



# ESECITAZIONE

S9 - L5



MICHELANGELO BORROMEO

# TRACCIA

**01**

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?

**02**

Impatti sul business : l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

**03**

Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre reti, 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 .

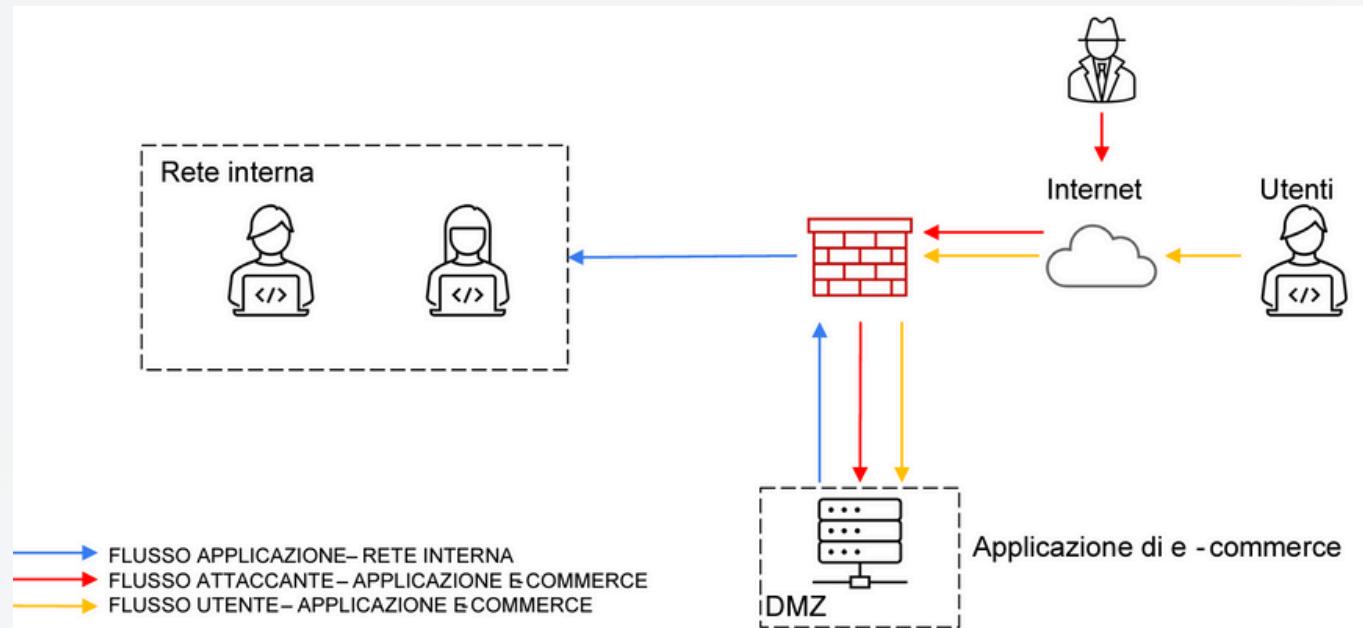
**04**

Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

**05**

Modifica «più aggressiva» dell'infrastruttura: anche una soluzione al punto 2) integrando eventuali altri elementi di sicurezza budget 5000-10000€

