzione disponibile, assicurandosi di avere risorse sufficienti (tempo e capacità di calcolo) per gestire simulazioni più lunghe o con più iterazioni.
Per quanto riguarda la configurazione degli iperparametri come il tasso di apprendimento (learning rate), il fattore di sconto (gamma), la dimensione del batch di addestramento e la frequenza di aggiornamento del target possono essere regolati secondo le configurazioni di base dell'agente DQL. Le scelte di questi parametri devono riflettere gli obiettivi della simulazione. Ad esempio, se l'obiettivo è valutare come un CSIRT altamente efficace influisce sulla mitigazione delle minacce, è possibile impostare i parametri in modo che il difensore intervenga in modo più aggressivo e reattivo. Al contrario, se si vuole valutare come un CSIRT meno efficace o assente influisce sulla propagazione delle minacce, è possibile ridurre l'intervento del difensore e rendere più difficile per l'agente attaccante essere ostacolato.
Per modellare una rete di una infrastruttura critica di una regione italiana, è stato necessario considerare una rete più complessa rispetto a quella descritta con i parametri standard. L'obiettivo è stato quello di avere un numero di nodi e credenziali più realistico, considerando la dimensione della rete e delle credenziali in modo da riflettere meglio la complessità di una rete di una infrastruttura critica. Tuttavia, il processo di modellazione specifico dipende dagli obiettivi della simulazione.
Rispetto ai parametri originali, è stato aumentato il numero di nodi a 92 ($size = 90$ a cui vanno aggiunti il nodo iniziale e quello finale) e il numero massimo di credenziali a 50 per riflettere una rete più grande e complessa che andasse a rispecchiare il più possibile una infrastruttura critica regionale. Queste modifiche hanno reso la simulazione più rappresentativa di una situazione in cui stiamo valutando la propagazione

delle minacce all'interno di una rete di infrastrutture critiche regionali.
Di seguito possiamo trovare alcune delle considerazioni generali che sono state valutate per modellare una rete di infrastruttura critica più realistica:

1. Numero di nodi e credenziali: è stato determinato il numero di nodi nella rete (ad esempio, server, dispositivi di rete) e il numero di credenziali (username e password) disponibili. La dimensione è dipesa dalla scala della rete che si è cercato di modellare.

2. Topologia di rete: è stata definita una topologia di rete realistica che rifletta la connettività tra i nodi. La simulazione definisce un insieme di reti seguendo uno schema specifico apprendibile dalle proprietà associate ai nodi.

3. Lo schema della rete è visibile in figura 2.4 ed è composto da un nodo di avvio a cui segue un chain pattern composto di nodi Linux e Windows e infine un nodo Linux contenente un flag che indica la fine della rete. La rete è parametrizzata dalla lunghezza della catena centrale Linux-Windows e si presuppone che il nodo iniziale sia compromesso e abbia un leak di credenziali che permette di connettersi agli altri nodi. Per ogni sezione "$NODO \rightarrow Windows$", il nodo ha una vulnerabilità locale che espone la password RDP alla macchina Windows e una serie di altre vulnerabilità trappola (con costo elevato e senza risultato). Per ogni sezione "$NODO \rightarrow Linux$", il nodo presenta una vulnerabilità locale che espone la password SSH alla macchina Linux e una serie di altre vulnerabilità trappola. La catena, come già accennato, termina con un nodo con un flag di reward.

Figura 4.1: Schema standard della rete in CyberBattleSim

Nonostante la rete possa sembrare troppo generica, è bene tenere presente che aumentare la complessità della rete e delle credenziali potrebbe richiedere più risorse computazionali, pertanto è stato necessario assicurarsi che il sistema in uso potesse gestire la simulazione senza richiedere un eccesso di risorse computazionali.
Per condurre simulazioni con diverse configurazioni di difensori, è possibile regolare diversi parametri nel codice essendo quest'ultimo già ben strutturato per testare differenti scenari. La configurazione di questi parametri dipende dall'obiettivo della simulazione e dal contesto descritto. Di seguito sono elencate le configurazioni di questi parametri, tenendo conto del contesto di una simulazione del comportamento di un CSIRT (Computer Security Incident Response Team) nella propagazione delle minacce. Per il nostro studio sono state effettuate quattro diverse simulazioni: simulazione senza difensore, simulazione con un difensore limitato, simulazione con un difensore discreto e una simulazione con un difensore ottimale.

Simulazione senza difensore (Nessun intervento del CSIRT):

- Sono stati definiti i parametri dell'ambiente ($size = 90$, $iteration\_count = 1000$, $maximum\_total\_credentials = 50$, $maximum\_node\_count = 100$, $training\_episode\_count = 20$) e dell'attaccante ($attacker\_goal = own\_atleast = 0$, $own\_atleast\_percent = 1.0$) in modo da renderli replicabili nei tre scenari successivi.
- Le dimensioni della memoria di riproduzione possono essere regolate in base alla complessità dell'ambiente. Per simulazioni in cui è coinvolto un CSIRT altamente efficace, è possibile aumentare la dimensione della memoria di riproduzione per consentire all'agente DQL attaccante di acquisire esperienze più ampie. Nel nostro caso, volendo valutare l'intervento di uno CSIRT in caso di propagazione di una minaccia, si è preferito usare un valore fisso in modo che l'attaccante abbia sempre le stesse risorse indipendentemente dal livello di efficacia del CSIRT che si prepara ad affrontare.
- È stato rimosso il difensore ed è stata eseguita la simulazione in modo da ottenere dei valori da prendere come rifermento per gli scenari successivi.

Simulazione con un difensore limitato (CSIRT poco capillare):

- È stato impostato $cyberbattlechain\_defender$ in modo che *DefenderConstraint* abbia un valore di $maintain\_sla$ prossimo a 0 o addirittura pari a 0 (nel nostro caso $maintain\_sla = 0.15$). Questo significa che il difensore non interverrà o sarà inefficace nel mantenere i servizi attivi oltre il 15%.
- Per un CSIRT meno efficace, è stata ridotta la probabilità di scansione (in questo caso $probability = 0.3$). Questo indica che il difensore interviene meno frequentemente e con meno probabilità di successo.
- Per un CSIRT meno efficace, è stata ridotta inoltre la frequenza di scansione a ogni 5 passi di tempo ($scan\_frequency = 5$) in modo da simulare un intervento meno frequente del CSIRT.

Simulazione con un difensore discreto (CSIRT con capillarità moderata):

- È stato impostato *DefenderConstraint* in modo che $maintain\_sla$ sia impostato su un valore moderato (in questo caso 0.6). Ciò significa che il difensore ha un'efficacia moderata e deve mantenere i servizi attivi oltre il 60%.
- Per un CSIRT con capillarità moderata, è stata ridotta la probabilità di scansione (in questo caso $probability = 0.55$) in modo tale che il difensore intervenga con meno frequenza rispetto a uno CSIRT altamente capillare.
- Per un CSIRT con capillarità moderata, è stata impostata una frequenza di scansione ogni 4 passi di tempo (episodi), simulando un intervento

meno frequente rispetto a uno CSIRT ottimale ma comunque con una frequenza più elevata rispetto a uno CSIRT con capillarità minima.

Simulazione con un difensore ottimale (CSIRT altamente efficace):

- È stato impostato *DefenderConstraint* in modo che *maintain_sla* sia impostato su un valore vicino a 1 o addirittura pari a 1 (in questo caso $maintain\_sla = 0.9$). Questo rappresenta un difensore altamente efficace che mantiene quasi perfettamente il livello di servizio (almeno il 90% dei servizi devono rimanere attivi).
- Per simulare un CSIRT altamente efficace, è stata impostata una probabilità di scansione elevata ($probability = 0.9$) in modo tale da far risultare il difensore molto attivo nella scansione delle risorse compromesse e nel reimaging.
- Per un CSIRT altamente efficace è stata impostata una frequenza di scansione elevata pari ad 2 passi di tempo (episodi), simulando un intervento molto frequente ma comunque realistico per uno CSIRT regionale.

Ognuna delle quattro simulazioni fornirà risultati che rappresentano l'effetto di diversi livelli di intervento del CSIRT sulla propagazione delle minacce. Le simulazioni mirano a rivelare come un difensore altamente efficace influisce sul comportamento dell'agente attaccante rispetto a un difensore meno efficace o assente. La prima simulazione rappresenta l'assenza di un difensore (CSIRT), il che implica che l'agente attaccante ha più libertà nell'effettuare attacchi. La seconda e la terza simulazione rappresentano un CSIRT meno efficace con una scansione meno frequente, una memoria di riproduzione leggermente più piccola e una probabilità di successo inferiore. Questo riflette una situazione in cui il CSIRT è meno competente nella mitigazione delle minacce. Infine, la terza simulazione rappresenta un CSIRT altamente efficace con una scansione frequente, una grande memoria di riproduzione e un alto tasso di successo in modo da rappresentare uno CSIRT a difesa di un'infrastruttura altamente protetta. Queste configurazioni dovrebbero consentire di esaminare gli effetti di un CSIRT altamente efficace, di due meno efficaci e della totale assenza di CSIRT sul comportamento dell'agente attaccante e sulla propagazione della minaccia. Le simulazioni sono state eseguite in modo sistematico, registrando i risultati e confrontando le metriche di interesse, come la propagazione e la mitigazione delle minacce, consentendo di valutare in modo approfondito come un CSIRT influisce sulla sicurezza informatica. Inoltre, valutando 20 episodi per ciascuna simulazione abbiamo ottenuto un campione significativo per analizzare le prestazioni in diverse situazioni.

4.1 Analisi dei risultati ottenuti

I risultati ottenuti mostrano quattro diverse simulazioni effettuate con agenti di attacco basati su strategie diverse. Per ogni episodio della simulazione, interrotto dopo 1000 iterazioni, vengono forniti i seguenti dettagli per ciascun episodio:

- **Episode X**: Rappresenta il numero dell'episodio in corso.
- ϵ: Mostra il valore corrente dell'epsilon-greedy exploration per quell'episodio.
- **Reward**: Rappresenta la ricompensa totale accumulata durante l'episodio.
- **last_reward_at**: Indica l'iterazione in cui è stata ottenuta l'ultima ricompensa.
- **Elapsed Time**: Mostra il tempo trascorso per l'episodio in formato `hh:mm:ss`.
- **Breakdown [Reward/NoReward (Success rate)]**: Fornisce una suddivisione delle ricompense ottenute durante l'episodio in diverse categorie, come "explore-local," "explore-remote," eccetera. Ogni categoria mostra il numero di ricompense ottenute e il tasso di successo per quella categoria.
- **exploit deflected to exploration**: Questo valore indica quante volte l'agente ha deciso di esplorare invece di sfruttare le conoscenze acquisite durante l'episodio.

Alla fine della simulazione di tutti gli episodi, sono disponibili i risultati complessivi. In generale, l'obiettivo dell'allenamento di questo agente di Reinforcement Learning (RL) è massimizzare le ricompense accumulate durante gli episodi, mentre si bilanciano l'esplorazione (per scoprire nuove strategie) e lo sfruttamento (per utilizzare le strategie conosciute). Gli episodi successivi mostrano una diminuzione graduale di ϵ indicando che l'agente impara a sfruttare di più la conoscenza acquisita man mano che l'allenamento prosegue.

CSIRT Assente

Nei risultati degli episodi della simulazione, c'è una progressione significativa nell'apprendimento dell'agente attaccante impegnato in un contesto in cui il difensore (CSIRT) è assente.
Episodio 1:

- L'agente ha esplorato principalmente, con un basso tasso di successo nelle azioni di attacco, ottenendo un reward di 932.
- L'attacco remoto e la connessione hanno avuto successo meno del 5% delle volte.
- Esplorazione e sfruttamento sono stati deflessi verso l'esplorazione.

Episodio 2:

- L'agente ha mostrato una maggiore efficienza nell'attacco ottenendo un reward di 1813.
- Le azioni di attacco remoto e connessione hanno avuto un tasso di successo compreso tra il 6% e il 24%.
- Nonostante un aumento del tasso di esplorazione, l'agente ha comunque effettuato più azioni di attacco rispetto all'episodio precedente.

Episodio 3:

- C'è stata un ulteriore crescita nell'efficienza dell'agente nell'effettuare azioni di attacco, soprattutto a livello locale ottenendo però un reward pari a 798.
- L'attacco remoto e di connessione hanno avuto un tasso di successo molto basso (motivo del reward altrettanto basso), ma l'agente ha continuato a ridurre l'esplorazione a favore dell'attacco.

Questi risultati iniziali mostrano che l'agente DQL sta inizialmente esplorando ampiamente l'ambiente, ma sta avendo difficoltà nel trovare azioni di sfruttamento efficaci. Man mano che l'epsilon diminuisce ulteriormente nei successivi episodi ci si aspetta che l'agente diventi più incline allo sfruttamento delle azioni efficaci.
Episodio 4:

- Vi è stato un importante miglioramento che ha portato a un reward di 4082, l'agente ha aumentato notevolmente il successo dell'attacco remoto e di connessione, raggiungendo il 10% e il 24% rispettivamente.
- L'agente ha ancora deflesso alcune azioni di attacco all'esplorazione.

Episodio 5:

- L'agente ha effettuato più azioni di attacco rispetto all'esplorazione ottenendo un reward di 5578.
- L'attacco locale è stato molto efficace (oltre il 90% di successo).
- Il tasso di successo dell'attacco remoto e di connessione è rimasto costante rispetto all'episodio precedente.

Episodio 6:

- Continua il miglioramento dell'efficienza dell'agente nei confronti dell'attacco, soprattutto a livello locale e remoto ottenendo un reward di 8258.
- L'attacco di connessione (`exploit-connect`) ha avuto un moderato tasso di successo (circa il 19%).

Episodio 7:

- L'agente ha ottenuto risultati notevoli in tutte le azioni di attacco, soprattutto a livello locale e di connessione, con successi superiori al 40% e ottenendo il reward massimo di 15964 registrando così il valore più elevato di ricompensa ottenuta in tutte le simulazioni.
- La fase di esplorazione è stata notevolmente ridotta.

