EPICODE

SECURITY OPERATION

Presentazione di: Pandolfi Luciano

INDICE

AZIONI PREVENTIVE (SQLI E XSS)

Per difendere l'applicazione Web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), si possono implementare le seguenti azioni preventive:

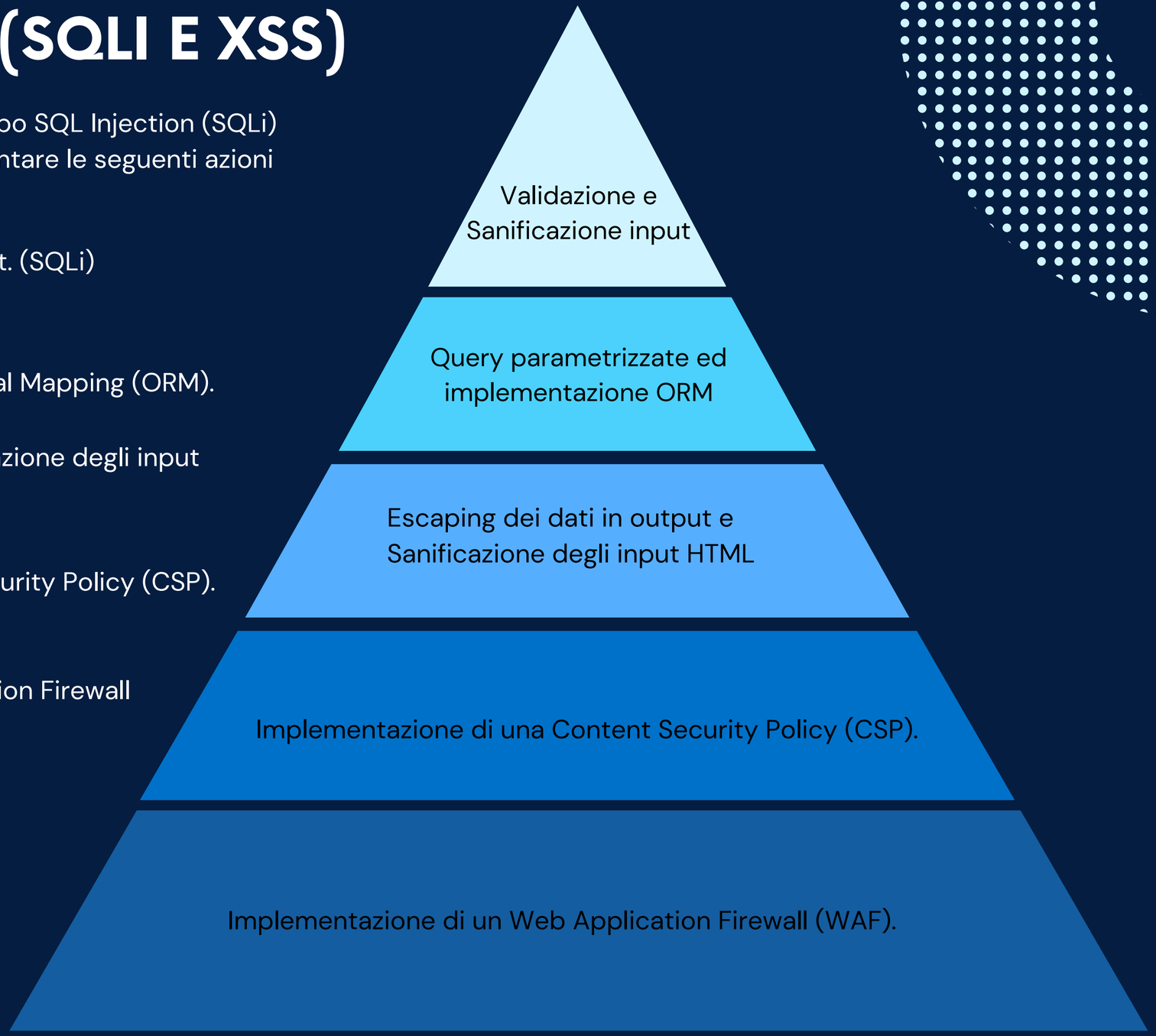
01 — Validazione e sanificazione degli input. (SQLi)

02 — Utilizzo di query parametrizzate ed implementazione di Object-Relational Mapping (ORM).