# AZIONI PREVENTIVE

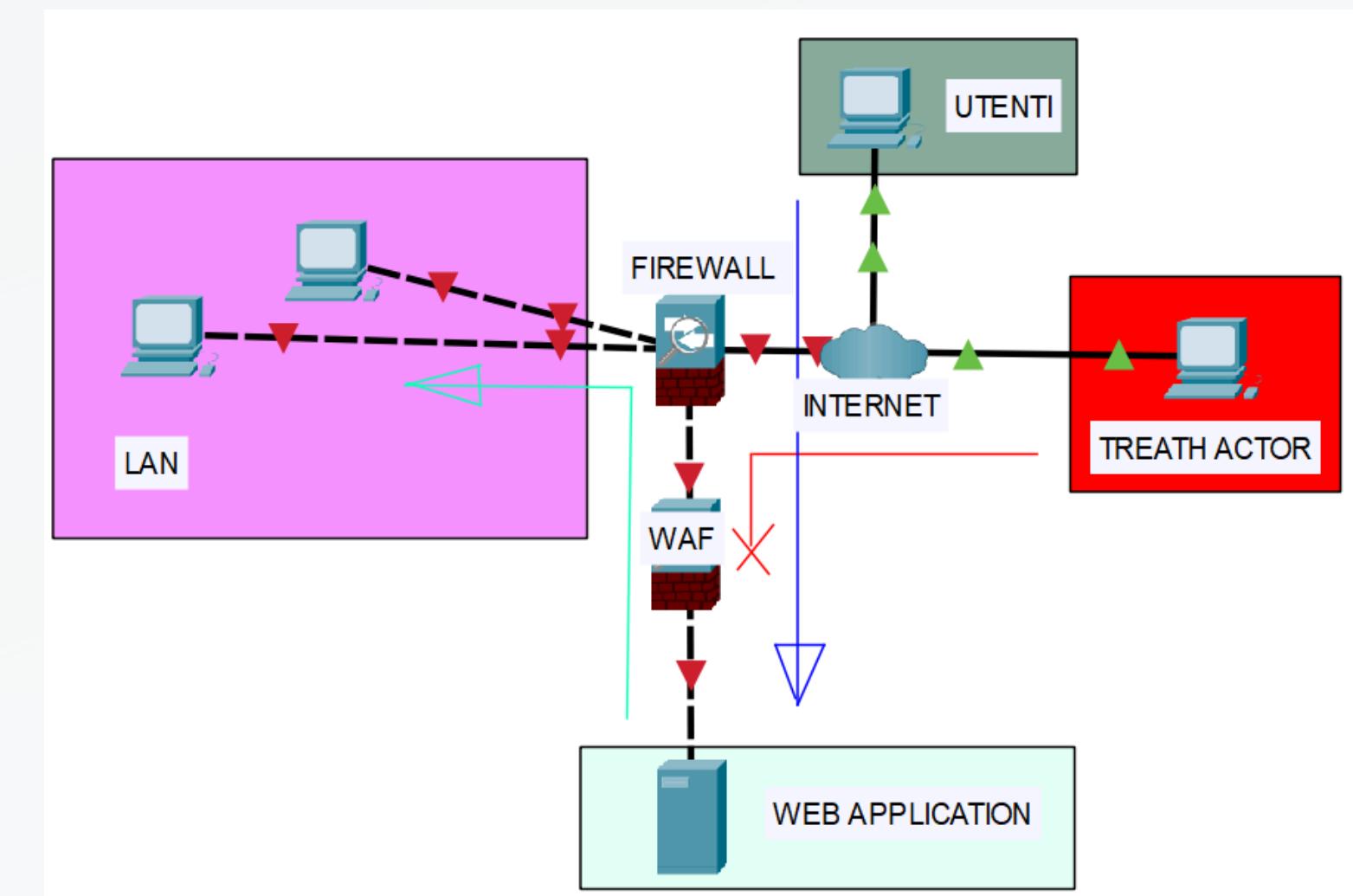


Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

Si consiglia di applicare il WAF ( Web Application Firewall ) progettato per proteggere le applicazioni web da attacchi comuni come SQL injection, cross-site scripting (XSS), file inclusion, e altri attacchi che mirano a sfruttare le vulnerabilità dell'applicazione web.

Il WAF analizza il traffico HTTP che entra ed esce dall'applicazione web per individuare attività sospette o dannose.