Episodio 8-20:

- L'agente ha continuato a migliorare l'efficienza nei suoi attacchi, con una ridotta esplorazione e un successo crescente nell'attacco dovuto al fatto che dall'episodio 8 in avanti l'attaccante è sempre riuscito a conquistare la totalità della rete, come mostrato in figura 4.2.

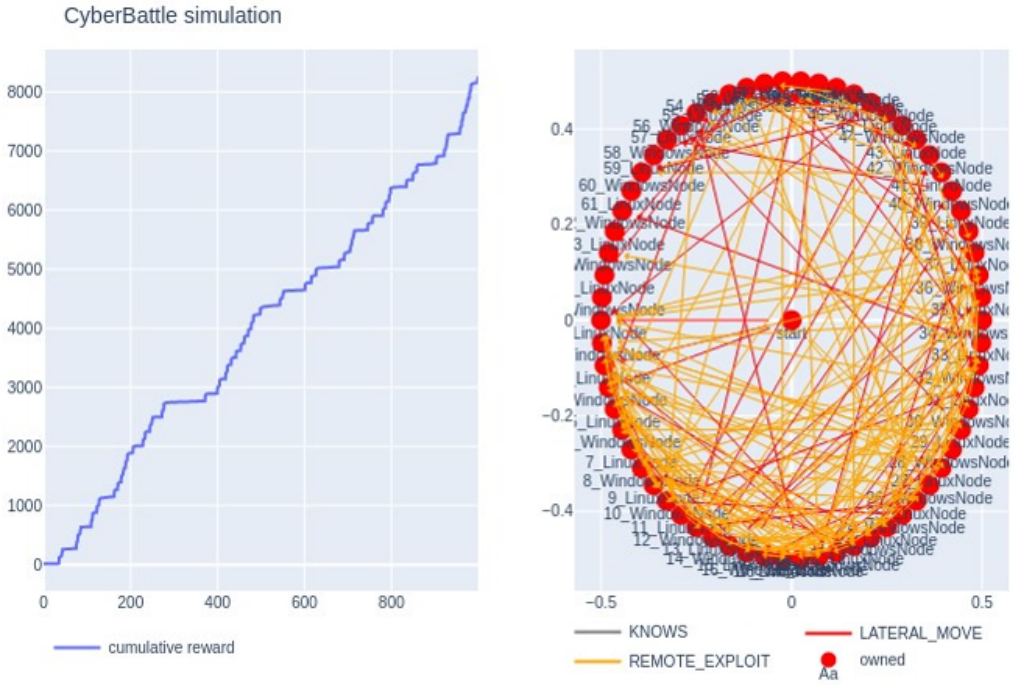

Figura 4.2: Propagazione della minaccia in caso di CSIRT Assente

In generale, questi risultati mostrano come l'agente DQL abbia imparato a bilanciare esplorazione ed esecuzione delle azioni nel corso dell'addestramento.
L'agente, grazie all'assenza del difensore CSIRT, ha mostrato una notevole capacità di apprendimento e miglioramento nella strategia di attacco. Dalla fase iniziale, in cui l'agente esplorava maggiormente, si è evoluto verso un atteggiamento più aggressivo, eseguendo azioni di attacco con maggiore successo man mano che gli episodi proseguivano. Il miglioramento continuo nell'efficienza dell'agente nell'attacco, specialmente a livello locale e remoto, mostra una promettente capacità di

adattamento e apprendimento.
I risultati della simulazione "Exploiting DQL" rappresentano una fase successiva dell'addestramento dell'agente DQL, in cui l'agente è stato impostato per eseguire principalmente azioni di sfruttamento senza esplorazione ($\epsilon = 0.0$).
Tutti e 20 gli episodi hanno mostrato una stabilità nei risultati con un pattern comune: terminano dopo 182-183 iterazioni con un reward quasi costante che si aggira tra 15274 e 15286. Questo è dovuto al fatto che in tutti gli episodi simulati l'attaccante riesce sempre a ottenere il suo scopo, conquistando la totalità della rete con alcune piccole differenze tra i vari episodi. Le azioni locali e di connessione hanno sempre un tasso di successo del 100%, con la sola eccezione di un fallimento nelle azioni locali nell'episodio 4.
Nella simulazione "Exploiting DQL (CSIRT Assente)", la stabilità del reward e del tasso di successo delle azioni eseguite sembra essere predominante. I risultati mostrano una buona performance in termini di esecuzione delle azioni, con un'elevata affidabilità e coerenza durante tutti gli episodi analizzati.
In questa ultima parte vengono esaminati i risultati riguardanti un processo di addestramento tramite esplorazione ($\epsilon - greedy$) di un modello coinvolto nell'analisi delle credenziali (Credential lookups) nell'ambito del CSIRT Assente.
I dati mostrano la progressione dei risultati lungo gli episodi e il tasso di successo durante l'esplorazione e lo sfruttamento di varie modalità di acquisizione di credenziali.
Episodio 1:

- Inizia con una frazione di esplorazione elevata, con un tasso di successo molto basso per l'acquisizione di credenziali sia in modalità locale che remota.
- L'exploit connect ha un tasso di successo del 100%, ma viene deflesso alla modalità di esplorazione.

Episodio 2:

- Si nota un leggero miglioramento nei tassi di successo sia per l'esplorazione locale che remota rispetto al primo episodio.
- Tuttavia, l'exploit connect, pur avendo un tasso di successo non nullo, viene ancora deflesso all'esplorazione.

Episodio 3-20:

- Proseguendo con gli episodi successivi, si osserva una tendenza al miglioramento graduale dei tassi di successo durante l'esplorazione, con variazioni irrilevanti.
- Tuttavia, l'exploit connect, pur ottenendo successo, viene in modo consistente deflesso all'esplorazione.

In generale, sembra che l'agente coinvolto abbia migliorato leggermente le sue prestazioni nell'acquisizione di credenziali durante l'esplorazione, ma sembra che, nonostante il successo ottenuto nella fase di exploit, venga spesso deflesso a una fase di esplorazione, probabilmente a causa dell'alta percentuale di esplorazione iniziale.

CSIRT poco capillare

Esaminiamo ora l'esecuzione dell'algoritmo Deep Q-Learning (DQL) con un focus particolare sulle attività di un CSIRT (Computer Security Incident Response Team) classificato come "Poco Efficace".
Episodio 1:

- Il reward ottenuto è pari a 1572.
- La maggior parte delle attività è stata di esplorazione locale e remota con successo limitato nelle attività di sfruttamento.

Episodio 2:

- Il reward ottenuto è pari a 2842.
- Si riscontra un maggiore successo nelle attività di sfruttamento remoto e locale rispetto all'esplorazione.

Episodio 3:

- Il reward ottenuto è pari a 3222.
- L'attaccante ha un discreto successo nelle attività di sfruttamento locale, con un equilibrio relativamente migliore tra esplorazione e sfruttamento.

Episodio 4:

- Il reward ottenuto è pari a 508.
- Il rendimento generale è significativamente inferiore, con quasi nessun successo nelle attività di sfruttamento ed esplorazione. Questo lo si potrebbe interpretare come una prima reazione da parte del CSIRT che riesce a tamponare la propagazione della minaccia.

Episodio 5-7:

- I reward ottenuti oscillano tra 2462 e 4114.
- Notiamo un buon successo nelle attività di sfruttamento locale e remoto, con una diminuzione delle attività di esplorazione non fruttuose le quali mantengono un successo limitato.

Episodio 8:

- Il reward ottenuto scende a 1688 indicando un ulteriore intervento del CSIRT per arginare la minaccia.
- Grazie all intervento del difendente si ottengono successi limitati sia nell'esplorazione che nello sfruttamento.

Episodio 9-10:

- I reward ottenuti sono pari a 3763 per l'episodio 9 e 5006 per l'episodio 10.
- L'attaccante riesce a ottenere ulteriori successi prevalentemente nelle attività di sfruttamento locale, con un successo significativo ma moderato nell'esplorazione.

Episodio 11-20:

- Si osserva un'alternanza di successo tra attività di esplorazione e sfruttamento, con variazioni nei tassi di successo relativi a ciascuna categoria, anche se in generale si mantiene un livello ragionevole di reward complessivo rispetto alla simulazione precedente (senza alcun difensore).
- A partire dall'episodio 15, per l'attaccante si osserva un miglioramento più sostanziale nelle attività di sfruttamento, specialmente a livello locale, se confrontato con l'esplorazione.

Gli episodi mostrano una variazione significativa nelle prestazioni, con un trend generale di miglioramento nelle attività di sfruttamento verso gli episodi finali a indicare che l'attaccante con il passare del tempo riesca a migliorare e affinare le proprie tecniche di attacco e avere un maggior successo ai danni del difendente. L'agente attaccante sembra apprendere e adattarsi progressivamente per ottenere un successo maggiore, specialmente nelle attività di sfruttamento locale.

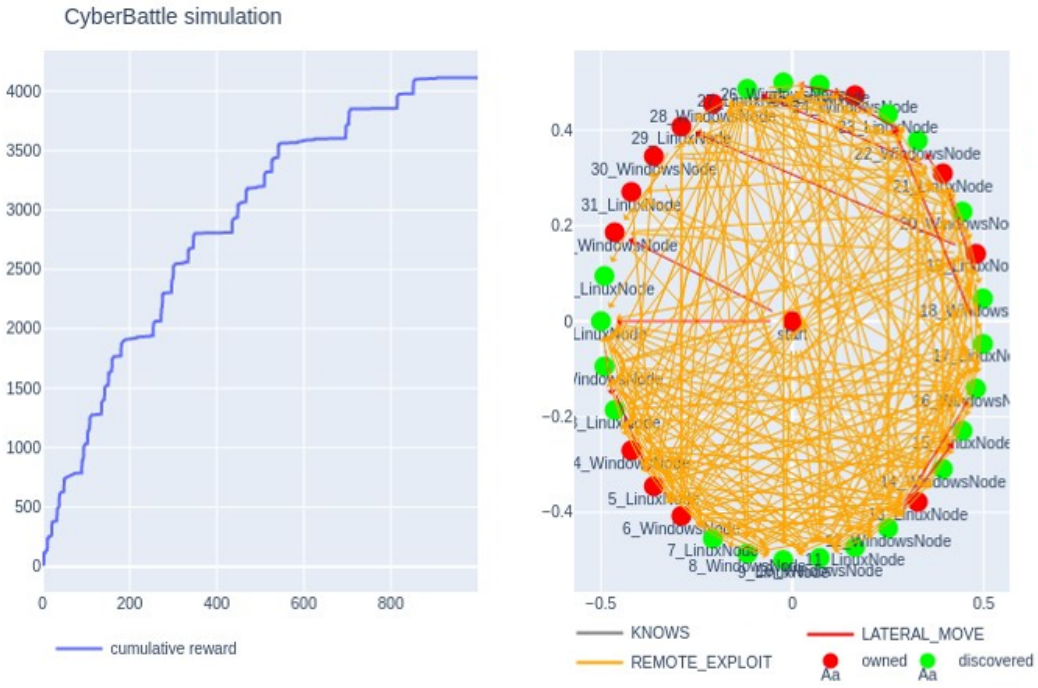

Figura 4.3: Propagazione della minaccia in caso di CSIRT poco capillare

Ciononostante l'attaccante riesce in media a ottenere risultati peggiori rispetto alla simulazione precedente, non riuscendo mai a ottenere il controllo sulla totalità

della rete, come mostrato precedentemente in figura 4.3.
L'analisi successiva si focalizza sull'addestramento di un agente in un ambiente simulato denominato "Exploiting DQL (CSIRT Poco Efficace)". L'obiettivo è valutare le prestazioni dell'agente attaccante, il suo apprendimento nel corso di una serie di 20 episodi e il miglioramento o peggioramento nel perseguire strategie d'attacco. Durante gli episodi, l'agente ha potuto esplorare e apprendere, evolvendo le sue tattiche per ottenere reward positivi attraverso attacchi mirati e, possibilmente, difese efficaci. Vediamo di seguito un analisi più dettagliata di alcuni episodi.
Episodio 1:

- Il reward ottenuto in questo episodio è stato di 2934.
- L'attacco remoto e la connessione hanno avuto un successo limitato, rispettivamente del 5% e dell 11%.
- Nonostante la tipologia di attacco sia mirata all'exploiting, l'esplorazione è stata minima ma efficace per l'attacco.

Episodio 2:

- Il reward ottenuto in questo episodio è stato di 2828.
- L'attacco remoto e la connessione hanno avuto successo rispettivamente con una probabilità del 6% e del 14%, indicando un leggero miglioramento rispetto all'episodio precedente.
- Nonostante un miglioramento, l'esplorazione è ancora presente.

Episodio 3:

- Il reward ottenuto in questo episodio è stato di 2308.
- L'attacco remoto e la connessione hanno avuto successo limitato, rispettivamente 5% e 13%.
- L'agente attaccante ha ridotto l'esplorazione ma, nonostante l'impiego di un difendente, ha ancora spazio per migliorare.

Episodio 4:

- Il reward ottenuto in questo episodio è stato di 4624.
- L'attacco remoto e la connessione hanno avuto successo limitato, rispettivamente 17% e 22%.
- L'esplorazione è stata notevolmente ridotta.

Episodio 5:

- Il reward ottenuto in questo episodio è stato di 5630.

- L'attacco remoto e la connessione hanno ottenuto successi notevoli, rispettivamente 12% e 41%.
- L'agente ha smesso di esplorare e si è focalizzato sull'attacco riuscendo a conquistare quasi la metà della rete (44 nodi), evidenziando un momento critico per il difendente.

Episodio 6:

- Il reward ottenuto in questo episodio è stato di 4978.
- L'attacco remoto ha avuto un successo limitato (11%), mentre la connessione remota è stata più efficace con una probabilità del 14% e riuscendo a conquistare però meno nodi rispetto alla precedente fase di attacco (39 nodi), mostrando una reazione da parte del difensore.
- L'esplorazione, durante questa fase, è stata ridotta a zero.

