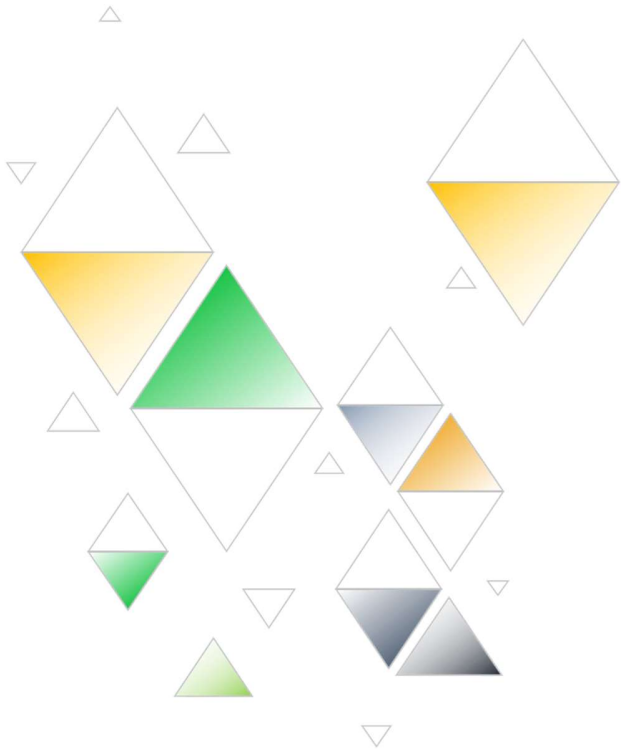
REPORT DI VALUTAZIONE SULLE SECURITY OPERATIONS

W20D4
Progetto M5
EPICODE



08/02/2025

PREPARATO E RIVISTO DA	**FEDERICO PRESTI**

SOMMARIO

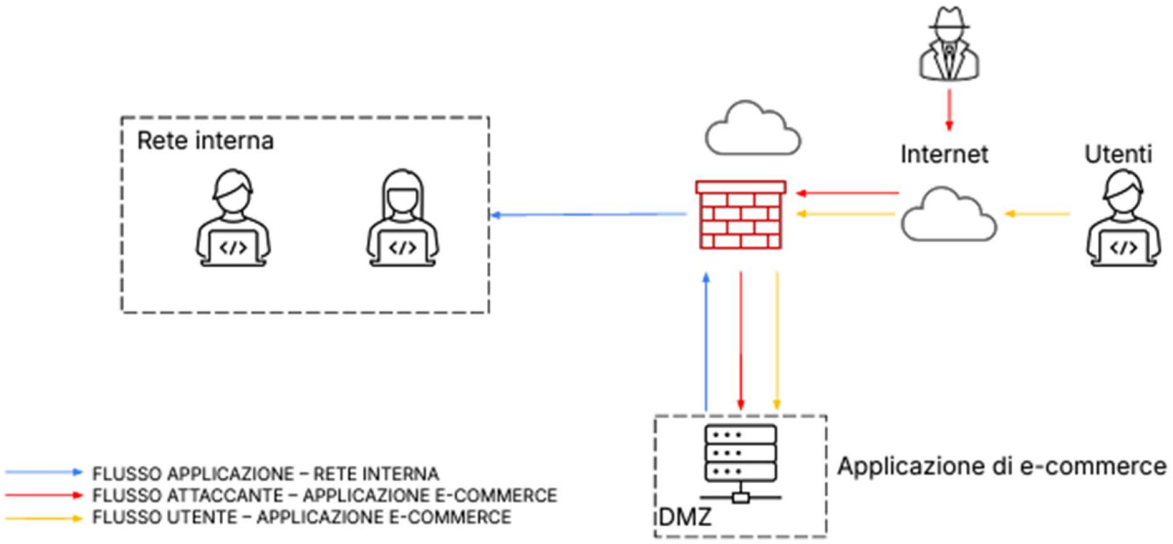
TRACCIA E CARATTERISTICHE DEL PROGETTO

NOME DEL PROGETTO	**Epicode Modulo 5**
PANORAMICA DELL'ESERCIZIO	Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti. 1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni 2. **Impatti sul business**: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per **10 minuti.** Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono 1.500 €** sulla piattaforma di e-commerce. **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica** 3. **Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta. 4. **Soluzione completa:** unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3) . 5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2 .**

Figura in Slide 2 o Architettura di rete iniziale

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



PUNTO N.1; AZIONI PREVENTIVE.