03 — Escaping dei dati in output e Sanificazione degli input HTML (XXS)

04 — Implementazione di una Content Security Policy (CSP).

05 — Implementazione di un Web Application Firewall (WAF).



IMPATTI SUL BUSINESS

CALCOLO DELLE PERDITE

- 1.500 € di perdita per ogni minuto di inattività
- Perdita totale: 15.000 € per 10 minuti di inattività

AZIONI PREVENTIVE

- Filtraggio del traffico e blocco IP
- SYN Cookies e scalabilità del server
- Sistemi di rilevamento e mitigazione DDoS
- Content Delivery Network

CALCOLO DELLE PERDITE

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.

Per calcolare l'impatto economico di un'interruzione del servizio, come in questo caso di attacco DDoS, si utilizza la formula del CoD (Cost of Downtime). Questa formula viene utilizzata quando viene stilato il Business continuity plan.

CoD = (GpM x TdI)

CoD = Costo del Tempo di Inattività

GpM = Guadagno per Minuto

TdI = Tempo di Inattività (in minuti)

CoD = (1500 euro x 10 minuti) = 15.000 euro

AZIONI PREVENTIVE

Integrare un sistema IPS (Intrusion Prevention System), capace tramite firme/analisi comportamentali di identificare ed in seguito di bloccare attività sospette o dannose prima che danneggi un sistema

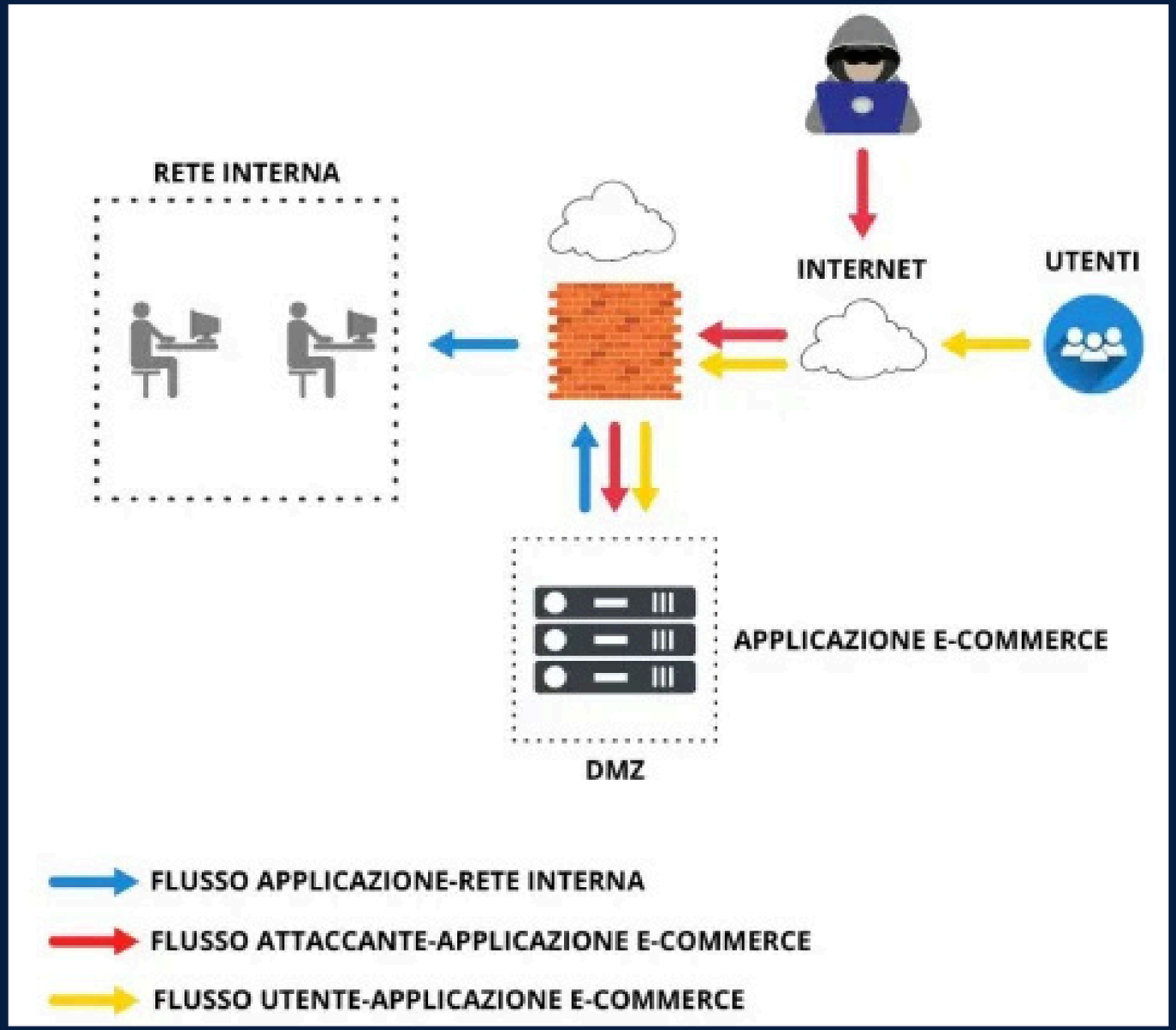
Integrare un sistema IDS (Intrusion Detection System) nella sicurezza aziendale, poiché grazie a questo strumento si può monitorare il traffico di rete e essere avvisati, tramite alert, se vengono riscontrati comportamenti anomali.