Episodio 7:

- Il reward ottenuto in questo episodio è stato di 404.
- L'attacco locale ha avuto un successo significativo (75%) riuscendo però ad attaccare con successo solamente 6 nodi della rete, mentre l'attacco remoto è stato meno efficace (1%).
- Questo indica una particolare controffensiva del difendente che è riuscito ad arginare maggiormente l'attaccante il quale ha concentrato la maggior parte dei propri sforzi (913 iterazioni) su attacchi da remoto, portandone a termine con successo solamente 8.
- L'esplorazione è stata ridotta ma non azzerata come nel precedente episodio.

Episodio 8-20:

- L'agente ha continuato a migliorare, ottenendo successi più significativi negli attacchi e riducendo l'esplorazione, non riuscendo però a ottenere mai un reward più elevato rispetto agli episodi precedenti.
- Il reward nei successivi episodi è variato notevolmente, indicando un intervento più efficace del difensore, ma è rimasto complessivamente positivo.
- In questi episodi attaccante e difendente si sono alternati ottenendo fasi molto positive per entrambi.
- Negli episodi 8, 9 e 10 abbiamo un maggior successo del difendente con reward quasi minimi per l'attaccante, il quale però riesce ad apprendere nuove strategie di attacco e migliorare i suoi risultati negli episodi successivi.

- Negli episodi 18, 19 e 20 tuttavia, il difensore riesce ad attivare ulteriori contromisure e a ottenere nuovi successi ai danni dell'attaccante.

L'agente nell'ambiente di "Exploiting DQL (CSIRT Poco Efficace)" ha mostrato un miglioramento progressivo nell'efficienza degli attacchi, riducendo l'esplorazione e concentrandosi maggiormente sull'attacco nel corso degli episodi. Dalla fase iniziale, in cui l'agente esplorava molto e ottenendo successi limitati, si è evoluto verso una strategia più aggressiva, con un successo significativo negli attacchi, soprattutto a livello locale e in alcune occasioni di connessione. L'agente ha smesso di esplorare, concentrandosi principalmente sull'attacco. I risultati degli episodi mostrano un progresso evidente nell'apprendimento dell'agente nel contesto specifico nonostante il difendente riesca con il passare degli episodi a disporre delle contromisure adeguate. Nel seguente esperimento con il modello di apprendimento $\epsilon - greedy$ (CSIRT poco efficace), si è puntato a valutare le azioni di esplorazione e sfruttamento nel contesto di ricerca di credenziali, permettendo di comprendere l'evoluzione dei tassi di esplorazione, i risultati delle azioni di esplorazione e sfruttamento, nonché le tendenze evidenziate durante i vari episodi.
Episodio 1-5:

- Gli episodi 1 e 3 mostrano risultati simili, presentano tassi di esplorazione intorno al 9% e successi di esplorazione inferiori all'8%.
- Gli episodi 2 e 4 presentano una leggera riduzione del tasso di esplorazione rispetto agli episodi 1 e 3, con successi di esplorazione inferiori al 6%.
- L'episodio 5 mostra una riduzione del tasso di esplorazione rispetto agli episodi precedenti, con un tasso intorno al 6% e un successo di esplorazione inferiore al 6%.
- In tutti questi episodi, sia le azioni di sfruttamento locale che remoto hanno successi inferiori al 3%.

Episodio 6-10:

- Gli episodi 6 e 7 mostrano una ridotta efficacia, con tassi di esplorazione compresi tra 5,8% e 5,3%. L'agente ha un'efficacia estremamente bassa nelle azioni di esplorazione, con tassi di successo inferiori all'1%.
- Gli episodi 8 e 9 mostrano tassi di esplorazione simili, con valori intorno al 4,5%, e successi di esplorazione inferiori al 5%.
- L'episodio 10 presenta una leggera diminuzione nel tasso di esplorazione rispetto agli episodi precedenti, con un valore di circa 3,9% e successi di esplorazione inferiori al 3%.
- In tutti questi episodi, le azioni di sfruttamento, sia locali che remote, hanno successi inferiori al 2%.

Episodio 11-14:

- Nei primi tre episodi, ossia gli episodi 11, 12 e 13, i valori di esplorazione rimangono relativamente costanti, con tassi attorno all'3%. I successi di esplorazione si attestano intorno al 5-6%.
- Nell'episodio 14, il tasso di esplorazione continua a diminuire, scendendo a circa 3,1%, mentre il successo nelle azioni di esplorazione è intorno al 5-7%.
- Le azioni di sfruttamento, sia locali che remote, continuano a mostrare successi molto limitati, inferiori al 2%, in tutti questi episodi.

Episodio 15-20:

- Nei primi tre episodi, ovvero gli episodi 15, 16 e 17, i valori dei tassi di esplorazione variano tra 2,9% e 2,6%. Il successo delle azioni di esplorazione oscilla tra l'8% e il 9%.
- Negli ultimi tre episodi, gli episodi 18, 19 e 20, i tassi di esplorazione diminuiscono ulteriormente, variando tra 2,4% e 2,1%. Il successo delle azioni di esplorazione rimane costantemente intorno al 5-6%.
- Le azioni di sfruttamento continuano a mostrare successi limitati, inferiori al 2%, in tutti questi episodi.

Dopo aver analizzato gli episodi, è possibile osservare che il modello $\epsilon - greedy$, mostra una variazione significativa nelle azioni di esplorazione e sfruttamento nel corso degli episodi. Nei primi cinque episodi, il modello ha avuto un tasso di successo molto basso, evidenziando una scarsa efficacia nel reperire le credenziali.
Gli episodi con una percentuale più bassa di successo e un'elevata tendenza all'esplorazione (episodi 1-5) indicano un migliore comportamento del difensore nel contrastare gli attacchi poiché l'attaccante non ha ottenuto le credenziali desiderate.
Episodi con bassi tassi di successo, come nell'intervallo 8-10, rappresentano una tendenza positiva dal punto di vista del difensore, indicando che l'attaccante non è riuscito a sfruttare vulnerabilità o a ottenere credenziali sensibili. Gli episodi 11-14 presentano un livello di successo leggermente superiore, ma comunque non ottimale, suggerendo un adeguato contrasto da parte del difensore contro l'attaccante.
Infine, gli episodi 15-20 con tassi di successo migliori indicano una minore capacità del difensore nel contrastare l'attaccante, permettendogli di ottenere un numero maggiore di credenziali. Pertanto, in generale, minori successi dell'attaccante corrispondono a un comportamento più efficace del difensore nel contrastare gli attacchi.

CSIRT moderatamente capillare

Esaminiamo ora l'esecuzione dell'algoritmo Deep Q-Learning (DQL) con un focus particolare sulle attività di un CSIRT (Computer Security Incident Response Team)

classificato come "moderatamente capillare".
Episodio 1:

- L'agente ha avuto un basso tasso di successo nell'esplorazione e negli attacchi ottenendo un reward di 1426.
- Le azioni di attacco remoto e di connessione (sia di exploit che di explore) sono state poco efficaci.
- L'agente ha mostrato poca efficacia sia nell'esplorazione sia nell'attacco.

Episodio 2:

- L'agente ha avuto una piccola crescita nei successi dell'attacco, specialmente nell'attacco locale riuscendo a ottenere un reward di 2216.
- Le azioni di esplorazione sono rimaste elevate.
- Il tasso di successo nell'attacco remoto e di connessione è rimasto invece basso.

Episodio 3:

- È stato osservato un aumento significativo nei successi dell'attacco locale con un reward ottenuto pari a 3096.
- Le azioni di esplorazione e l'efficacia degli attacchi remoto e di connessione hanno avuto poche variazioni rispetto ai precedenti episodi.

Episodio 4:

- L'efficienza nell'attacco locale è rimasta alta ottenendo per l'exploit local un tasso di successo del 92% e un reward complessivo di 2342.
- L'agente ha mostrato un discreto incremento nella percentuale di successo nell'attacco remoto e di connessione.
- Un piccolo numero di azioni di attacco è stato deflesso verso l'esplorazione.

Episodio 5:

- Ancora una volta, l'agente ha mostrato un'efficacia superiore nell'attacco locale con un tasso di successo dell'85% e un reward complessivo di 3114.
- Il tasso di successo nell'attacco remoto e di connessione è rimasto costante rispetto all'episodio precedente.

Episodio 6:

- L'efficienza nell'attacco locale è rimasta stabile ottenendo un tasso di successo dell'83% nonostante il reward ottenuto sia di 1956.

- Gli attacchi remoto e di connessione hanno ottenuto un tasso di successo più basso rispetto all'attacco locale.
- Le azioni di attacco deflesse verso l'esplorazione sono diminuite rispetto agli episodi precedenti.

Episodio 7:

- Si è verificata un'efficacia notevole nell'attacco locale con un tasso di successo dell'84%, con risultati migliori rispetto agli attacchi remoto e di connessione, rispettivamente di 9% e 7%.
- Le azioni di esplorazione sono state significativamente ridotte, concentrando l'agente maggiormente sull'attacco.

Episodio 8-20:

- Continuo miglioramento nell'efficacia complessiva dell'agente, concentrandosi soprattutto sull'attacco locale.
- Gli attacchi remoto e di connessione hanno mostrato un miglioramento, anche se non paragonabile all'efficacia dell'attacco locale.
- L'agente ha ridotto progressivamente le azioni di esplorazione a favore dell'attacco.

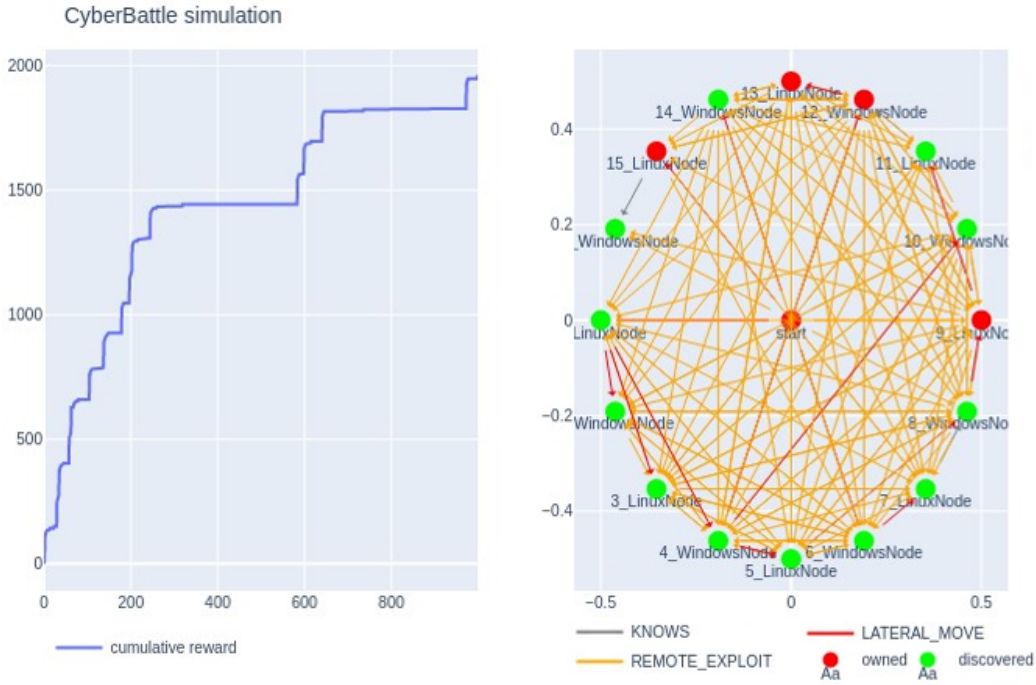

Figura 4.4: Propagazione della minaccia in caso di CSIRT moderatamente capillare

Il modello DQL (CSIRT moderatamente capillare) ha mostrato un apprendimento progressivo, con un chiaro sviluppo nella strategia di attacco. La crescita dell'efficacia nei confronti dell'attacco, soprattutto a livello locale, indica una certa capacità di adattamento e apprendimento del modello. Sebbene gli attacchi remoto e di connessione abbiano avuto successi più modesti, grazie all'intervento del difendente, l'agente ha mostrato un notevole miglioramento nell'efficacia complessiva nel corso degli episodi, con una riduzione delle azioni di esplorazione a favore dell'attacco.
Ciononostante, il reward complessivo è stato mediamente più basso rispetto alle simulazioni precedenti indicando una miglior protezione della rete da parte del difendente, come mostrato in figura 4.4.
L'analisi successiva si focalizza sull'addestramento di un agente in un ambiente simulato denominato "Exploiting DQL (CSIRT moderatamente capillare)". Vediamo di seguito un'analisi più dettagliata di alcuni episodi.
Episodio 1:

- L'agente ha sperimentato una bassa efficienza nelle azioni di attacco ottenendo comunque un reward di 2776.
- I tassi di successo nelle azioni di attacco remoto e di connessione sono stati limitati a circa il 7% e il 4% rispettivamente.
- L'agente ha sperimentato un notevole tasso di fallimento nell'esecuzione degli attacchi.

Episodio 2:

- C'è stata un aumento leggero ma significativo nella performance di attacco traducendosi di conseguenza in un reward più elevato, pari a 3604.
- L'efficienza dell'attacco remoto è aumentata al 28%, mentre l'attacco di connessione è cresciuto al 21%.
- Nonostante questo, una considerevole quantità di attacchi è fallita dimostrando una considerevole attività difensiva.

Episodio 3:

- Il tasso di successo nell'attacco di connessione è notevolmente aumentato al 44% portando così a ottenere un reward di 3576.
- L'agente ha migliorato leggermente la sua efficienza nell'attacco remoto (22%).

Episodio 4:

- L'agente ha sperimentato un calo significativo nel rendimento dell'attacco facendo abbassare il reward a 1234.

- Tutte le azioni di attacco hanno avuto un successo inferiore al 12%, andando a sottolineare un intensa azione difensiva da parte del CSIRT.

