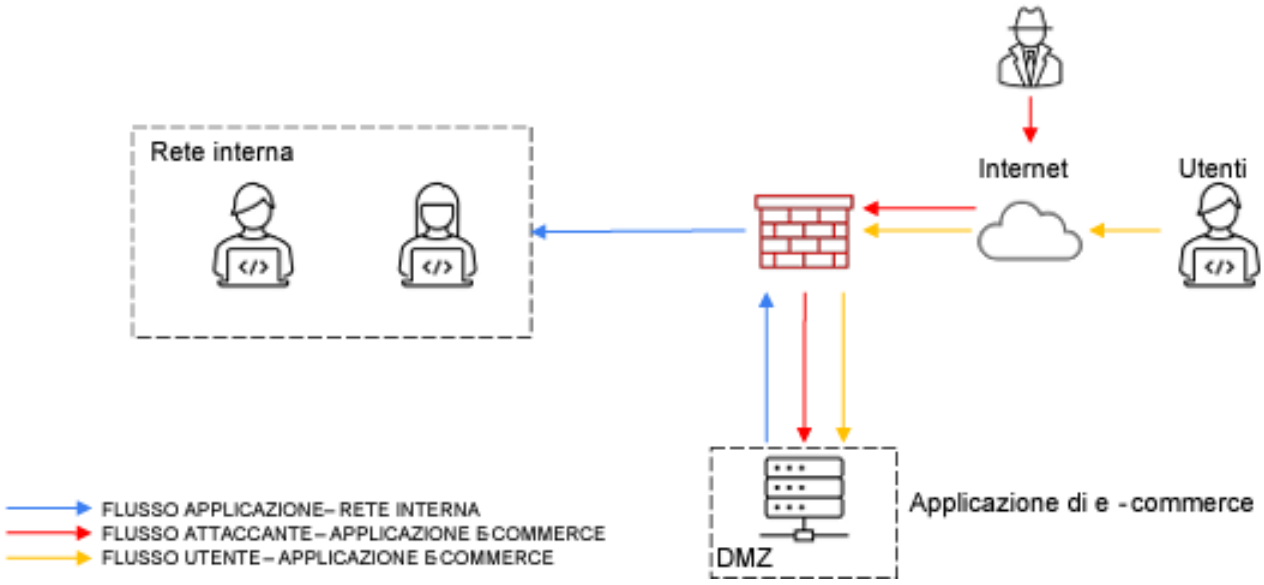
CS0424IT

PROGETTO S9-L5

RETE INIZIALE:

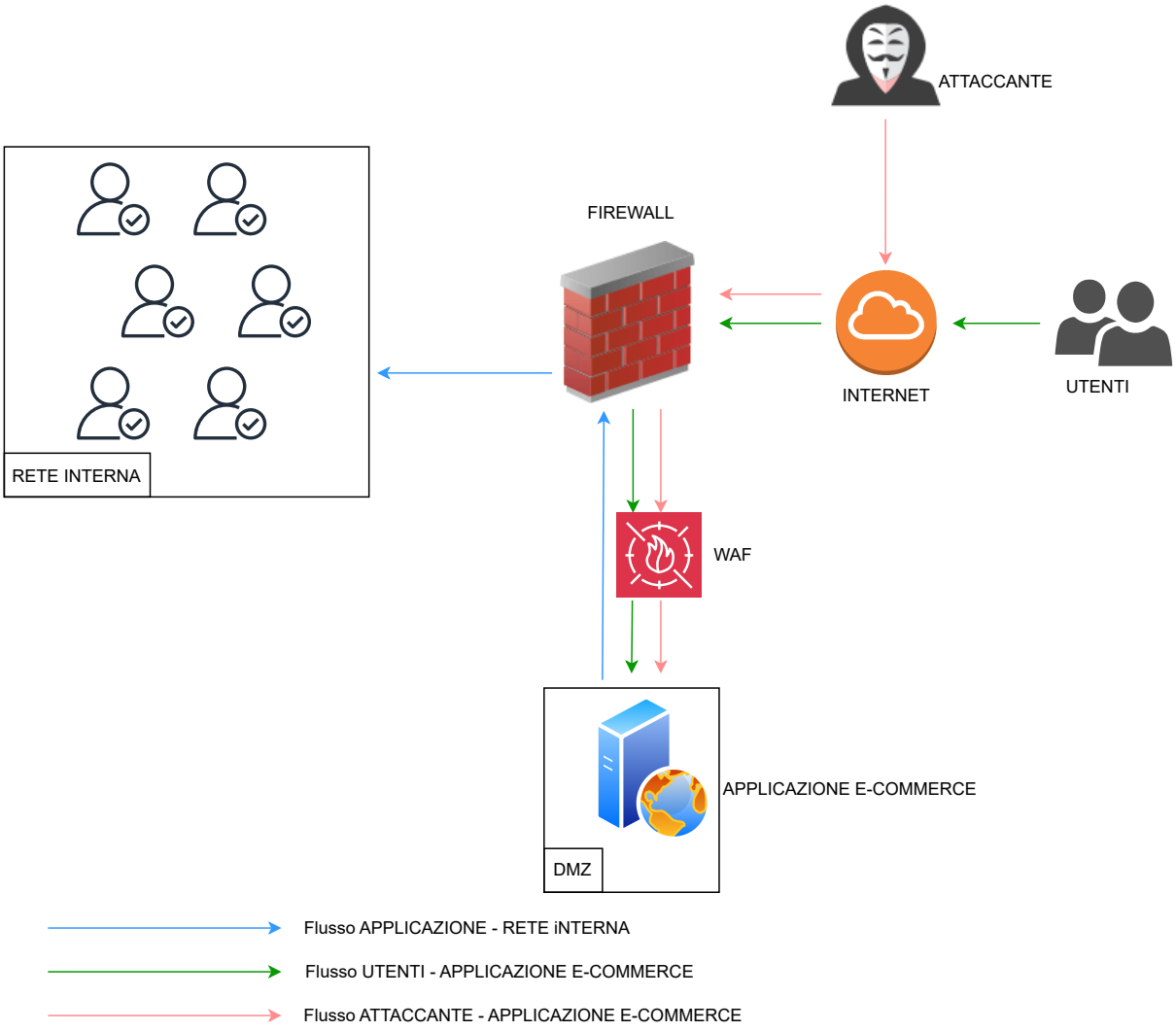


1. **Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?**

- **Santificazione** e **validazione** degli input, per rimuovere i caratteri potenzialmente pericolosi e validare che gli input rispettino i formati attesi. Inoltre è fondamentale
- Implementare un **WAF** per filtrare e bloccare il traffico HTTP/HTTPS verso la Applicazione di E-Commerce. Con le giuste configurazioni il WAF protegge da attacchi come XSS, SQLi, DDoS, LFI, RFI, Bruteforce, e tanti altri attacchi a livello di applicazione. Il WAF deve essere posizionato tra la DMZ e il Firewall della rete.

- Eseguire patch e aggiornamenti regolarmente

- Implementare policy di sicurezza anche a livello di Firewall di rete e di Applicazione, così da avere un ulteriore doppia protezione e co



2. **L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione per 10 minuti.**
   Calcolare l'impatto sul business dovuto al disservizio, considerando che in media ogni minuto gli utenti spendono 1.200€ sulla piattaforma di e-commerce.
   Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Se in un minuto di inattività la perdita è mediamente di 1.200€, in 10 minuti si avrà una SLE massima stimata di 12.000€.
Ci sono delle possibili azioni preventive che si possono applicare per risolvere/mitigare questa problematica.