La Figura in Slide 2, rappresenta un'architettura di rete in cui un'applicazione di e-commerce è ospitata in una DMZ (zona demilitarizzata) ed è accessibile tramite Internet per consentire agli utenti di effettuare acquisti. Tuttavia, viene evidenziato un rischio di sicurezza significativo: la rete interna è raggiungibile dalla DMZ a causa delle policy del firewall.

Questo significa che, se un attaccante compromette il server nella DMZ, potrebbe potenzialmente accedere alla rete interna.

SCENARIO: Attacco di tipo SQL INJECTION

SQL Injection (SQLi) è una vulnerabilità di sicurezza che consente a un attaccante di manipolare le query SQL inviate a un database.

Accade quando un'applicazione non valida o sanitizza correttamente l'input utente, permettendo all'attaccante di inserire comandi SQL dannosi che possono:

- **Accedere a dati sensibili:** Visualizzare informazioni non autorizzate, come credenziali o dati personali.
- **Modificare dati:** Alterare, eliminare o aggiungere record nel database.
- **Eseguire comandi dannosi:** In alcuni casi, può permettere l'esecuzione di comandi sul server.
- **Compromettere l'intero sistema:** Esfiltrare dati o prendere il controllo del server

STRUMENTI

Analisi con tool di scansione automatica come NESSUS e ACUNETIX.

AZIONI CONSIGLIATE

Oltre alla modifica delle policy del Firewall si consiglia l'implementazione di una Content Security policy (CSP)

Stima del rischio di un attacco SQL INJECTION secondo il punteggio CVSS:

Da 6.5, in caso di esposizione limitata di dati (RISCHIO MEDIO) a 10, in caso di esecuzione di shell remote e controllo del server (CRITICO), dove il downtime del server in termini economici rappresenta il rischio più elevato.

SCENARIO: Attacco di tipo Cross-site scripting (XSS)

Il **Cross-Site Scripting (XSS)** è una vulnerabilità di sicurezza comune nelle applicazioni web che consente a un attaccante di iniettare codice JavaScript dannoso in una pagina web visualizzata da altri utenti.

Questo attacco si verifica quando l'applicazione non valida o sanitizza correttamente l'input dell'utente, consentendo l'esecuzione di script arbitrari nel browser delle vittime.

Gli attacchi XSS possono avere diverse conseguenze:

- **Furto di cookie e sessioni:** Gli attaccanti possono rubare cookie di sessione per autenticarsi come un altro utente.
- **Phishing:** Gli attaccanti possono iniettare form di login falsi.
- **Distribuzione di malware:** Gli script possono reindirizzare le vittime verso siti dannosi.
- **Defacement:** Modifica del contenuto della pagina web.

STRUMENTI

Analisi con tool di scansione automatica come NESSUS, NIKTO o anche NMAP + Script N.S.E.

AZIONI CONSIGLIATE

Oltre alla modifica delle policy del Firewall si consiglia l'implementazione di un Web Application Firewall (WAF)

Le soluzioni proposte nella dinamica di questa infrastruttura di rete, mettono in evidenza dei problemi alla base:

- Qualsiasi attaccante infatti può provare ad accedere all'infrastruttura applicativa;
- Un attaccante potrebbe sferrare un attacco alla rete interna;
- Un attacco di tipo DOS o D-DOS potrebbe mettere sia la DMZ e conseguentemente l'applicazione di E-Commerce offline.