Episodio 5:

- Durante questo episodio abbiamo riscontrato un notevole miglioramento con il tasso di successo nell'attacco locale che ha superato il 90% e un reward di 5630.
- Gli attacchi remoti e di connessione sono stati più efficienti con tassi di successo del 5% e del 30% rispettivamente.
- Nonostante la buona capacità difensiva del CSIRT l'attaccante è stato in grado di sviluppare tattiche più efficaci e ottenere così risultati migliori durante questo episodio.

Episodio 6:

- Nonostante un miglioramento nell'efficienza, l'agente ha avuto tassi di successo nell'attacco compresi tra il 9% e il 13% e un reward complessivo sceso a 2890.
- Durante l'episodio 6 il difensore è riuscito a utilizzare contromisure più adeguate e arginare in modo più efficace la minaccia rispetto al precedente episodio.

Episodio 7:

- L'attaccante ha ottenuto un'efficacia notevole nell'attacco remoto, raggiungendo il 24% di successo, nonostante però il reward sia pressoché rimasto invariato (2804).
- L'attacco di connessione ha avuto un tasso di successo del 3%, mentre l'attacco locale è stato altamente efficiente (74%).

Episodio 8-20:

- Nel complesso, l'agente ha mostrato un'alternanza tra episodi di maggiore e minore efficienza nell'attacco, con alcuni tassi di successo più alti e altri inferiori, indicando un'interferenza variabile del difensore.
- L'attacco locale ha mantenuto una certa stabilità nel suo alto tasso di successo, mentre l'efficienza dell'attacco remoto e di connessione ha mostrato fluttuazioni.
- Nonostante alcuni picchi di successo, specialmente nell'attacco locale, la presenza del difensore sembra aver influenzato l'efficacia degli attacchi remoti e di connessione in modo più significativo.

L'analisi episodica mostra una variazione considerevole nelle prestazioni dell'agente. Anche se ha sperimentato picchi di successo, specialmente nell'attacco locale, la sua efficienza nell'attacco remoto e di connessione è stata più incostante suggerendo che la presenza di un difensore abbia influito sulle prestazioni dell'agente attaccante.

L'agente attaccante ha dimostrato una capacità di apprendimento e miglioramento, ma è evidente una maggiore difficoltà nell'ottenere buoni risultati, specialmente nelle azioni di attacco a distanza, indicando un'interferenza significativa del difensore.
Esaminiamo ora i risultati degli episodi relativi alla simulazione "Credential lookups" con la strategia $\epsilon - greedy$ implementata in un contesto di CSIRT con capillarità moderata. Questi risultati indicano l'efficacia e le dinamiche della strategia di apprendimento dell'agente.
Episodio 1:

- La strategia di esplorazione è stata utilizzata notevolmente, mostrando un basso tasso di successo in generale e un reward di 1297.
- I tipi di attacco "exploit" hanno ottenuto tassi di successo minimi e sono alcuni sono stati deflessi verso l'esplorazione.

Episodio 2:

- Persiste un uso massiccio della strategia di esplorazione, con bassi tassi di successo in entrambi gli attacchi e l'esplorazione, con un reward totale di 766.
- Anche in questo episodio, l'attacco "exploit" è stato spesso deviato verso l'esplorazione.

Episodio 3:

- Ancora prevalenza dell'esplorazione, con tassi di successo generalmente bassi e un reward di 1039.
- L'attacco "exploit" continua a essere deviato verso l'esplorazione.

Episodio 4:

- La strategia di esplorazione domina le azioni, con successo minimo negli attacchi e un reward di solo 508.
- L'attacco "exploit" viene deviato verso l'esplorazione in numerose occasioni.

Episodio 5:

- Utilizzo significativo della strategia di esplorazione, con scarsi risultati nei tentativi di attacco e un reward totale di 269.
- Gli attacchi vengono dirottati verso l'esplorazione in diverse istanze.

Episodio 6:

- L'esplorazione continua a essere l'opzione principale, con successo limitato negli attacchi e un conseguente reward di 250.
- Gli attacchi "exploit" sono spesso deflessi in esplorazione.

Episodio 7:

- Un leggero miglioramento nei punteggi totali, con una predominanza dell'esplorazione e un reward totale di 1897.
- Gli attacchi "exploit" vengono ancora deviati verso l'esplorazione.

Episodio 8-20:

- Persiste un trend di alto utilizzo della strategia di esplorazione con successo limitato negli attacchi, indicando una risposta difensiva efficace in termini di deviare gli attacchi verso azioni meno dannose.
- Il difensore sembra essere in grado di rilevare e neutralizzare gli attacchi effettuati, spingendo l'agente attaccante verso l'esplorazione.

I dati rivelano un uso massiccio della strategia di esplorazione $\epsilon - greedy$, con tassi di successo piuttosto bassi nei tentativi di attacco, suggerendo un efficace reazione difensiva nel ridurre l'impatto dell'agente attaccante. L'agente difensore sembra essere efficace nel contrastare gli attacchi e nel prevenire il raggiungimento dei loro obiettivi.
I dati evidenziano che il difensore ha un impatto significativo nell'impedire il successo degli attacchi. Gli attacchi "exploit" vengono spesso deviati verso l'esplorazione, indicando una difficoltà nell'ottenere successo nel contesto di questo ambiente di simulazione. La deviazione degli attacchi verso l'esplorazione mostra un'azione difensiva attiva che riduce l'efficacia e l'impatto dannoso degli attacchi dell'agente. L'efficacia del difensore emerge nell'indirizzare gli attacchi verso azioni meno dannose, limitando il danno complessivo che l'agente attaccante potrebbe infliggere.
Sulla base di questi dati, è plausibile affermare che un rafforzamento delle strategie difensive potrebbe ulteriormente ridurre l'efficacia degli attacchi e deviare l'agente attaccante verso azioni sempre più inoffensive.
In conclusione, i risultati dimostrano che l'intervento del difensore ha un impatto notevole nell'indebolire l'efficacia dell'agente attaccante, evidenziando una solida strategia difensiva che riduce l'impatto dei tentativi di attacco e orienta l'agente verso azioni meno dannose.

CSIRT altamente capillare

Esaminiamo ora l'esecuzione dell'algoritmo Deep Q-Learning (DQL) con un focus particolare sulle attività di un CSIRT (Computer Security Incident Response Team) classificato come "altamente capillare".
Episodio 1:

- Bassa efficienza generale nell'attuare con successo gli attacchi, sia in modalità esplorativa che di sfruttamento.

- Pochi attacchi hanno avuto successo, con una tendenza a deviare da strategie di sfruttamento a strategie esplorative ottenendo un reward totale di 252.

Episodio 2:

- I risultati mostrano una minima crescita nell'efficacia degli attacchi, ma ancora con una bassa percentuale di successo riuscendo a migliorare di poco il reward totale (254).
- Una parte degli attacchi è stata deviata da strategie di sfruttamento a strategie esplorative.

Episodio 3:

- Miglioramento significativo nell'efficacia degli attacchi esplorativi, con un tasso di successo più alto rispetto ai precedenti episodi e un reward totale di 1824.
- Gli attacchi exploit hanno mostrato una crescita leggera ma significativa.

Episodio 4:

- Un calo significativo nella performance generale degli attacchi rispetto all'episodio precedente arrivando al reward totale minimo di 145.
- Poche strategie di attacco hanno avuto successo e alcuni attacchi sono stati deviati da sfruttativi a esplorativi.

Episodio 5:

- Miglioramento significativo nell'efficacia di entrambe le modalità di attacco, sia esplorative che di sfruttamento portando il reward complessivo a 2020.
- Maggiore successo negli attacchi sfruttativi, con una variazione minore verso le strategie esplorative.

Episodio 6:

- Una performance mista con alcuni miglioramenti nell'efficacia degli attacchi, ma una diminuzione significativa del successo nel complesso abbassando il reward totale a 910.
- Un alto numero di strategie di attacco sono state deviate verso l'esplorazione rispetto allo sfruttamento.

Episodio 7:

- In questo episodio si riscontra un miglioramento rispetto al precedente, con un'efficacia crescente negli attacchi, specialmente quelli esplorativi e un reward totale di 1680.

- Tuttavia, persistono ancora deviazioni significative di strategie di sfruttamento verso l'esplorazione.

Episodio 8-20:

- La tendenza generale mostra fluttuazioni nella performance degli attacchi.
- Anche se ci sono stati alcuni miglioramenti, la deviazione di strategie di attacco dallo sfruttamento all'esplorazione è stata significativa, influenzando il successo complessivo degli attacchi.

Gli attacchi subiscono un'interferenza costante e significativa da parte del difensore, con una deviazione frequente delle strategie di attacco dallo sfruttamento all'esplorazione. L'interferenza del difensore ha compromesso l'efficacia degli attacchi, con un notevole impatto sulla riuscita degli stessi, come raffigurato in figura 4.5.

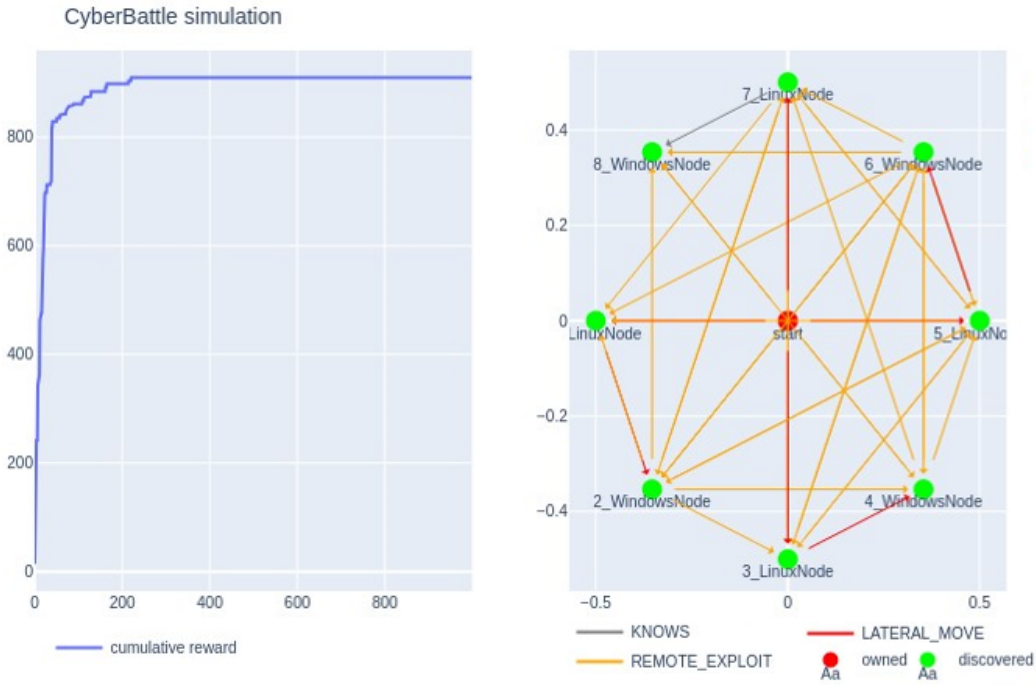

Figura 4.5: Propagazione della minaccia in caso di CSIRT altamente capillare

Nonostante alcuni episodi abbiano mostrato miglioramenti da parte dell'attaccante, le deviazioni causate dal difensore hanno influito positivamente sul successo complessivo degli attacchi (riducendone l'efficacia e la propagazione).
L'azione difensiva ha creato ostacoli significativi per l'efficacia generale degli attacchi, costringendo l'agente attaccante a modificare costantemente le strategie.
L'intervento del difensore ha influenzato pesantemente gli attacchi, deviando continuamente le strategie di attacco da sfruttamento a esplorazione. Questa interferenza ha ridotto notevolmente il successo complessivo degli attacchi.
L'analisi successiva si focalizza sull'addestramento di un agente in un ambiente

simulato denominato "Exploiting DQL (CSIRT altamente capillare)" per valutare le prestazioni dell'agente nei vari tipi di esplorazione ed exploit. Vediamo di seguito un'analisi più dettagliata di alcuni episodi.
Episodio 1:

- Il success rate è complessivamente basso in esplorazione remota e di connessione, con un 32% in sfruttamento locale.
- Gli exploit remoti e di connessione mostrano diversi tassi di successo 30% e 3% rispettivamente.
- Ciononostante il reward complessivo è ci 2988 ed è da considerarsi abbastanza elevato.

Episodio 2:

- Miglioramento generale del tasso di successo, soprattutto nell'exploit remoto (39%) rispetto all'esplorazione (25%) ottenendo un reward totale di 2842.
- Anche se l'exploit remoto ha mostrato un miglioramento, potrebbe essere dovuto a una difesa più debole in questo episodio.
- Gli exploit di connessione rimangono bassi (4%).

Episodio 3:

- Anche in questo episodio si riscontrano elevati successi negli exploit remoti e di connessione (58% e 4%), con miglioramenti nell'exploit locale (28%).
- Il reward complessivo è migliorato rispetto all'episodio precedente (3974).
- L'exploit di connessione rimane basso, indicando una difesa efficace in quest'area.

Episodio 4:

- Il tasso di successo è complessivamente basso, tranne per l'exploit locale (47%).
- Gli exploit remoti e di connessione mostrano bassi tassi di successo (33% e 1%).
- Il reward complessivo ottenuto è inferiore ai precedenti episodi (1518) e il difendente sembra contrastare efficacemente l'exploit di connessione.

Episodio 5:

- Esplorazione con tassi di successo variabili. Miglioramento nell'exploit remoto (40%) il quale però non si traduce in un reward totale più elevato (1476) evidenziando un miglioramento della strategia del difensore.
- Il tasso di successo degli exploit di connessione rimane basso (1%).

Episodio 6:

- Success rate bassi in tutte le modalità di esplorazione ed exploit, tranne un leggero miglioramento nell'exploit remoto (2%).
- le strategie del difendente continuano a migliorare consentendo all'attaccante di ottenere un reward di 898.

Episodio 7:

- Miglioramento della percentuale di successo dell'exploit locale (25%), indicando possibili punti deboli nella difesa e traducendosi in un reward complessivo di 2426.
- La percentuale di successo dell'exploit remoto e di connessione rimane modesta (6% e 15%).