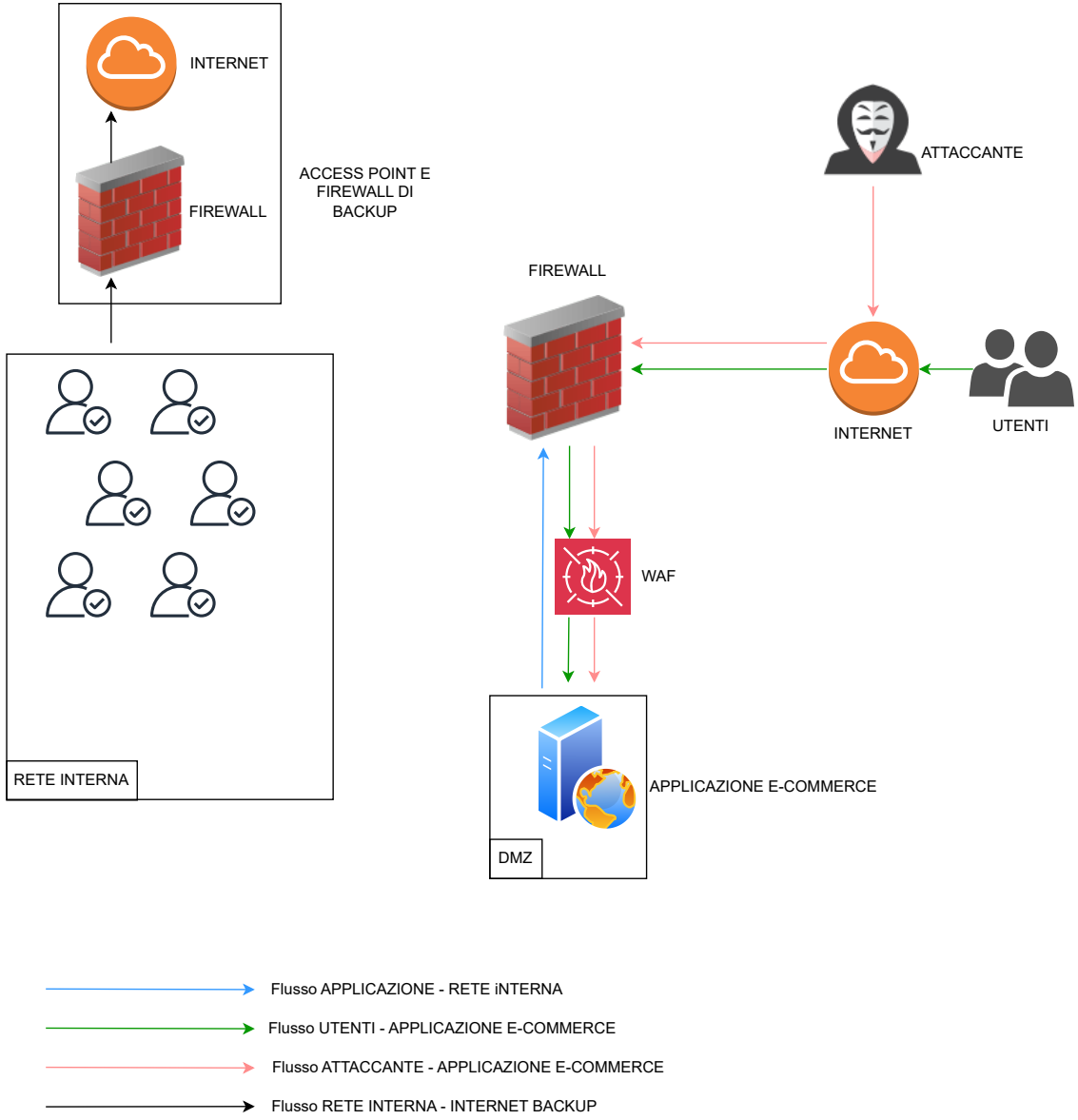
- **Soluzioni contro gli attacchi DDoS:** implementare software/hardware progettati appositamente per riconoscere gli attacchi di questo tipo e andare a proteggere la disponibilità dei servizi. Ad esempio utilizzare servizi cloud che rilevano e mitigano questi attacchi e che supportano l' auto-scaling per aumentare automaticamente le risorse in risposta a eventuali picchi di traffico.

- **Monitoraggio attivo con SIEM e SOAR:** Il SIEM raccoglie, analizza e correla i dati i log e gli eventi di sicurezza tra i vari dispositivi e applicazioni in tempo reale fornendo visibilità centralizzata e allarmi sugli incidenti di sicurezza. Il SOAR integra strumenti di sicurezza per automatizzare e orchestrare le risposte agli incidenti, migliorando l'efficienza operativa e riducendo i tempi di reazione.