BACKUP
Fare dei backup ricorrenti è un strategia necessaria per permettere all'azienda di ripristinare i sistemi in caso di incidente.

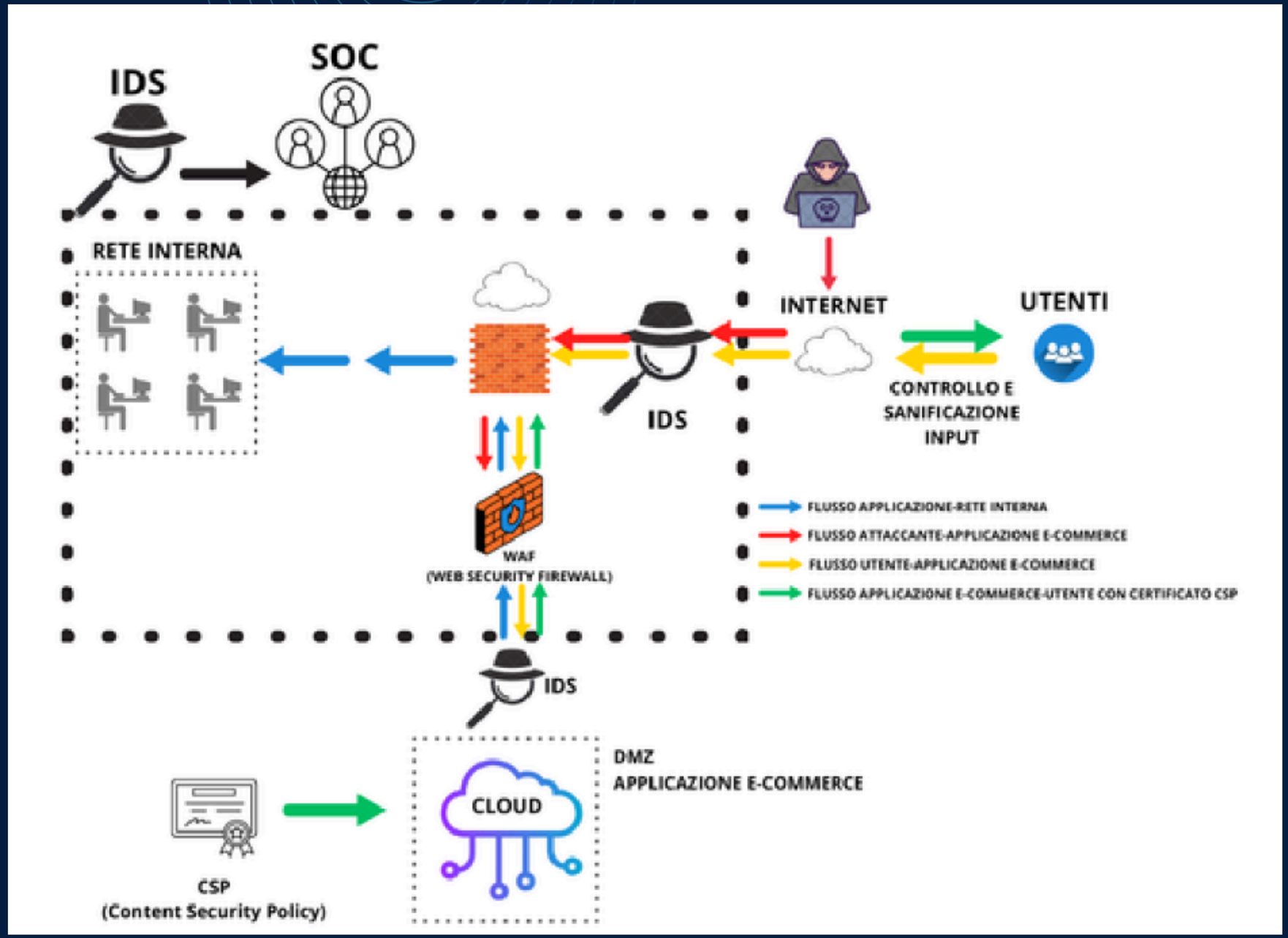
CLOUD
Implementare un cloud a livello di sicurezza e gestione delle memorie all'interno di una rete aziendale favorisce la scalabilità delle risorse in modo dinamico, garantisce una maggiore disponibilità agli utenti delle risorse e una più rapida Business Continuity (con backup o disaster recovery integrati) alle aziende.