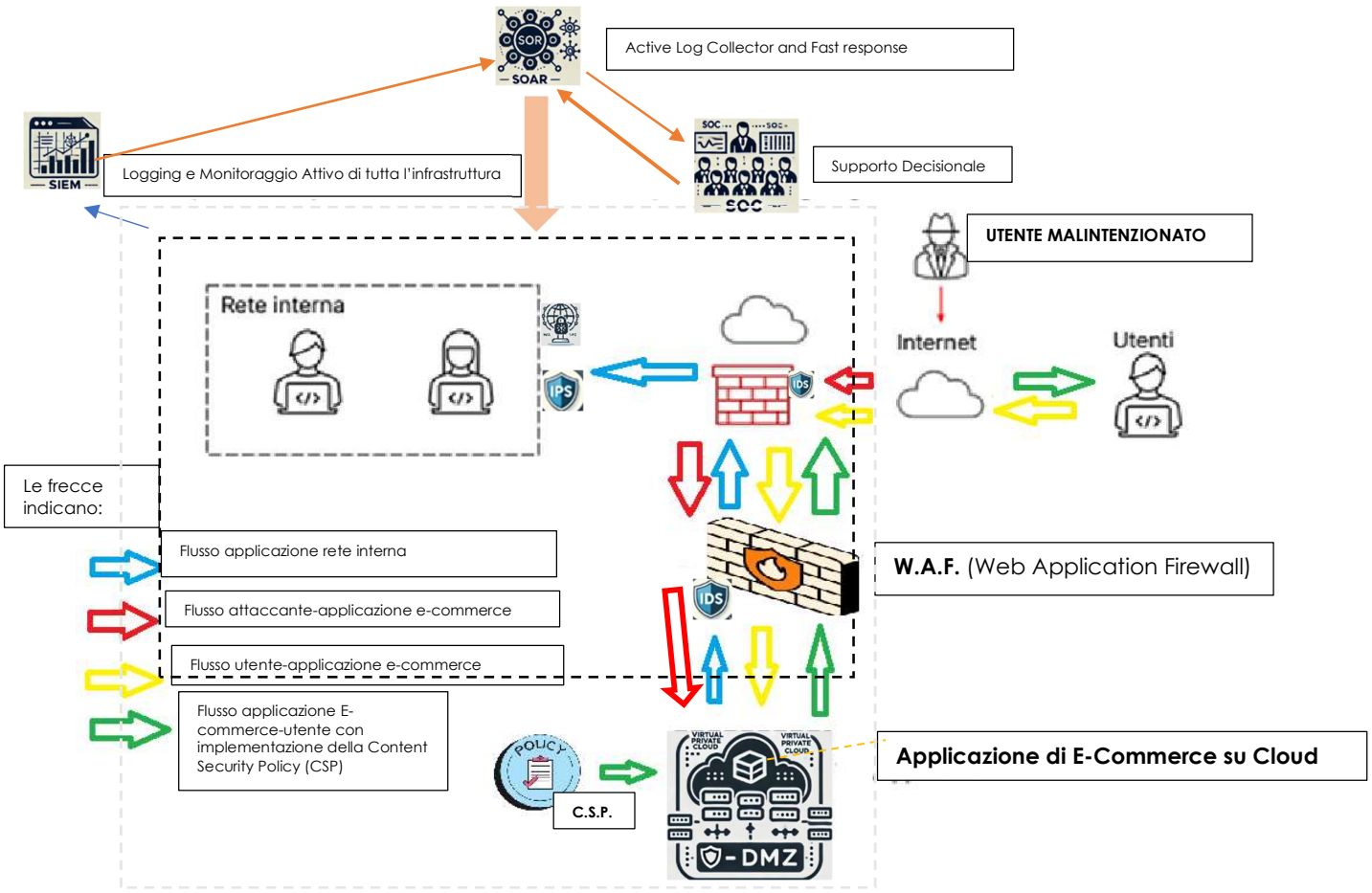
Adotteremo quindi queste misure preventive:

- Adotteremo una V.P.C (Virtual Private Cloud) per rendere così la DMZ contenente l'applicazione di E-Commerce scalabile su vari server;
- Adotteremo strutture automatizzate come SOAR (Security Orchestration, Automation and Response) per velocizzare la rilevazione di eventuali anomalie in combinazione con strumenti SIEM (Security Information and Event Management) come Splunk, specializzati nella raccolta, analisi e correlazione degli eventi di sicurezza, fornendo visibilità e avvisi grazie anche a strumenti I.D.S. e I.P.S

Stima del rischio di un XSS secondo il punteggio CVSS:

Il punteggio CVSS di base per un attacco XSS può variare da 4.5 (Media) a 7.0 (Alta), a seconda delle circostanze specifiche. Nel nostro scenario, trattandosi di un sito di e-commerce l'impatto economico è elevato, quindi il punteggio adottato rispecchierà questa stima.