Episodio 8-20:

- Risultati altamente variabili. Fluttuazioni evidenti nei tassi di successo dell'exploit e dell'esplorazione.
- Miglioramenti in alcune sessioni, mentre altre mostrano tassi di successo costantemente bassi.
- I miglioramenti, in particolare nell'exploit remoto, possono indicare aree in cui la difesa potrebbe essere rafforzata.

I risultati indicano che il difensore sembra efficace nel contrastare gli attacchi in determinate modalità. Tuttavia, sono presenti punti deboli, specialmente nell'exploit di connessione.
L'agente attaccante mostra una significativa variazione nelle prestazioni tra i vari episodi. Sebbene siano presenti miglioramenti in alcuni aspetti, come l'exploit remoto e locale in alcuni casi, i bassi tassi di successo dell'exploit di connessione e le fluttuazioni generali suggeriscono una notevole instabilità nelle prestazioni dovuta a un efficace intervento del difendente.
Le fluttuazioni nelle prestazioni suggeriscono un'adattabilità variabile della difesa alle diverse tipologie di attacchi. Miglioramenti in alcune sessioni, soprattutto nell'exploit remoto, possono indicare la necessità di rafforzare la difesa in altre modalità di attacco. Valutare questi dati potrebbe fornire indicazioni utili per potenziare la difesa contro gli exploit e garantire una maggiore coerenza nell'efficacia difensiva.
Esaminiamo ora i risultati degli episodi relativi alla simulazione "Credential lookups" con la strategia $\epsilon - greedy$ implementata in un contesto di CSIRT altamente capillare. Questi risultati indicano l'efficacia e le dinamiche della strategia di apprendimento dell'agente.

Episodio 1:

- Basso rendimento complessivo, con tassi di successo molto limitati in tutte le modalità di esplorazione e sfruttamento con un reward di 250.
- Gli exploit sono stati deviati all'esplorazione in 9 casi.

Episodio 2:

- Un miglioramento leggero nelle prestazioni generali con un reward totale di 387.
- Il tasso di successo rimane basso, con ulteriori 26 exploit deviati all'esplorazione.

Episodio 3:

- Rendimento inferiore rispetto all'episodio precedente con un reward totale di 267.
- Ulteriori 54 exploit sono stati deviati all'esplorazione.

Episodio 4:

- Un picco nel rendimento dell'attaccante (reward di 517), con una maggiore percentuale di exploit deviati all'esplorazione (67 casi).

Episodio 5:

- Miglioramento significativo rispetto agli episodi precedenti con un reward di 620.
- Tuttavia, 42 exploit sono stati deviati all'esplorazione.

Episodio 6:

- Riduzione del rendimento con un reward totale di 250 e con 41 exploit deviati all'esplorazione.

Episodio 7:

- Notevole miglioramento rispetto all'episodio precedente (reward totale di 502), ma con 51 exploit deviati all'esplorazione.

Episodio 8-20:

- Rendimento altalenante con diverse fluttuazioni nei successi dell'agente.
- Gli exploit deviati all'esplorazione rimangono un problema costante.

L'analisi degli episodi evidenzia una variabilità significativa nelle prestazioni del sistema di agenti di ricerca delle credenziali, con rendimenti altalenanti in diverse fasi. Nonostante alcuni miglioramenti in alcuni episodi, i tassi di successo rimangono complessivamente bassi in tutte le modalità di esplorazione e sfruttamento. Inoltre, il sistema sembra costantemente deviare gli exploit verso l'esplorazione anziché l'utilizzo efficace, suggerendo una difesa efficace o un meccanismo di deviazione degli attacchi. Nonostante l'agente tenti ripetutamente di sfruttare le vulnerabilità, i risultati mostrano che l'agente difendente riesce a prevenire la maggior parte degli attacchi con una deviazione sistematica degli exploit verso l'esplorazione.
L'analisi dei dati rivela che il sistema difensivo impiegato ha dimostrato un'efficacia notevole nel prevenire gli attacchi dell'agente. La deviazione costante degli exploit verso l'esplorazione indica un'azione difensiva robusta che riduce significativamente il successo degli attacchi effettuati dall'agente. Ciò suggerisce un'adeguata capacità difensiva nel contrastare gli attacchi mirati alle vulnerabilità, impedendo all'agente di sfruttarle con successo. Tuttavia, nonostante l'apparente efficacia del sistema difensivo, potrebbe essere utile esplorare ulteriori strategie difensive per consolidare ulteriormente la protezione contro attacchi più sofisticati o per adattarsi a nuove tecniche utilizzate dall'agente nel tentativo di evitare la deviazione degli exploit.

4.1.1 Spunti per prove successive

Aumentare il numero di episodi e iterazioni potrebbe consentire all'agente di apprendere ulteriormente.
Testare diverse strategie di esplorazione, come l'uso di politiche di esplorazione diverse da $\epsilon - greedy$, potrebbe essere utile per migliorare le prestazioni dell'attaccante e trovare di conseguenza nuove sfide per l'agente difendente.
L'aggiustamento delle dimensioni della rete o degli iperparametri potrebbe influire sulle capacità dell'agente attaccante nel trovare credenziali, creando scenari più complessi per il difendente.
L'incorporazione di conoscenze esterne o la generazione di dati sintetici per l'addestramento potrebbe essere considerata per migliorare le prestazioni dell'agente attaccante nella ricerca di credenziali portando il difensore a dover fronteggiare uno scenario più complesso.
Modellare la rete in maniera più complessa, rispetto allo schema semplicistico usato da CyberBattleSim, potrebbe aumentare la qualità e la rappresentatività della simulazione rendendola di fatto applicabile a scenari più realistici o addirittura esistenti.

Capitolo 5

Discussione dei risultati e conclusioni

Nell'approfondire l'importante ruolo del CSIRT nell'ambito della sicurezza informatica e nella gestione della propagazione delle minacce, emerge con chiarezza l'impatto significativo derivante dalla presenza di un Computer Security Incident Response Team (CSIRT) nell'ambiente di un'infrastruttura. Questa osservazione rivela una distinzione marcata ed evidente tra la propagazione delle minacce in assenza di intervento da parte del CSIRT e l'effetto dell'introduzione di un tale team.
In un contesto privo di intervento da parte del CSIRT, le minacce si diffondono più liberamente, determinando impatti più gravi sia sui servizi che sulla sicurezza dell'infrastruttura. Al contrario, l'introduzione di un CSIRT, anche a livelli di capillarità minima o moderata, mostra un'influenza positiva nel mitigare tali minacce, seppur con differenze non sostanziali tra questi due livelli. Andando a guardare

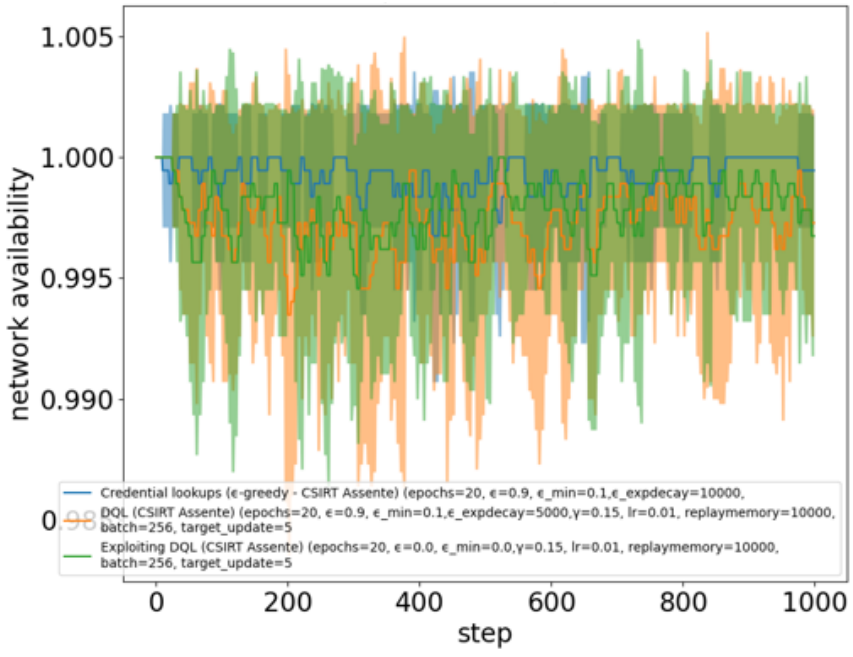

Figura 5.1: Network availability (CSIRT poco capillare)

la figura 5.1, per quanto riguarda un CSIRT Minimo e la figura 5.2 per quanto riguarda un CSIRT a elevata capillarità, possiamo notare come la disponibilità della rete (`Network Availability`) abbia un andamento altalenante rispetto a uno quasi

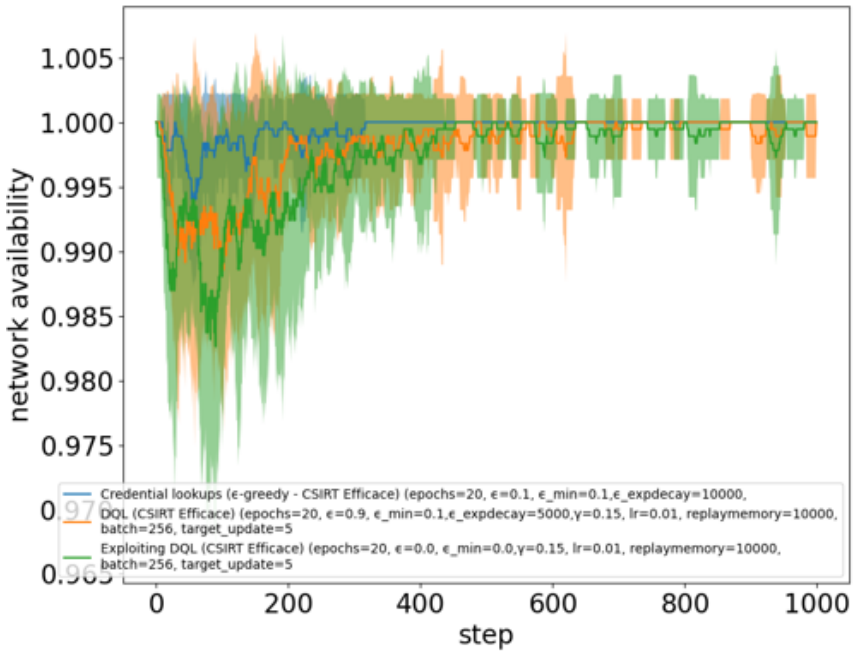

Figura 5.2: Network availability (CSIRT altamente capillare)

costante nel secondo caso. Questo indica che uno CSIRT altamente capillare riesce a mantenere un alto livello di disponibilità della rete durante tutta la fase di attacco andando a contrastare in maniera più efficace le mosse dell'attaccante rispetto a uno CSIRT poco capillare.

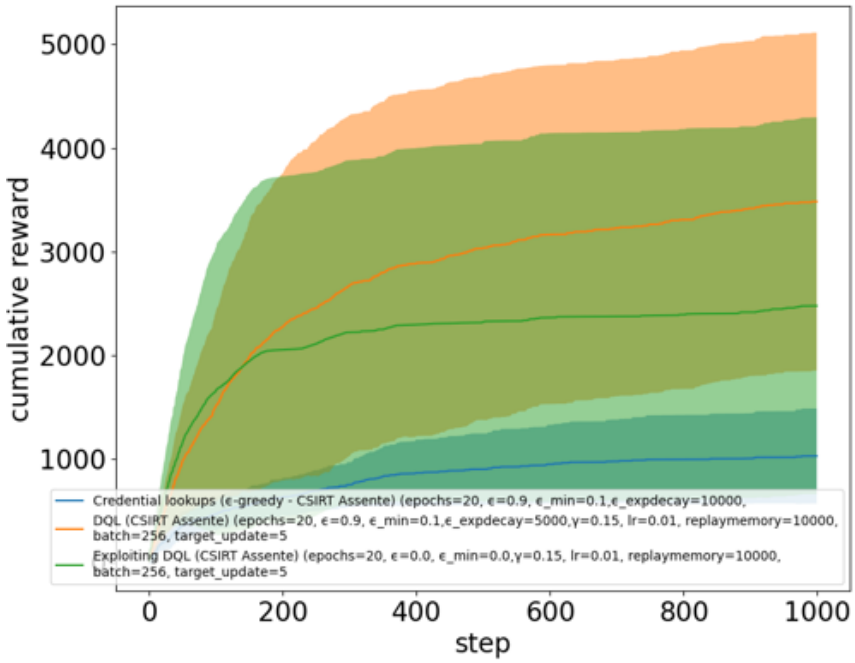

Figura 5.3: Cumulative reward (CSIRT poco capillare)

Allo stesso modo, andando a confrontare la figura 5.3, la quale illustra il guadagno

cumulativo dell'attaccante (`Cumulative Reward`) ai danni di uno CSIRT poco capillare, con la figura 5.4, facente invece riferimento a un CSIRT altamente capillare, possiamo notare come nel secondo caso (CSIRT altamente capillare) l'attaccante faccia molta più fatica a ottenere delle ricompense maggiori rispetto al primo caso (CSIRT poco capillare), indicando anche in questa occasione una protezione maggiore della rete e una difesa più efficace da parte di uno CSIRT con capillarità elevata.