NAC
Introdurre un NAC è di fondamentale importanza per gestire e controllare gli accessi all'interno della rete interna assicurandoci che solo i dispositivi autorizzati possano avere accesso alla rete interna o agli asset da proteggere.

ARCHITETTURA DI RETE (INIZIALE)



AZIONI PREVENTIVE



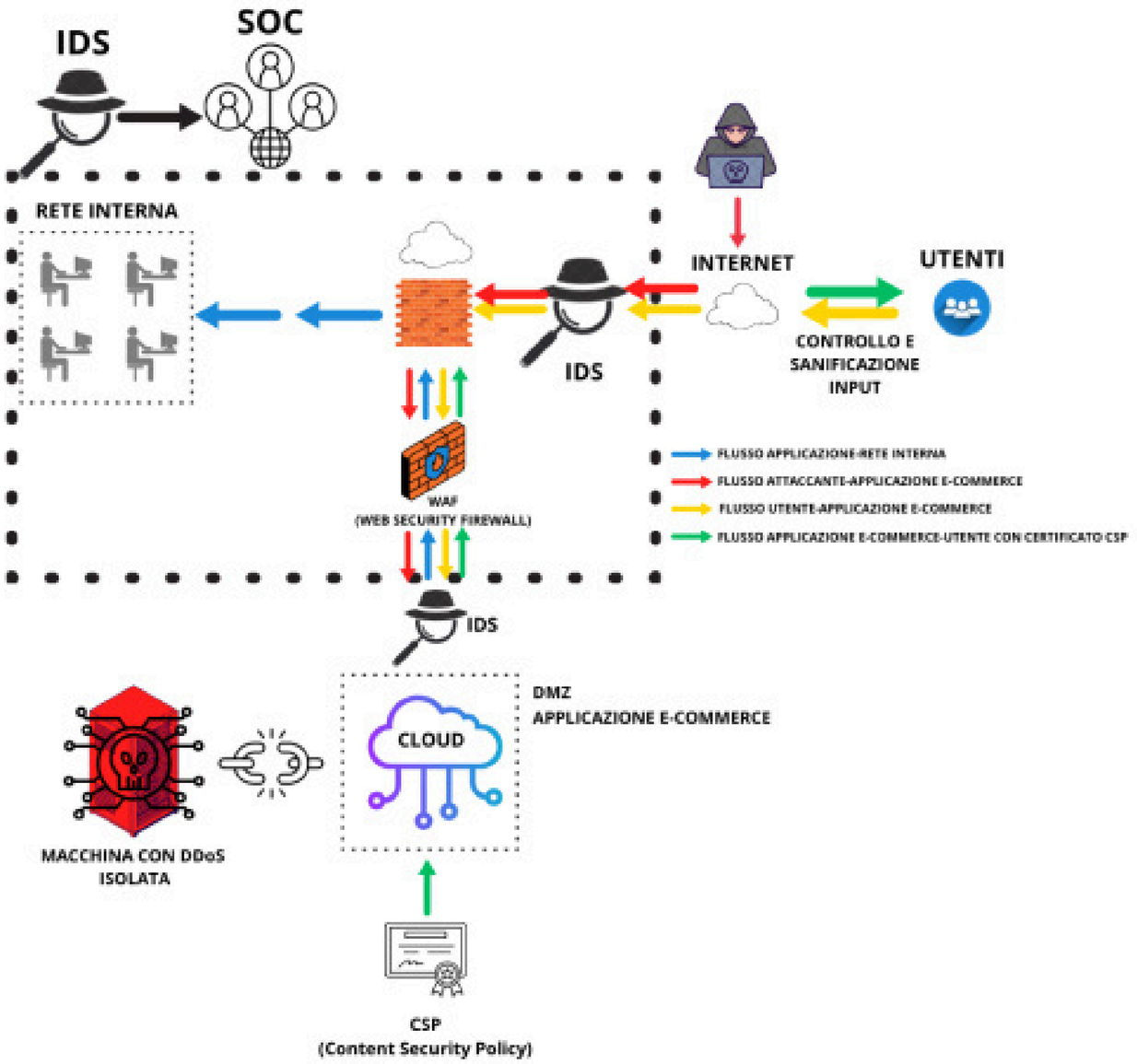
RESPONSE

SQLi/XSS Protections:
- Input Sanitization
- Web Application Firewall (WAF)
- Content Security Policy (CSP)

DDoS Protections:
- CDN (Content Delivery Network)
- Rate Limiting
- Mitigation Services

Malware Response:
- Network Segmentation
- Server Isolation

Advanced Protections:
- Zero Trust Security
- AI Monitoring



RESPONSE + MODIFICA AGGRESSIVA

1 RESPONSE

Creare una VLAN di quarantena per la macchina infetta oppure un VPC (Virtual Private Cloud) isolandola dal resto della rete. Queste strategie ci permettono di eseguire applicazioni aziendali sensibili in un ambiente sicuro, creare una rete privata per risorse cloud senza accesso diretto da internet e
garantire un alta scalabilità e flessibilità delle risorse.

2 RESPONSE

Per implementare la sicurezza dell'applicativo possiamo utilizzare strumenti come in figura:
-WAF: Web Application Firewall con policy che filtrano il traffico in entrata;
-CSP: Content Security Policy in modo tale che limiti l'inserimento di codice malevolo.
-IDS e IPS: il primo che monitoro il traffico di rete e manda alert, il secondo svolge in autonomia funzioni di blocco delle minacce.

3 MODIFICA AGGRESSIVA

Inoltre possiamo adottare un'architettura di rete Zero Trust completa inserendo anche un NAC così da poter gestire gli accessi;
utilizzare un honeypot per poter attirare e monitorare potenziali attacchi;
implementare soluzioni di sicurezza basate su Intelligenza Artificiale e Machine Learning.

4 SOLUZIONE PER BUSINESS CONTINUITY

Possiamo trovare una soluzione agli impatti sul business utilizzando un cloud (come in figura) in modo da diminuire di molto il Tempo Di Inattività poiché oltre la possibilità di segmentare risorse garantisce anche backup di ripristino.
Inoltre con IDS ed IPS riusciamo ad individuare ed isolare la macchina infetta in modo da poter monitorare o prevenire un simile attacco.

EPICODE

Grazie per la visione!!