Primo Grafico con utilizzo delle modifiche proposte ed implementato con una segmentazione ulteriore della rete e con monitoraggio attivo dei flussi utente.



PUNTO N.2; IMPATTO FINANZIARIO.

L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per **10 minuti.** Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono 1.500€** sulla piattaforma di e-commerce.

Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

<table>
<tr><th colspan="2">STIMA</th><th>SPIEGAZIONE</th></tr>
<tr><td>GUADAGNO PER MINUTO</td><td>€1500</td><td rowspan="2">Per stimare il danno economico causato da un'interruzione del servizio, come nel caso di un attacco DDoS, si applica la formula del Costo del Tempo di Inattività (CoD). Questa metodologia è frequente nella redazione di un Piano di Business Continuity.
La formula del CoD calcola il costo basandosi sul guadagno per ogni minuto di operatività e sulla durata dell'interruzione.</td></tr>
<tr><td>TEMPO DI INATTIVITA'</td><td>10 minuti</td></tr>
<tr><td>METODOLOGIA DI DETERMINAZIONE</td><td colspan="2">CoD = (Costo del Tempo di Inattività) moltiplicato per GpM (Guadagno per Minuto) da come risultato il TdI = Tempo di inattività (in minuti)</td></tr>
<tr><td>PERDITE</td><td colspan="2">Cost of Downtime (COD) = 1500 euro x 10 minuti = 15.000 euro.

La perdita sarà uguale a 15.000 euro per 10 minuti di inattività.</td></tr>
</table>

AZIONI PREVENTIVE IN CASO DI ATTACCO D-DOS

Nel caso di specie, possono essere implementate queste soluzioni, (alcune già adottate nello scenario precedente) per fornire una risposta rapida, efficace e duratura che sono:

- **Effettuare backup regolari**, strategia fondamentale per permettere all'organizzazione di ripristinare i propri sistemi dopo un incidente.
- **L'adozione di un sistema di Network Access Control (NAC),** essenziale per regolare e monitorare gli accessi nella rete aziendale, assicurando che solo i dispositivi autorizzati possano accedere agli asset critici.
- **L'implementazione di soluzioni cloud** nella gestione della sicurezza e dell'archiviazione dati aziendali migliora la scalabilità delle risorse, aumenta la disponibilità per gli utenti e accelera la continuità operativa con opzioni integrate di backup e disaster recovery.
- **Usare un sistema di rilevamento delle intrusioni** (IDS, Intrusion Detection System) nella struttura di sicurezza aziendale è essenziale, poiché questo dispositivo permette di

monitorare il traffico di rete e fornisce notifiche tramite alert in caso di rilevamento di comportamenti anomali.

- **Incorporare un sistema** di Intrusion Prevention System (IPS), che utilizza firme e analisi comportamentali **per rilevare e successivamente bloccare attività sospette o dannose** prima che possano arrecare danno ai sistemi, è altrettanto cruciale.

Stima del rischio di un attacco D-DOS secondo il punteggio CVSS:

Il punteggio CVSS di base per un attacco di questo tipo è abbastanza alto e può variare da 7.0 (Criticità Alta) a 10 (Critica) a seconda delle circostanze specifiche. Nel nostro scenario, trattandosi di un sito di e-commerce, l'impatto economico è la prima preoccupazione poiché **nel caso il disagio si estendi per un'ora di inattività si può potenzialmente arrecare un danno di 90.000 euro all'azienda.**

PUNTO N.3; RESPONSE IN CASO DI INFEZIONE DA PARTE DI UN MALWARE

L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
Modificate la figura in slide 2 con la soluzione proposta.