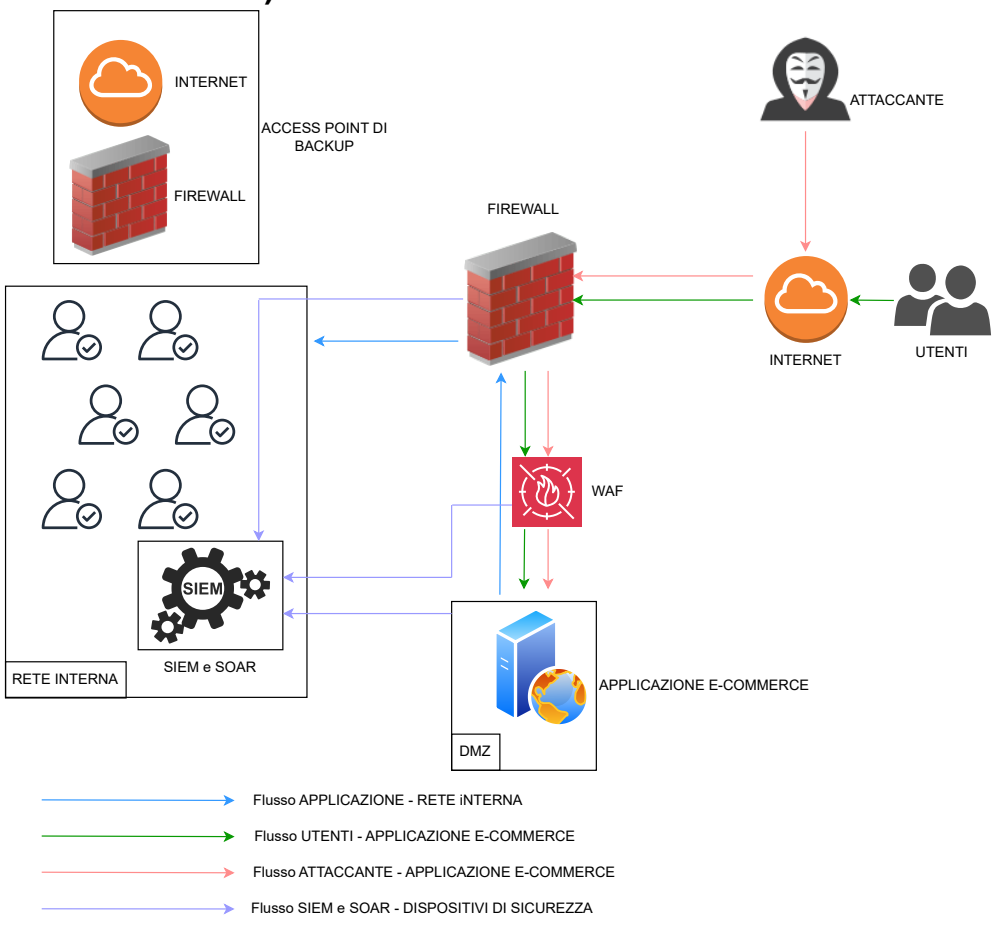
- **Backup e ridondanza:** Per evitare le possibili perdite è fondamentale avere un copia di tutti i servizi e asset critici. Oltre che il backup costante dei dati è importante avere un duplicato di tutto i componenti già configurati e aggiornati, pronti per essere attivati in caso di attacchi o incidenti.

3. **L'applicazione Web viene infettata da un malware.**
   La priorità è che il malware non si propaghi sulla vostra rete,
   è anche utile non rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