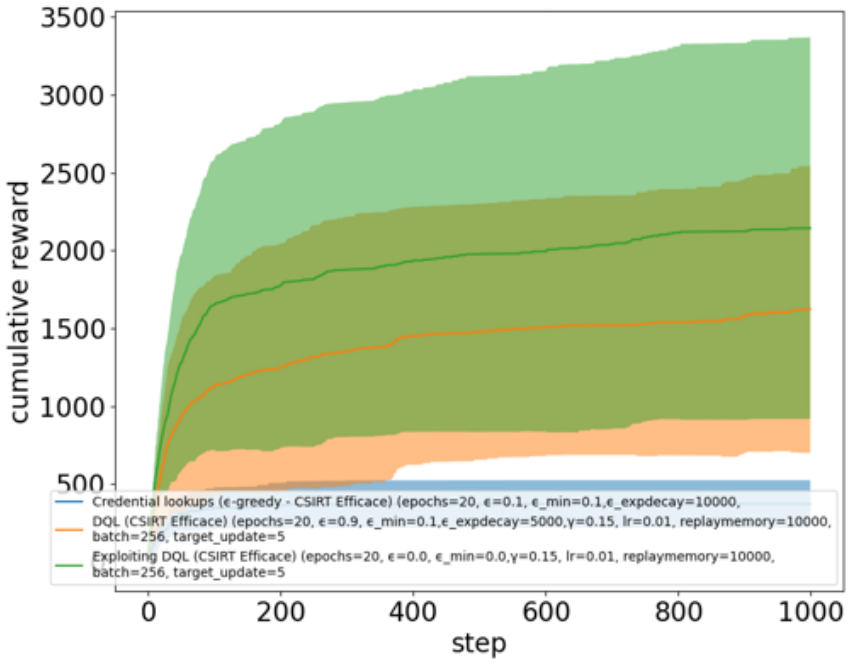

Figura 5.4: Cumulative reward (CSIRT altamente capillare)

Pertanto, sebbene sussistano differenze minori tra i primi due livelli di efficienza (CSIRT poco capillare e CSIRT moderatamente capillare), è con uno CSIRT a elevata capillarità che si osserva una distinzione sostanziale, come chiaramente evidenziato in figura 5.5. In questo scenario, l'efficacia nell'affrontare le minacce è notevolmente superiore (il reward ottenuto dall'attaccante risulta molto inferiore), fornendo un livello di sicurezza che si distingue nettamente rispetto agli altri livelli di capillarità del CSIRT indipendentemente dalla tipologia di attacco utilizzata (Figura 5.6). È in questa variazione di efficacia che si rileva una chiara distinzione nella protezione e nel contrasto delle minacce informatiche.
La decisione di implementare un particolare livello di capillarità del CSIRT deve essere ponderata attentamente, considerando la natura e il valore della constituency che si intende proteggere. Livelli più elevati di capillarità ed efficienza richiedono risorse finanziarie considerevoli e devono essere bilanciati dal valore economico e dall'importanza della constituency. Una constituency ad alto valore economico potrebbe richiedere uno CSIRT altamente capillare ed efficace, giustificando l'investimento per garantire un livello superiore di sicurezza.

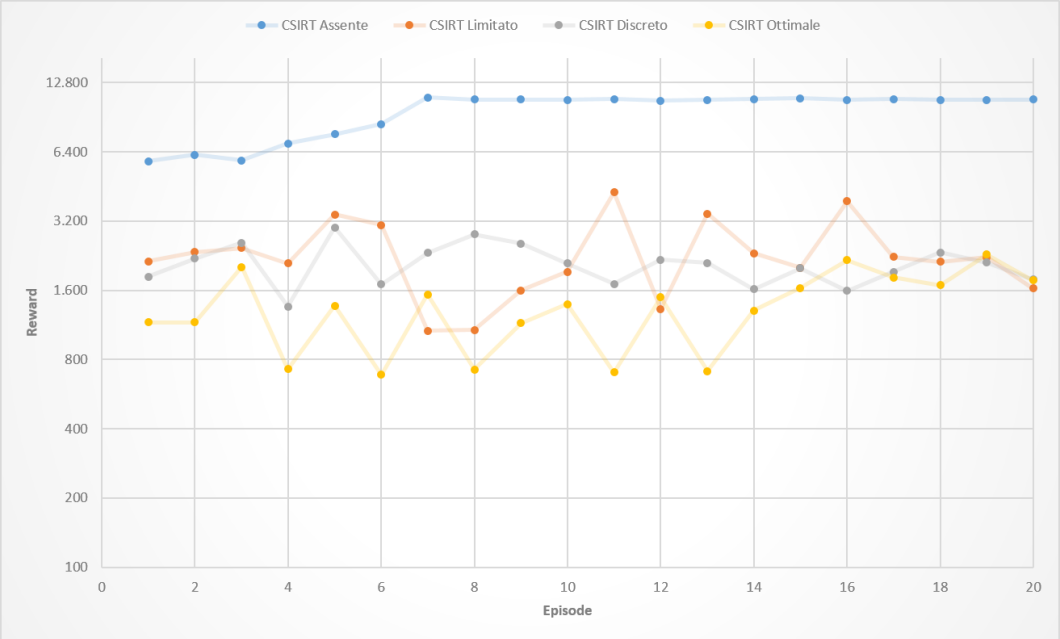

Figura 5.5: Cumulative reward ottenuto dall'attaccante

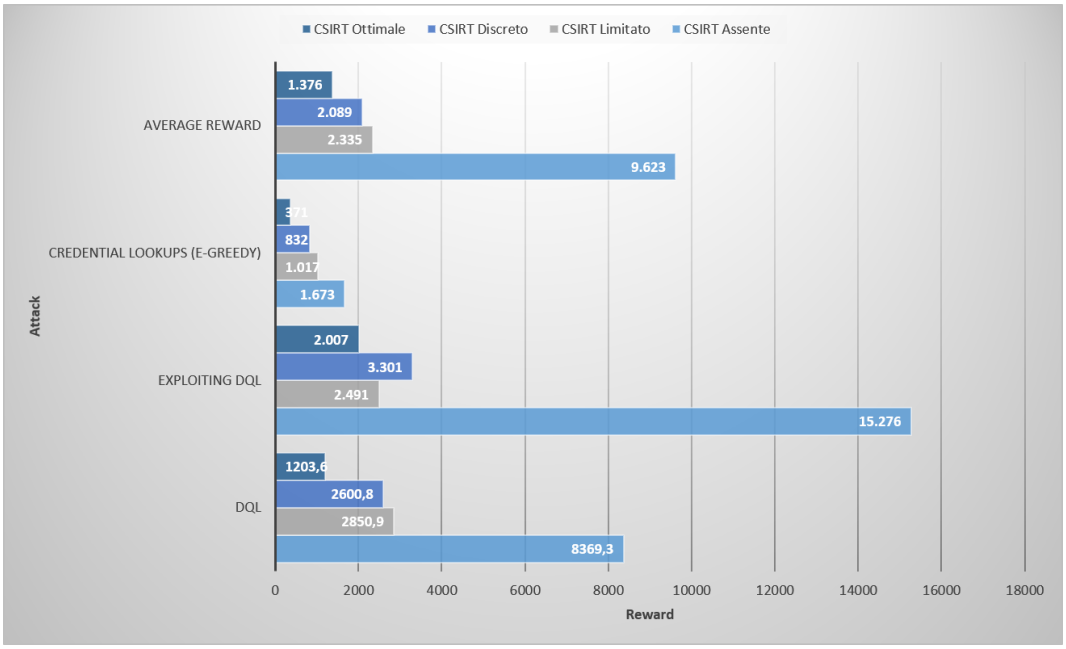

Figura 5.6: Reward ottenuto nelle tre tipologie di attacco

In conclusione, la presenza di un CSIRT in qualsiasi forma si rivela cruciale per la sicurezza informatica. Tuttavia, la decisione sul livello di capillarità ed efficienza del CSIRT deve considerare attentamente la relazione tra il livello di sicurezza garantito e le risorse economiche disponibili, bilanciando l'efficacia con la sostenibilità finanziaria.

5.1 Sviluppi futuri

Sulla base dei risultati e delle osservazioni ottenute dalle simulazioni precedenti, ci sono diversi spunti per ulteriori prove successive nell'addestramento dell'agente DQL in un contesto di sicurezza informatica. Di seguito vengono elencate alcune idee con le quali proseguire lavori futuri:

1. Variazione nei parametri di apprendimento: Modificare i parametri di addestramento come il tasso di apprendimento (learning rate) o il fattore di sconto (gamma) per valutare l'impatto sulle prestazioni dell'agente. Un tuning adeguato dei parametri può influenzare significativamente l'apprendimento dell'attaccante rendendolo un antagonista più difficile da gestire per l'agente difendente.

2. Esplorazione di diverse architetture di rete: Testare diverse architetture di rete per l'agente DQL, come reti neurali convoluzionali (CNN) o reti neurali ricorrenti (RNN), per valutare se alcune strutture neurali sono più adatte per le sfide specifiche della sicurezza informatica.

3. Aumento della complessità dell'ambiente: Introdurre ambienti più complessi e realistici con una maggiore varietà di azioni e scenari di attacco. Ciò aiuta a migliorare l'abilità dell'agente nel gestire situazioni più realistiche.

4. Esplorazione di algoritmi di apprendimento alternativi: Prove con altri algoritmi di apprendimento automatico come PPO (Proximal Policy Optimization), A3C (Asynchronous Advantage Actor-Critic), o algoritmi di apprendimento profondo multi-agente (MARL) per valutare le loro prestazioni nel contesto della sicurezza informatica.

5. Sfide di avversarial training: Introdurre sfide di addestramento avversarial in cui agenti avversari cercano di violare il sistema difeso da un agente DQL. Questo testerebbe la robustezza delle strategie di difesa dell'agente.

6. Monitoraggio delle violazioni di sicurezza: Introdurre una componente di monitoraggio in modo che l'agente debba anche rilevare e reagire alle violazioni di sicurezza nel sistema. Questo rappresenterebbe una sfida realistica per l'agente.

7. Esplorazione dell'interpretabilità: Studiare metodi per rendere l'agente DQL più interpretabile, in modo che le sue decisioni siano comprensibili agli esperti di sicurezza informatica.

8. Introduzione di nuove metriche di valutazione: Definire metriche di valutazione aggiuntive che tengano conto della complessità e delle specificità della sicurezza informatica, oltre alla semplice ricompensa.

9. Esplorazione di nuove strategie di sfruttamento: Sviluppare nuove strategie di sfruttamento basate su informazioni rilevanti per la sicurezza informatica come l'analisi comportamentale degli attaccanti.

10. Sviluppo di un interfaccia grafica che permetta la modellazione della rete e la modifica degli iperparametri dell'agente attaccante e del difendente, in modo che sia possibile l'utilizzo del software di simulazione anche a utenti meno esperti.

Questi spunti offrono molte opportunità per ulteriori ricerche e sperimentazioni nell'ambito dell'apprendimento automatico per la sicurezza informatica. La combinazione di questi approcci potrebbe portare a un notevole miglioramento nella capacità di difesa dei sistemi informatici da parte degli agenti intelligenti.

Bibliografia

[1] Microsoft Defender Research Team. Cyberbattlesim. https://github.com/microsoft/cyberbattlesim, 2021. Created by Christian Seifert, Michael Betser, William Blum, James Bono, Kate Farris, Emily Goren, Justin Grana, Kristian Holsheimer, Brandon Marken, Joshua Neil, Nicole Nichols, Jugal Parikh, Haoran Wei.

[2] Ministero della Giustizia. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, dpcm 24 gennaio 2013. *GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA*, 3 2013.

[3] Ministero della Giustizia. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. *GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA*, 87, 4 2017.

[4] CISR. Comitato interministeriale per la sicurezza della repubblica. https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/comitato-interministeriale-per-la-sicurezza-della-repubblica-cisr.html, 2023. Accesso il 14 novembre 2023.

[5] DIS. Dipartimento delle informazioni per la sicurezza. https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html, 2023. Accesso il 14 novembre 2023.

[6] NCS. Nucleo per la cybersicurezza. https://www.acn.gov.it/agenzia/coordinamento-interministeriale, 2023. Accesso il 14 novembre 2023.

[7] CNAIPIC. Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche. https://www.interno.gov.it/it/temi/sicurezza/crimine-informatico/centro-nazionale-anticrimine-informatico-protezione-infrastrutture-critiche-cnaipic, 2020. Accesso il 14 novembre 2023.

[8] COR. Comando per le operazioni in rete. https://www.difesa.it/SMD_/COR/Pagine/default.aspx, 2021. Accesso il 14 novembre 2023.

[9] CERT-Difesa. Computer emergency response team del ministero della difesa. https://www.difesa.it/SMD_/COR/Pagine/CERT_Difesa.aspx, 2021. Accesso il 14 novembre 2023.

[10] Ministero della Giustizia. Attuazione della direttiva (ue) 2016/1148 del parlamento europeo e del consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'unione. *GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA*, 132, 6 2018.

[11] CERT-AgID. Computer emergency response team dell'agenzia per l'italia digitale. `https://cert-agid.gov.it/chi-siamo/`, 2020. Accesso il 14 novembre 2023.

[12] Ministero della Giustizia. Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - csirt italiano. *GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA*, 262, 11 2019.

[13] ENISA. NIS Directive and national CSIRTs, Info Note, February 2016.

[14] Ministero della Giustizia. Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. *GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA*, 222, 9 2019.

[15] ENISA. Csirts by country - interactive map. `https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map`, 2020. Accesso il 14 novembre 2023.

[16] ENISA. Un approccio graduale alla creazione di un CSIRT, 2006.

[17] West-Brown Moira J, Stikvoort Don, Kossakowski Klaus-Peter, Killcrece Georgia, Ruefle Robin, and Zajicek Mark. Handbook for Computer Security Incident Response Teams (CSIRTs). *SOFTWARE ENGINEERING INSTITUTE CARNEGIE MELLON UNIVERSITY*, 4 2003.

[18] Killcrece Georgia, Kossakowski Klaus-Peter, Ruefle Robin, and Zajicek Mark. Organizational models for computer security incident response teams (csirts), 12 2003.

[19] Jutta Breyer, Rocco Defina, Terry Hook, Frédéric Lau, Riccardo Scquizzato, and Clare Thornley. CWA16458, European ICT professionals role profiles - Part 1: 30 ICT profiles. *COMITÉ EUROPÉEN DE NORMALISATION*, 2018.

[20] Gallotti Cesare and Guasconi Fabio. Certificazioni professionali in sicurezza informatica 2.0. *QUADERNI CLUSIT*, 6 2013.

[21] ENISA. Baseline capabilities for National / Governmental CERTs, Part 1, Version 1.0 (initial draft), 2009.