Integrazione tra DMZ VPC e NAC per un tempestivo isolamento della macchina

Il meccanismo che viene attivato non solo disconnette e isola la macchina infetta, ma permette anche al cloud di ripristinare l'ambiente in una nuova ubicazione attraverso backup attivi.
Parallelamente, l'applicazione compromessa viene deliberatamente esposta per fungere da honeypot, attirando l'attenzione dei cybercriminali e consentendo al Threat Intelligence Team operante nel SOC di analizzare le tecniche degli attaccanti e rafforzare le strategie di prevenzione e risposta**.**
Nell'ambito dello schema proposto, l'integrazione di queste tre tecnologie è fondamentale per garantire una risposta rapida agli incidenti, la continuità operativa e un'analisi efficace delle minacce. Ogni componente ha un ruolo specifico ma complementare nella protezione dell'applicazione di e-commerce e nella gestione delle minacce.
Ecco come l'integrazione tra DMZ, VPC e NAC opera concretamente nell'ambiente descritto:

DMZ: Il Primo Livello di Difesa

La DMZ funge da primo livello di difesa contro le minacce esterne. Ospitando il server web dell'applicazione di e-commerce, la DMZ agisce come punto di accesso controllato per

tutto il traffico internet in entrata, bloccando attacchi mirati come SQL injection e XSS prima che possano raggiungere componenti più critici della rete.

VPC: Sicurezza e Isolamento Avanzati

La VPC contiene le risorse essenziali dell'applicazione di e-commerce, incluse le basi di dati e i server di applicazioni, che necessitano di protezione e isolamento da accessi non autorizzati. All'interno della VPC, subnet dedicate e gruppi di sicurezza forniscono un controllo granulare del traffico e isolano le risorse di backend da quelle esposte nella DMZ. Questo isolamento aiuta a prevenire la propagazione di attacchi all'interno della rete aziendale e garantisce che le operazioni critiche possano continuare anche durante un tentativo di intrusione.

NAC: Controllo di Accesso e Risposta Rapida

Il NAC svolge un ruolo cruciale nell'identificare e gestire i dispositivi che tentano di connettersi alla rete. Implementato sia nella DMZ che nella VPC, il NAC assicura che solo dispositivi autenticati e conformi alle politiche di sicurezza aziendale possano accedere alle risorse di rete. In caso di rilevamento di un dispositivo infetto o sospetto, il NAC può rapidamente disconnettere o isolare la macchina infetta, impedendo la diffusione del malware e limitando i danni.