( Il traffico tra l'applicazione nella DMZ e la rete interna non necessita di passare attraverso il WAF se si considera che la rete interna è di fiducia. )



# BUSINESS IMPACT

l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce .  
Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

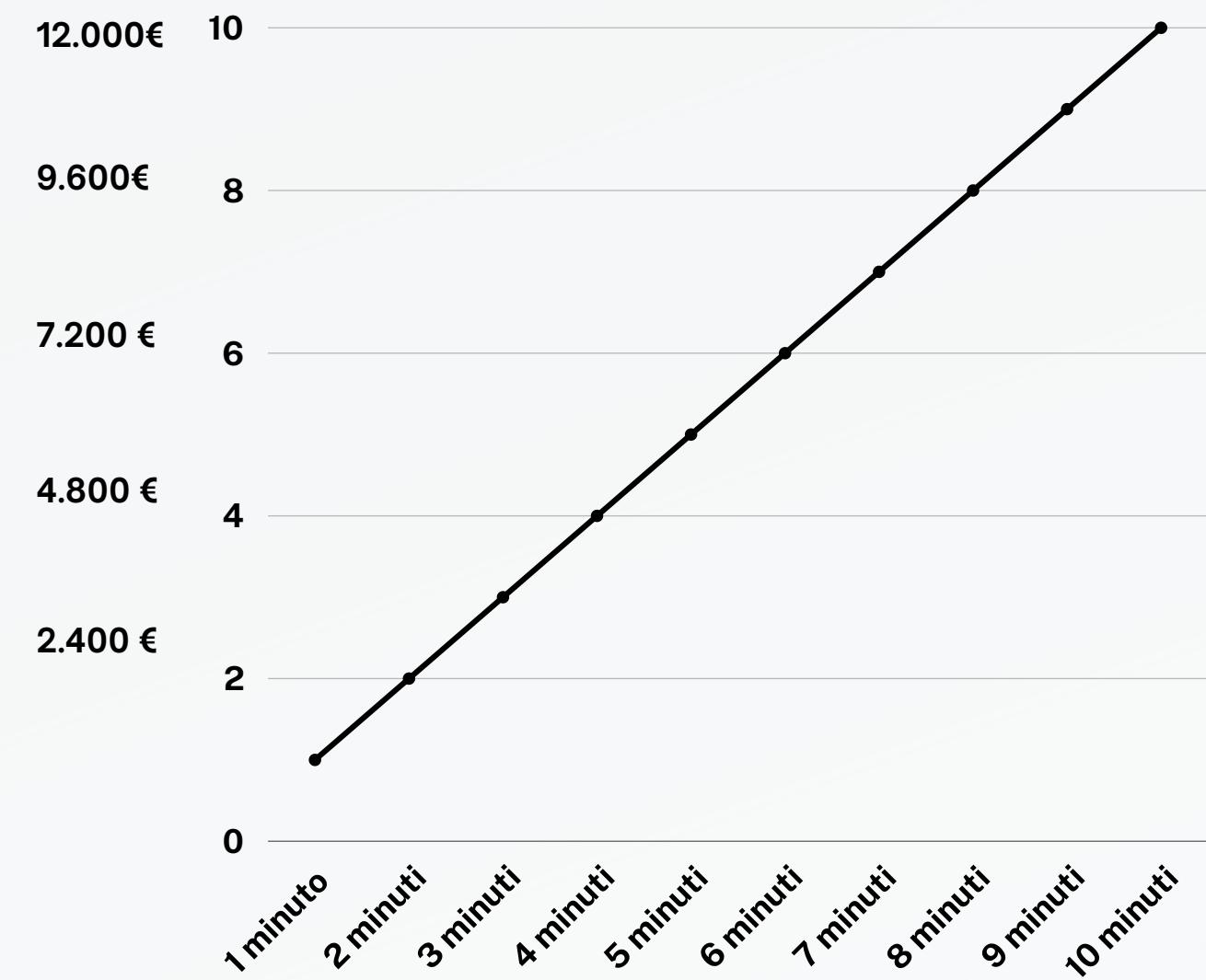
Se gli utenti spendono in media 1.200 € al minuto sulla piattaforma di e-commerce,  
la perdita di entrate per 10 minuti di inattività può essere calcolata come:

**Perdita di entrate = minuti di interruzione X entrata al minuto**

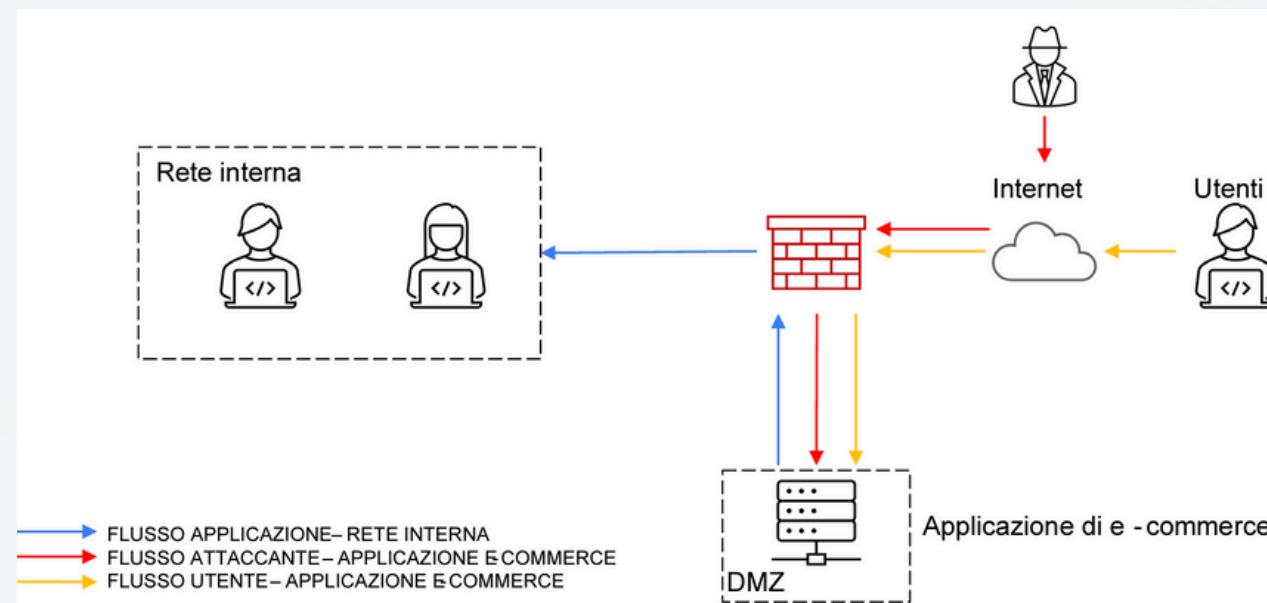
**Perdita di entrate = 10 minuti X 1.200 al minuto = 12.000€**

Per prevenire un interruzione del servizio a causa di un attacco si potrebbero:

- Implementare sistemi che monitorano il traffico di rete per rilevare attività sospette e possono bloccare automaticamente gli attacchi in corso come **IDS/IPS**
- Avere piani di Disaster recovery e backup pronti per essere attivati rapidamente in caso di attacco. immettendo un dispositivo come il “ **Raid 5** ” così che il traffico possa essere reindirizzato ad un server di backup senza interruzione. E’ importante effettuare backup regolari dei dati in modo che possano essere recuperati in caso di perdita di dati o attacco.