[22] ENISA. Baseline Capabilities of National / Governmental CERTs, Part 2: Policy Recommendations, Version 1.0 (initial draft), 2010.

[23] ENISA and Andrea Dufkova. ENISA's recommendations on baseline capabilities, Update, December 2014.

[24] AGiD. Misure minime di sicurezza ict per le pubbliche amministrazioni, 2016.

Ringraziamenti

Mi è doveroso dedicare questo spazio del mio elaborato alle persone che hanno contribuito, con il loro instancabile supporto, alla realizzazione dello stesso e senza le quali questo lavoro di tesi non esisterebbe nemmeno.
In primis, un ringraziamento speciale al mio relatore Prof. Marco Baldi, al mio correlatore Prof. Luca Spalazzi e al Dott. Lorenzo Principi, per la loro immensa pazienza, per i loro indispensabili consigli e per le conoscenze trasmesse durante tutto il percorso di stesura dell'elaborato. Grazie per avermi permesso di lavorare a un progetto avvincente e interessante come questo, a cui ho avuto la fortuna di poter partecipare e contribuire. Grazie a voi aggiungo un nuovo capitolo a un già ricco bagaglio di conoscenze e competenze del mio percorso magistrale.
Ringrazio infinitamente mia madre che mi ha sempre sostenuto, appoggiando ogni mia decisione, dalla scelta del mio percorso di studi, non sempre facile e in discesa come pensavo, alla scelta di andare per ben due volte a studiare all'estero e anche alle più banali scelte amorose o di vestiario. Grazie anche per essermi venuta a trovare a Cracovia e per aver capito il mio desiderio di condividere una tale bellezza con qualcuno della mia famiglia.
Ringrazio anche mio padre per avermi trasmesso la sua passione in ogni lavoro e progetto dal più piccolo e umile al più grande mai fatto insieme.
Senza di voi, sicuramente non ci sarei io e soprattutto non sarei diventato la persona che sono oggi.
Ringrazio anche mio fratello Davide, bomber e capitano della futsal Amici84 (così dicono) e, che dir se ne voglia, anche se a volte finiamo in cagnara (quasi sempre meno), ti voglio un mondo di bene e ogni giorno mi ricordi quanto sia bello condividere quasi tutto con un fratello, dalle partite di calcetto/otto a quelle alla PlayStation in cui il Goblino supremo ancora skilla quando ha le mani montate al verso giusto (per poi passare a momenti di Giorgino power), passando per un'infanzia piena di ricordi insieme.
Ringrazio poi i miei zii e i miei cugini, Noemi, Nicholas, Martina, Emanuele e Maria Chiara, perché "nu sette" insieme, ne potremmo raccontare all'infinito tra campagna, casa di nonna, natali, cene, capodanni, pasque e festività di qualsiasi religione etnia e cultura, purché si magni bé. Sono immensamente felice e fiero di poter vantare di una famiglia così grande e così unita, nella quale siamo cresciuti insieme. Ah sì, aggiungo anche il cugino acquisito Stefano, dal quale apprendo ogni giorno nuove nozioni agrarie e sulle difficoltà nella coltivazione dei fagiolini e della produzione del vino; "me sa che te tocca insegnarmi un po' di più e nello specifico a breve". Spero

qualsiasi cosa accada di non perdervi mai.
Infine ringrazio i miei nonni, Pio e Alessandro, anche se non ci sono più, e le mie nonne, Quirina e Paola e per avermi viziato e voluto bene come solo i nonni sanno fare. Grazie nonna Paola per avermi mostrato ogni giorno la pacatezza, la calma e la pazienza che solo tu hai. Grazie nonna Rina per avermi cresciuto in campagna, tra tutti i cugini e i parenti più stretti, per avermi mostrato quanto è bello passare il tempo in famiglia, quanto è bello viaggiare (in Crociera e in Polonia) e grazie soprattutto per farci ridere e mangiare tutti insieme a ogni festività o ricorrenza che sia. Siete e sarete sempre una delle cose più preziose che ho.
Passiamo ora a ringraziare la mia seconda famiglia, persone con le quali trascorro la maggior parte del mio tempo quando non sono tra le quattro mura domestiche. Vorrei esprimere la mia profonda gratitudine alla persona straordinaria che è la mia ragazza. Grazie per essere stata al mio fianco durante questo lungo e impegnativo percorso di studio chiamato Magistrale. Hai rappresentato una fonte inesauribile di supporto, comprensione e amore, anche se ogni volta che gioca il Milan o qualche derby finisce sempre in cagnara. Senza il tuo sostegno costante, non avrei mai potuto completare questa tesi. La tua pazienza, gentilezza e incoraggiamento sono stati i miei pilastri in ogni momento di dubbio e fatica anche quando ero a chilometri e chilometri di distanza. Questo traguardo è anche tuo, e non posso che ringraziarti per aver reso questo viaggio così speciale. Grazie, amore mio. Se riesci anche a fare qualche goal con quell'8 sulle spalle sarebbe perfetto, così diamo un senso a cicciabellabomber.
Simone, ti ringrazio ogni giorno per la semplicità che mi dimostri in ogni cosa, per me sei una sorta di fratello maggiore dal quale cerco di carpire il più possibile. Su una cosa resterò intransigente, l'amore per la Samb lo lascio tutto a te, per carità. A breve in compenso possiamo organizzare qualche sciatina nei dintorni o qualche missione di recupero e bonifica di ordigni esplosivi.
Arianna, la tua amicizia è dolce e inaspettata, sempre presente nei momenti più belli e importanti. Purtroppo anche tu sei sul lato sbagliato di Milano, d'altronde tu e Aurora vi somigliate in molte cose e vi completate nelle rimanenti. Come un buon vino, ma anche con molto buon vino, la vostra e la nostra amicizia è migliorata con il tempo, raggiungendo sfumature che solo il tempo può creare. L'amore che tu e Simone avete per Maya e Whisky, così come per il buon cibo e vino, rispecchiano la vostra anima gentile. Anche se, tra due derby opposti, il nostro legame è il vero trionfo in questa partita chiamata amicizia.
Elise, grazie per la tua forza e determinazione marchio di fabbrica evidente a chiunque ti veda lottare sul campo. Il tuo impegno che metti nel calcetto, dove ti ho visto migliorare tantissimo rispetto ai primi anni e nel tennis è ispirante, ma è la tua tenacia nella vita che mi insegna a lottare. La tua amicizia è come ogni partita che abbiamo giocato, sempre piena di passione e grinta, anche dopo un espulsione. Grazie di cuore.
Chiara, la tua forza è un faro di ispirazione che guida i pescatori al rientro a casa.

Affrontare un intervento al crociato e ancora intraprendere il Cammino di Santiago dimostra il tuo coraggio senza limiti, o forse anche un briciolo di follia. Come il cammino stesso, la tua vita è un viaggio straordinario e coraggioso. Grazie per aver compreso il mio desiderio di tornare a Cracovia e di condividere la tua forza con tutti noi. Spero di rivederti presto.
Chiara Bertolda, grazie per esserti sempre informata sul mio avanzamento della tesi e nello studio, abbiamo condiviso la sofferenza e la crociata contro l'università italiana, spero che anche tu potrai presto provare le stesse emozioni che sto vivendo io in questi giorni.
Meli, una delle prime amiche che Aurora mi ha presentato in un pomeriggio afoso al Vela Club, ti è bastato il tempo di una pausa dal lavoro per capirmi e approvarmi: "sappiamo tutti che era un test", fortunatamente l'ho superato.
Ramona e Davide, capitano e mister grazie per essere guide di passione e forza nel mondo del calcetto. Ramona, la tua leadership silenziosa ispira la squadra con il tuo impegno, nonostante la tenuta fisica di Alexander Pato ai tempi d'oro. A fine anno ti mando le fatture delle varie farmacie e studi specialistici che ho dovuto visitare per essere diventato il vostro tifoso numero 1. Siete da infarto. Davide, il tuo talento come allenatore trasmette passione e insegnamenti preziosi anche a chi il campo lo vede solo con il fischietto sulla bocca e i cartellini in tasca. Per ora ci siamo incontrati solo a Castignano, con un freddo record e un campo pietoso. Spero di poterti arbitrare nuovamente, perché sul 15-2 c'è poco da dire a un arbitro, sono stato letteralmente uno spettatore. Insieme, siete un vero esempio di dedizione e forza, potrei ascoltarvi le ore a parlare di episodi di campo o di vita quotidiana. Grazie per tutto quello che fate. "Mo vogghie vede ssu furne quann me lu facet vedè all'opra".
Un grazie di cuore ai mie colleghi Elia, Riccardo, Paolo, Nicola e Simone, con alcuni di voi ho condiviso quasi l'intero percorso universitario (tranne le due fughe in Polonia) e con altri uno o più anni della triennale e della magistrale. Ho voluto scrivere colleghi perché fa molto figo, se scrivevo compagni di avventure, di esami, di disperazione, di Mimmo, di "non so se", di MPRAI e anni di fuoricorso avrei sminuito quella che è la nostra amicizia e la nostra esperienza in ambito ingegneristico. È grazie a voi che ho superato i momenti, gli esami (tranne quelli che ho fatto in Polonia per ben due volte) e i progetti più difficili. Senza voi e i vostri consigli, non so come e quando ce l'avrei fatta.
Rimanendo sul settore maschile dei ringraziamenti, volevo dedicare due parole ai nuovi arrivati nella mia vita. Per primi impossibile non nominare i quattro moschettieri. Non sapete la gioia, di avervi avuto per sei mesi incredibili a Cracovia. Mattia, il mio coinquilino, solo noi sappiamo cosa significa vivere 6 mesi in ulica Mazowiecka piętnaście, dom trzynaście. Grazie per essere venuto a trovarmi anche durante la mia seconda avventura polacca. Madonna che delirio e quanti ricordi, inutile elencarli tutti anche perché almeno il 90% di questi andrebbero censurati. Sei stato un signor coinquilino.

Matte, il mio clone, grazie per tutto, per essere un punto di confronto fisso, visto soprattutto la tua somiglianza caratteriale. A tal punto da seguirmi nella mia folle avventura di ritorno a Cracovia. Non sarà mai stata selvaggia e delirante come la prima ma è davvero qualcosa di unicamente nostro. Non nascondo che a volte è stato difficile passare davvero tutto sto tempo insieme, forse ero preoccupato di cancellare qualche vecchio ricordo cercando di emulare i quattro moschettieri o forse eravamo davvero troppo cresciuti per alcune cose. Alla fine non era poi così male starsene sul divano di Plac Nowy e vedere ininterrottamente episodi di The Office finché uno dei due non crollava, eravamo felici e andava bene così, nonostante tutte le difficoltà che la distanza e la nostra età evidenziavano ogni giorno ci siamo sempre tirati su il morale nei giorni tristi e ne siamo usciti con un nuovo capitolo da aggiungere alla voce Cracovia.
Michael, Maicol, Mike, Miché o che dir si voglia, lu pescià (in realtà "quill de sant'Annna"), il primo a incontrare sul volo alla partenza che mi si presentò cercandomi di spiegare da dove venisse non sapendo che all'aeroporto di Pescara, proveniente da Ancona, ci fosse nientemeno che "n'Ascula". Capito questo è stato un attimo a presentarsi come il ragazzo di Sant'Anna, nemmeno di Centobuchi perché chi è della zona conosce la differenza. Serve aggiungere altro? Compagno di allenamenti e di stempie e di qualche calcetto. Non ti ringrazierò mai abbastanza per avermi invitato all'ultimo calcetto che abbiamo fatto insieme.
Sappiamo tutti che continueremo a rivederci e scriverci su WhatsApp, non ci ha fermato un lockdown figurati un pochino di distanza, prossima tappa Istanbul da Osman a farci il trapianto.
Ringrazio poi l'altro settore di Cracovia, quello sportivo e quello del secondo semestre. Grazie Janek, non so nemmeno se verrai alla festa o se riuscirò a venirti a trovare di nuovo, chissà forse ti starò traducendo queste righe o forse te le girerò WhatsaApp già tradotte. Ti volevo ringraziare innanzitutto per avermi dato una casa, per chi non lo sapesse proprio "Gianekko" è stato l'unico capace di soddisfare tutte le richieste abitative di due Chef italiani i quali avevano settato un'asticella abbastanza elevata che ha reso la ricerca dell'appartamento quasi un'impresa impossibile. Ma soprattutto grazie per l'altra casa che mi hai trovato, quella in cui sono stato accolto fin da subito e che può essere sostituita con la parola famiglia. Mi hai visto un giorno in tram con il borsone e le scarpe da calcetto e mi hai subito chiesto di giocare per la squadra della tua città. Ebbene si, un portiere italiano della Politechnika Krakowska ha vestito la maglia numero 6 del Sygnał Włosienica. Non avevo minimamente capito che giocavi a calcio fuori da Cracovia in un paesino vicino Oświęcim (città nota per altri campi) ma l'ho capito subito la prima volta quando abbiamo preso il pullman per andare a giocare "in casa". Grazie per avermi accolto a casa tua, presentato la tua famiglia, invitato a cena, alla festa dell'Ochotnicza straż pożarna w Włosienica, alle serate e soprattutto nel tuo appartamento l'ultima settimana prima di tornare a casa. Grazie per tutti i ricordi insieme e per non avermi lasciato solo a casa tutto il tempo.