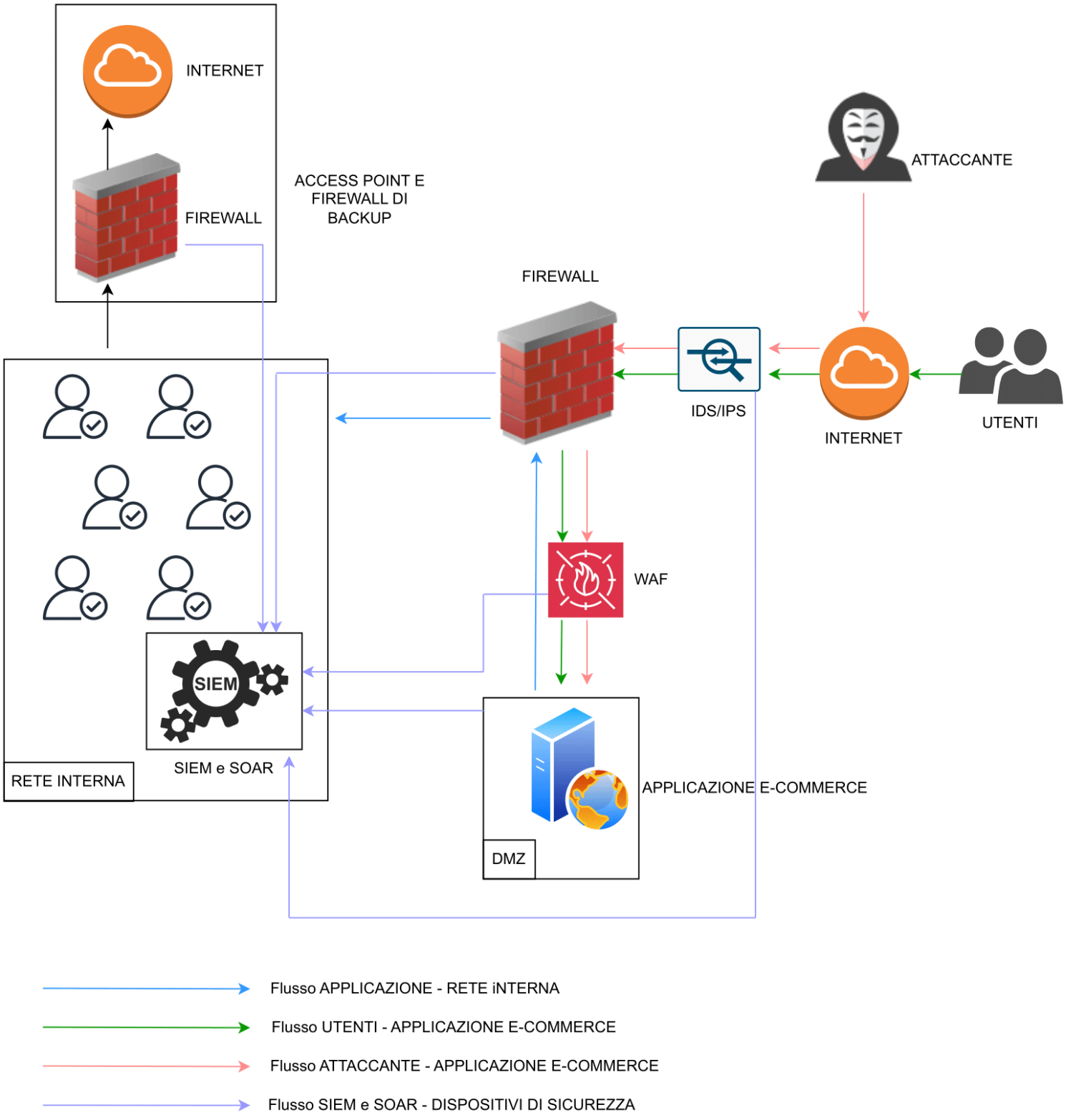
Per prima cosa il **CSIRT** andrà a isolare la macchina infettata **scollegandola dalla rete interna**. Per garantire l'accesso a internet dalla rete interna è importante predisporre soluzioni di backup, ad esempio avere un access point e un firewall già configurati, da attivare in questi casi.
E' importante **non rimuovere** l'accesso dell'attaccante e **non spegnere** la macchina infettata per consentire al CSIRT di effettuare un **analisi forense** con lo scopo di capire la **natura dell'attacco** e le **vulnerabilità sfruttate**.
Poi inizierà la **fase di ripristino** della macchina compromessa utilizzando versioni di backup verificate e non compromesse.
Infine con tutte le informazioni ottenute il CSIRT lavorerà per **rinforzare le misure di sicurezza per prevenire gli attacchi futuri.**



4. **unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)**



5. **Modifica «più aggressiva» dell'infrastruttura integrando eventuali altri elementi di sicurezza. Budget 5000-10000 euro.**



La soluzione proposta è in parte realizzabile con un investimento iniziale a partire dai 6.000€ non implementando SIEM e SOAR (15.000€ + 15.000€)

- Soluzione più economica a partire da 6.000€ (senza SIEM e senza SOAR)
- Soluzione completa a partire da 36.000€ (utilizzando hardware con i requisiti minimi e utilizzando soluzioni cloud-based e/o open source)

Con un budget di 5.000€-10.000€ è possibile migliorare la sicurezza della rete ma resta comunque non sufficiente, soprattutto considerando le SLE degli asset presenti.

Per fare un esempio, calcolando l' ALE di un attacco DDoS all' applicazione di E-Commerce della durata di 60 minuti (durata breve) e considerando un ARO di 1 (prudenziale) l'aziende può potenzialmente perdere 72.000€ all'anno a causa di attacchi DDoS.

SLE (60 minuti offline)	ARO	ALE
72.000	0,3	21.600
	0,5	36.000
	0,8	57.600
	1	72.000
	1,5	108.000
	2	144.000

Da questi calcoli si può osservare come un attacco DDoS della durata di 60 minuti (tempo molto basso considerando le attuali condizioni) ricevuto dalle 0,3 alle 2 volte in un anno può portare all'azienda una perdita annua stimata dai 21.600€ ai 144.000€.