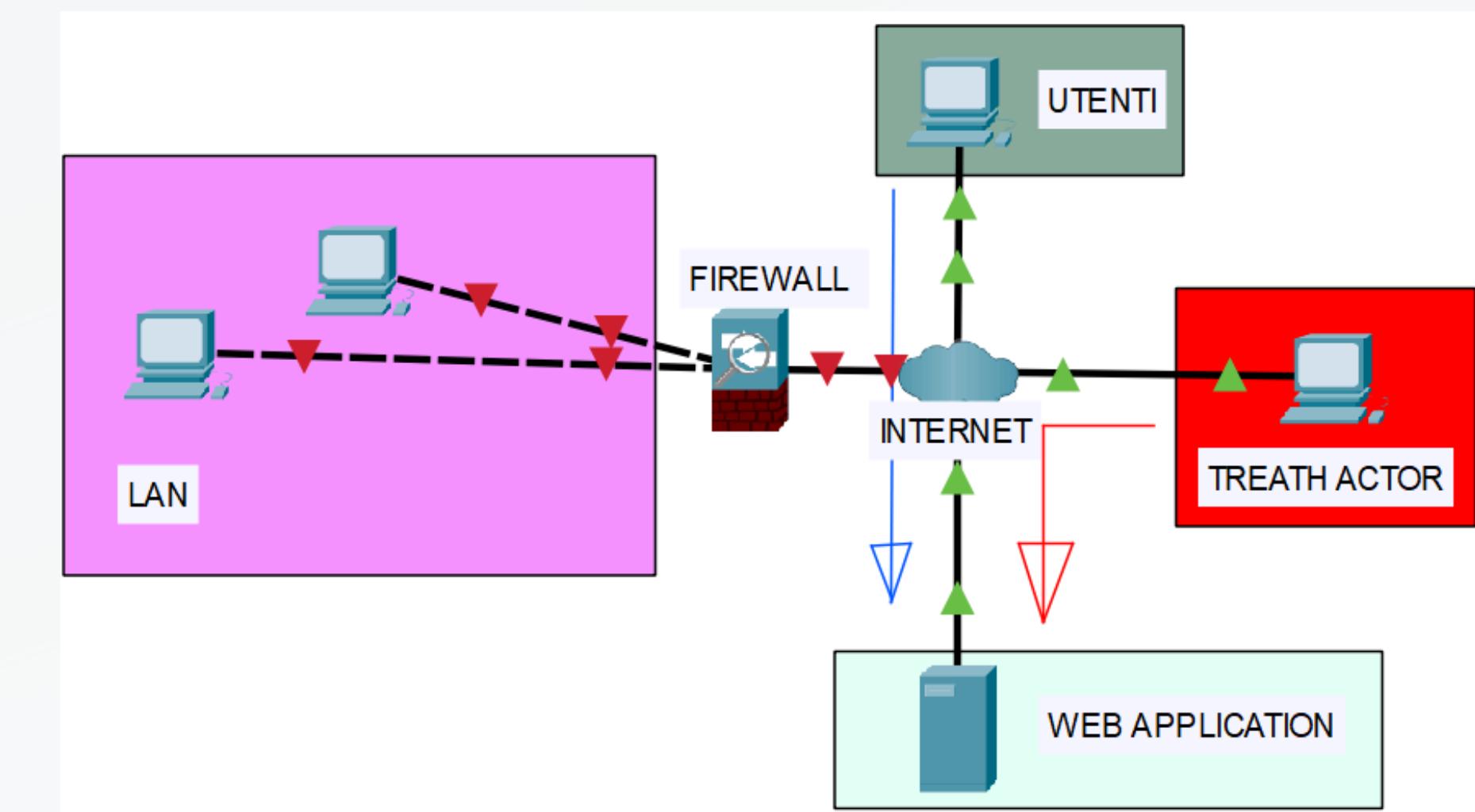
# INCIDENT RESPONSE



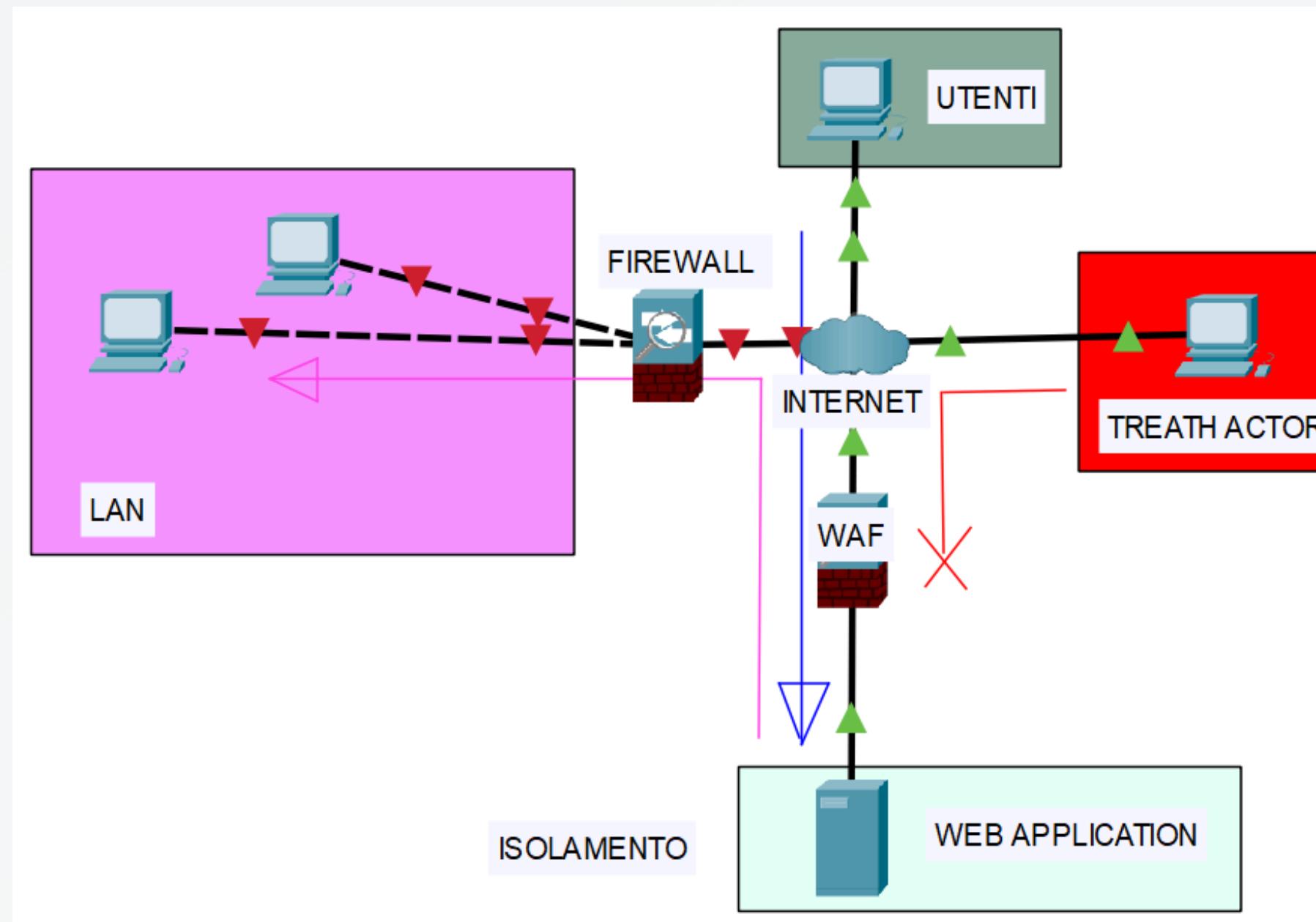
Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.  
Modificate la figura in slide 2 con la soluzione proposta .

Una delle fasi di Incident Response è l'isolamento, e consiste nel disconnettere completamente il sistema infetto dalla rete locale, limitando l'accesso dell'attaccante alla rete interna.