Fast Response, Business Continuity e Threat Intelligence Analysis

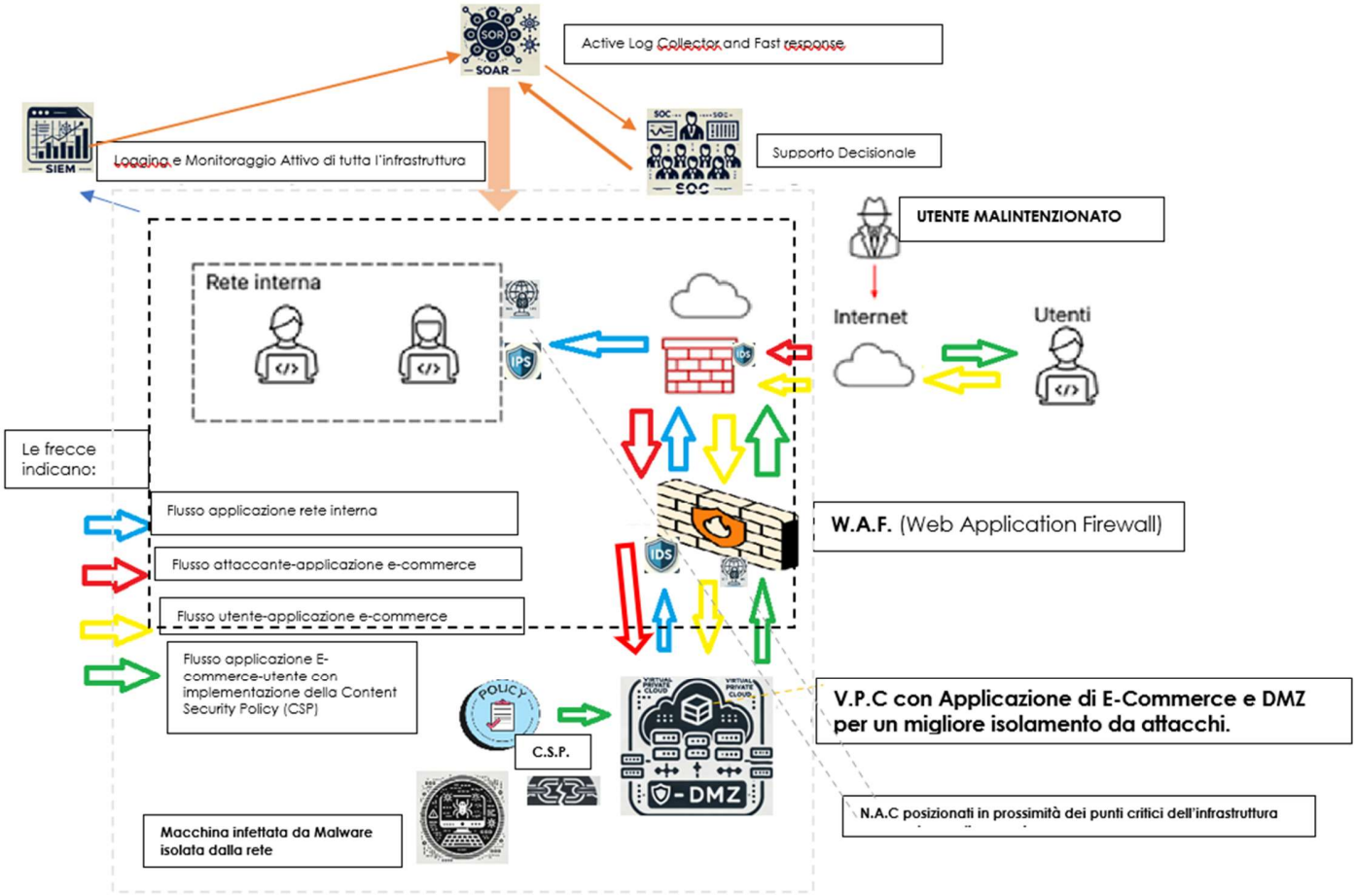
L'integrazione tra DMZ, VPC e NAC permette una risposta tempestiva in caso di incidenti. Questo approccio non solo limita l'impatto di un attacco, garantendo la continuità delle operazioni commerciali, ma fornisce anche dati preziosi per l'analisi delle minacce.
Le informazioni raccolte attraverso il monitoring attivo e gli eventi di sicurezza registrati dal NAC e dagli altri componenti di sicurezza sono analizzate per identificare i pattern di attacco, migliorare le strategie di sicurezza e sviluppare una conoscenza approfondita del panorama delle minacce.

Stima del rischio di un attacco malware secondo il punteggio CVSS:

Supponendo una mancanza di mitigazioni specifiche oltre quelle standard e basandoci su una configurazione comune, possiamo ipotizzare un punteggio base CVSS di circa 8.0 - 9.0, che indica un livello di gravità "Alto". Tuttavia, con le misure di sicurezza implementate in questo scenario, il punteggio potrebbe abbassarsi a circa 4.0-5.0, indicando un rischio moderato.

SECONDO GRAFICO IMPLEMENTATO E SOLUZIONE COMPLETA;

3° E 4° PUNTO DELLA TRACCIA



PUNTO N.5: SOLUZIONE CON MODIFICA <<PIÙ AGGRESSIVA>> DELL'INFRASTRUTTURA

Una soluzione più aggressiva, richiede innanzitutto **l'adozione di una architettura di rete di tipo "zero trust"** basata sul concetto cardine della Cybersecurity: la triade C.I.A.

Questo principio assume che le minacce possano originarsi sia all'interno che all'esterno delle reti aziendali e che nessun utente o dispositivo debba essere fidato implicitamente. Questo grazie all'autenticazione continua, all'autorizzazione ed alla verifica per ogni accesso alle risorse di rete, indipendentemente dalla posizione dell'utente o del dispositivo;

Andremo ad implementare dunque una **segmentazione di rete avanzata per limitare lateralmente il movimento in caso di intrusione;**

Detto ciò, anche in base agli sviluppi recenti possiamo adottare un approccio di difesa basato su **Intelligenza Artificiale (AI) e Machine Learning** per rilevare comportamenti sospetti e anomalie che possono sfuggire ai sistemi di sicurezza tradizionali.

Ultimo comportamento ma non ultimo, specialmente in termini di prevenzione di attacchi D-DOS, investire in tecnologie di **sandboxing e isolamento avanzato.**

Grazie per la visione.