Grazie Zuza per essere un esempio di grande amicizia, iniziata a una normale lezione di Entrepreneurship and startup for Engineers e culminata in numerosi viaggi in giro per la Polonia e per l'Italia. Wrocław, Warszawa, Kraków e Bielsko-Biała, trekking su monti Tatry e pomeriggi di studio e divertimento passati insieme a tutto il team sono stati ogni giorno un grande esempio della tua amicizia e delle tue abilità come ingegnere e come puppy shooter.
Manu, grazie per essere stata un punto di riferimento tra il gruppo Erasmus e il gruppo di ingegneri polacchi, unica collega con la quale condividevo entrambi i gruppi. Ci siamo divertiti molto insieme nelle numerose gite organizzate da Zu e Miko ma anche a qualche evento Erasmus o semplicemente a qualche serata in compagnia. Grazie per avermi spiegato tutto del sud America, spero un giorno di poter venire a visitare la tanto decantata Caracas.
Grazie Riccardo, unico Milanista all'estero, con cui ho potuto gioire del bellissime partite di merda viste al 442. Ogni volta che ci andavamo carichi come due ultras, prendevamo scoppole clamorose, come con il Toro in coppa, le altre evito di rimembrarle. Abbiamo visto e perso tutti i derby insieme, ma arriverà il nostro momento un giorno, inizio quasi a pensare che portiamo sfiga. Grazie per aver passato con me l'esame di Intelligenza Artificiale, sbroccando pomeriggi interi grazie a Ilona e ammattendoci a programmare robot aspirapolvere capaci di uscire dai labirinti, salvo poi scoprire che la soluzione era molto più semplice. Grazie anche per essere venuto a tifarmi al palazzetto dello sport della PK, abbiamo vinto anche grazie al tuo tifo. Trovare un marchigiano a Cracovia ha reso il tutto simile a casa senza mai farmene sentire troppo la mancanza.
Grazie Riza, per le serate più assurde e soprattutto per le corse chilometriche insieme. Ringrazio poi le mie due flatmates, con cui ho condiviso il la parte più drammatica del lockdown, la reclusione nello stesso appartamento con un uomo dai versi animaleschi e dallo stile di vita di Bob l'aggiusta tutto. Che dire, grazie per le risate, i pranzi insieme, l'avermi rassicurato sul mio arrivo in piena pandemia, le cazzate e i problemi amorosi. Una soap-opera spagnola in confronto ai nostri sei mesi è niente. Spero possiate venire alla mio secondo tentativo di rivedervi, mi avete già ignorato a Cracovia, riuscirete mai a liberarvi per la mia laurea?
È arrivato il momento di scrivere due parole anche per i miei amici, che hanno continuato a sostenermi ed hanno vissuto con me quasi ogni istante di questa mia magistrale. Se fate parte di questa categoria vuol dire che ormai mi conoscete, chi più chi meno, e sapete già tutto ciò che ho da dirvi, ma, soprattutto, sapete anche che questa è l'unica parte di tutto "sto lavoro" che andrete a leggere.
Comincio con il ringraziare i ragazzi di corso Amendola 59. "Tommà come te lo devo dire?". Con una delle frasi più iconiche del Fabaria rally; inizio dal ragazzo con cui ho condiviso la casa per quasi tutti i miei anni universitari. Arrivato il mio secondo anno, mi sono accaparrato la mia prima matricola e non l'ho lasciata più. Le avventure di Corso Amendola sono state meno di quelle di via Costa sicuramente, ma tra falegnameria, tinteggiatura della casa e fantacalci ci siamo divertiti. Spero

che a te e a Loré sia piaciuta Cracovia e le sue bellezze, ci siamo capiti. Grazie per essermi venuto a trovare, non so se Lorenzo leggerà anche questa parte nel dubbio lo metterò subito dopo così non si affatica tanto a sfogliare. Sicuro di poterti avere sempre al mio fianco in ognuna delle più disparate mattate da fare o in ognuno dei momenti più seri della mia vita, spero che questa amicizia continui negli anni, non si sa mai dovessi aver bisogno di qualche lastra urgente.
L'altro storico coinquilino, dal quale sono stato ingiustamente separato per un anno sei tu Loré. O Amico che dir si voglia, ma non de tutti. Tu mi hai letteralmente cresciuto, la tua matricola, il tuo sacco da box, il tuo manichino per esplorazioni "analtomiche" o scientificamente parlando la tua creazione. Dai derby visti insieme, sponde rigorosamente opposte, ai consigli e confronti politici ma senza mai abbandonare l'enorme mole di cazzate dette e fatte insieme e se non hai letto sopra, per essere venuto a trovarmi nell'Est Europa. Spero di non perderti mai di vista e di rimanere sempre noi nonostante tutto, pure se tifi la squadra sbagliata di Milano, anche perché dove lo trovo uno con un campetto da calcetto e un lago tutto suo? Aspetto ancora di andare a pesca, "cojone".
Rimanendo in tema cameretta come non menzionare Michele, per me Mike all'inglese. Il vero uomo di via Costa in tutto e per tutto e non solo per la maggiore esperienza e per i veri consigli di vita; ma soprattutto per le opere d'arte contemporanea che riuscivi a creare con la tua montagna di vestiti. O per la brillante idea, appoggiata ed eseguita dal sottoscritto, di dare fuoco a un lavandino, con rischio di incendio e di esplosione dell'appartamento, per, diremmo oggi, sanificare l'ambiente. Grazie davvero Mike perché se c'è uno che ho sempre ammirato in silenzio e al quale vorrei somigliare sotto alcuni aspetti, sei tu.
Sté anche tu fai parte degli irriducibili di via Costa, della spina nel fianco al dominio incontrastato dell'Impero Galattico, parte fissa dell'Alleanza Ribelle. Se qualcuno ha mai cercato di ottenere "poooooteeereeee illimitato" io ti ringrazio per l'esatto opposto; per la semplicità nel vivere e per la schiettezza e sincerità nei miei confronti. Non ringrazio invece Spiga per non aver mai creduto nella resistenza e per essere passato al lato oscuro della forza, ma si sa, ogni storia per essere avvincente necessita del buono che tradisce tutti diventando un temibile cattivo. Anche se un temibile cattivo in realtà per me non lo sei mai stato, anzi, il contrario, uno dei ragazzi più buoni e semplici che io abbia avuto la fortuna di incontrare. Grazie per avermi fatto compagnia durante tutti questi anni con meme, video, fantacalcio e aver mantenuto caldo l'asse Cracovia-Tolentino; mi hai davvero dimostrato di essere un vero amico. D'altronde non potevo dubitare di un carrista esperto come te, ci siamo spalleggiati e aiutati in numerose battaglie alla guida dei mezzi più disparati tentando inutilmente di controbilanciare la potenza inaudita dei carri ppw notoriamente impenetrabili dai nostri modesti T26E5 Patriot. A volte abbiamo idee e pareri contrastanti, ma sono sicuro che sai che molte cose in realtà le dico soprattutto per farti incazzare. Spero di poter passare ancora parecchio tempo insieme a te, online e offline, soprattutto per la miriade di cose che abbiamo in comune e che capiamo solo noi.

Ringrazio infine uno degli ultimi, anzi dei primi di via Costa, Quartino, primo ad accogliere una matricola all'inizio della sua avventura.
Passiamo poi a un altro pezzo da e del 90. Genius grazie per tutto; non so da dove cominciare. Altra guida che ho avuto durante il mio percorso, baluardo ed esempio della fede. La tua capacità di riflessione sui temi più reali che la vita ti pone e la semplicità con la quale esponevi il tuo pensiero a riguardo mi hanno sempre disarmato. Grazie soprattutto per avermi sfidato e fatto diventare uno dei migliori arbitri della sezione di Ascoli Piceno, non te ne sarò mai grato abbastanza, anche se oramai sono passato al Futsal cercando di emulare le orme di Angelo Galante. Grazie per avermi fatto da OA personale e per avermi sempre dato i consigli giusti in campo e per avermi riaccolto sull'italico suolo non appena il carrello del Gaelico aviomotore si è poggiato a terra. Con te non serve sperare, so che la distanza non è abbastanza per minare un amicizia così grande.
Ultimo degli anconetani, ma non per ordine di importanza, ringrazio Mattia. Con te so di non dover aggiungere altro, ogni parola sarebbe superflua. Solo noi sappiamo quanto abbiamo condiviso ad Ancona prima e in Polonia poi. Mi dispiace che non sei potuto venire per un'ulteriore visita in modo da ripetere quei 3 giorni da soli a Cracovia. Una spalla su cui piangere, un degno avversario a calcetto, un amico vero, ma soprattutto un ragazzo in tutto e per tutto uguale a me. Peccato anche tu abbia i tuoi difetti ma ti capisco, con il tuo carattere e il tuo cuore non potevi che innamorarti della pazza di Milano. Sicuro di poter condividere con te nuove avventure, ti aspetto per il nostro prossimo viaggio a Cracovia, in Islanda, in Albania e in tutti gli altri posti che vogliamo aggiungere. Da qualche parte dovremmo cominciare no?
Finisco con il ringraziare tutti gli amici di Ancona, purtroppo non ho abbastanza tempo e spazio per scrivere a ognuno di voi, altrimenti qualche riga in più ve le avrei dedicate.
Clara, l'unica Ascolana in terra nemica. Grazie per i discorsi eterni in macchina insieme, grazie anche per quando dormivi o quando ti ci sentivi male. Grazie anche per la mole di reels che mi mandi, una risata la strappi sempre. Se avrai bisogno di SIK l'aggiustatutto di nuovo, tieni in considerazione qualche pranzo, oppure il cash altrimenti o qualche altro sistema di pagamento in natura o tramite baratto. Grazie per la tua dolcezza e per la tua onestà disarmante "scojattolinni".
Giulia, grazie per essere rimasta mia amica anche se ti do sempre fastidio e se so essere davvero stronzo a volte; mi dispiace che tue tecniche non abbiano mai funzionato. Grazie per avermi fatto studiare, ma soprattutto per essere stata una vera amica in facoltà e anche al di fuori. Purtroppo ti sei persa Cracovia e anche la mia laurea, ti toccherà riandarci da sola mi dispiace.
Sara, grazie per tutto, per sentirci ogni tanto, per l'invito a Roma per la carbonara e per vedere una partita del Milan, non so se troverò mai tempo e spazio dato che l'ultima volta a San Siro non sono nemmeno andato a vedere il Milan purtroppo. Prometto che cercherò di mantenere la parola data, anche se tra le partite da arbitrare e gli impegni del week-end non riesco mai a trovare un giorno libero.

Giulia Pia grazie per avermi permesso di condividere con una parte dell'università e soprattutto della difficoltà al ritorno a casa dopo la prima avventura Erasmus. Sappiamo come ci si sente e ne abbiamo parlato numerose volte, ti ringrazio per essere quell'amica che non ti aspetti, chi ci avrebbe scommesso dopo tutti questi anni?
Grazie Ferro per avermi dimostrato con i fatti che se uno ha piacere di fare qualcosa fino in fondo allora farà di tutto davvero, compresi alcuni sacrifici per esserci e non perdersi nulla. Mi hai stupito con la tua presenza 3 anni fa e continui a farlo presentandoti a ogni cena APAB o motivo per rincontrarsi e raccontarsi qualcosa di nuovo.
Filippo "El Puerk" e Lorenzo "Paciuozz", grazie per aver esteso la vostra amicizia al fratello del capitano della vostra squadra (non mi sta costringendo a scriverlo lo giuro), non era per nulla scontato. Il primo è il futsal, anche se Davide fa i goal, il secondo era il futsal anche se a sentirlo parlare è ancora uno dei talenti più cristallini del calcio marchigiano, forse intendevi a EAFC? Ho avuto la fortuna di condividere con voi lo stesso terreno di gioco e la sfortuna di dovervici vedere giocare sopra. Ogni partita di futsal mi fate perde 10 anni di vita, per fortuna sono venuto poche volte a vedervi.
Tony, lo gnorri, grazie per avermi fatto compagnia online su ogni Call Of Duty uscito dopo il 2011. Le warzonate infinite, le kill, le cagate, le risate ma soprattutto grandi chiacchierate degne di una grande amicizia.
Mariani, Cocci e Ferretti, il trio AIA, gli unici che mi capiscono davvero quando si tratta di arbitraggio. Voi sapete cosa significa andare ad arbitrare a Petritoli, in culo ai lupi, con un freddo boia ed essere insultati dal primo all'ultimo minuto, senza un apparente motivo. Sapete anche le fatiche e i sacrifici che si fanno per portare avanti questa passione, ma soprattutto siete persone dalle quali cerco sempre di carpire qualcosa sia dentro che fuori dal campo. Signor Mariani, da te vorrei prendere la voglia e la dedizione che metti per arrivare in serie A, anche se a volte la reputo esagerata e completamente immotivata, non essere troppo frettoloso o duro con te stesso. Dal signor Cocci vorrei prendere la gestione dei calciatori e l'atletismo in campo, vedere una montagna di muscoli andare così forte fa sempre un certo effetto, anche se ultimamente riesco a tenere il passo in allenamento. Dal signor Ferretti vorrei prendere la credibilità e la simpatia, riusciresti a convincere un calciatore che si può segnare da calcio di punizione indiretto e nessuno ti darebbe torto. Grazie per essere degli ottimi esempi e amici.
Non mi sono scordato di voi affatto. Davidì e Nello, grazie per aver condiviso con me la passione per l'Ascoli Calcio, nata soprattutto dai vostri ripetuti inviti alle partite del Picchio. Grazie per esserci stati sempre nei momenti di svago e divertimento, come tornei di calcio, gite fuori porta, giornate allo stadio o serate al cinema. Siete due grandi esempi di amicizia, spero di potermi sdebitare a breve con voi, non mi sono scordato della cena a Cermignano.
Dulcis in fundo la *old school*. I due Andrei, miei amici da una vita, finalmente

ci siamo vi sto per raggiungere tra i lavoratori sottopagati; grazie AB per avermi dimostrato che la passione nel lavoro vale più di tutto il resto, il tuo fisico fa capire davvero quanta passione ci sia, mentre quello dell'altro Andrea fa capire quando esattamente la passione non c'è. André diciamocelo, il tuo sistema immunitario non è mai stato un grande ostacolo per virus e batteri capaci di stenderti KO con un raffreddore. Grazie però per avermi dato testimonianza che nonostante i tempi siano cambiati c'è ancora chi decide di intraprendere un cammino insieme a un altra persona. Vero, Chiara, Ari e Paola grazie per essere ogni giorno testimonianza vera di una grande amicizia che è iniziata oramai più di quindici anni fa e che non vedrà mai la fine.
Ad Maiora Semper

Ascoli Piceno, Settembre 2023

Simone ONORI