Tuttavia la macchina è ancora connessa ad internet ( 4G ) così da poter analizzare i vettori di attacco ed avere più informazioni sulle dinamiche sull'attaccante



# SOLUZIONE COMPLETA



- Combinare azione preventiva e incident response offre una strategia di sicurezza completa e resiliente, che non solo previene gli attacchi ma assicura anche una risposta efficace quando gli attacchi si verificano.
- Questo approccio integrato migliora la capacità dell'organizzazione di proteggere le proprie risorse, limitare i danni e recuperare rapidamente, mantenendo la continuità operativa e la fiducia degli utenti.

# AGGRESSIVE SOLUTION

Migliorare la sicurezza della rete integrando eventuali altri elementi di sicurezza budget 5000-10000€

Rilevamento e Prevenzione delle Intrusioni (IDS/IPS):

- IDS: Monitora il traffico di rete per rilevare attività sospette o malevoli e avvisa gli amministratori.
- IPS: Oltre a rilevare, blocca attivamente gli attacchi identificati.

**IPS / IDS**

Snort (Open Source)

Gratuito

eventuale supporto 1.000€

Suricata (Open Source)

Gratuito

eventuale supporto 1.500€

# AGGRESSIVE SOLUTION

Logging e Monitoraggio (SIEM e SOAR):

- Registrazione degli Eventi: Il firewall perimetrale registra i log di accesso e le attività, compresi i tentativi di accesso bloccati e le connessioni consentite.
- Monitoraggio Continuo: Gli amministratori possono monitorare il traffico in tempo reale per rilevare attività sospette e rispondere tempestivamente agli incidenti.

**SIEM**

LogRhythm  
4.200€  
all'anno

**SOAR**

Cortex XSOAR  
4.000€  
all'anno

Elastic Security  
3.500€  
all'anno per supporto

TheHive  
1.500€  
all'anno per supporto

# AGGRESSIVE SOLUTION

Ridondanza di Software:

- Failover Software: Software che monitora lo stato dei sistemi e può trasferire automaticamente il controllo a un sistema di backup in caso di guasto.  
Esempi: Cluster di failover, database replicati.
- Backup dei Dati: Copie regolari dei dati su supporti diversi o in posizioni diverse per garantire il ripristino in caso di perdita dei dati

**BACKUP  
SOFTWARE**

Veeam Backup & Replication

1,300€  
all'anno

Acronis Cyber Backup

1,000€  
all'anno

# AGGRESSIVE SOLUTION

Ridondanza di Hardware:

- Server Ridondanti: Utilizzo di server di backup che possono subentrare in caso di guasto del server principale. Esempi: Cluster di server, RAID (Redundant Array of Independent Disks) per dischi rigidi.
- Alimentazione Ridondante: Utilizzo di più unità di alimentazione per garantire che un singolo punto di guasto nell'alimentazione non comprometta l'intero sistema. Esempi: Alimentatori ridondanti nei server, UPS (Uninterruptible Power Supply) per continuità elettrica.

## RAID

Seagate IronWolf Pro

600€

Senza dischi

LSI MegaRAID

300€

Senza dischi

## HDD

Toshiba N300 4TB

100€ cadauno

Seagate IronWolf 4TB

250€ cadauno

## UPS

UPS(power supply)

APC X 2000VA

1.200€

CyberPower

500€

# AGGRESSIVE SOLUTION

Calcolo totale spesa per 1 anno

articoli	articoli	unità	prezzo
IDS / IPS	Snort (Open Source)	1	1.000 €
SOAR	Thehive	1	1.500 €
SIEM	LogRhythm	1	4.200 €
BACKUP SOFTWARE	Veeam Backup & Replication	1	1.200 €
RAID 5	Seagate IronWolf Pro	1	600 €
HDD	Toshiba N300 4TB	4	400 €
UPS	APC Smart-UPS X 2000VA	1	1.200 €
	<b>TOTALE</b>	10	<b>10.100 €</b>

# AGGRESSIVE SOLUTION

Calcolo totale spesa per 1 anno

articoli	articoli	unità	prezzo
IDS / IPS	Suricata (Open Source)	1	1.500 €
SOAR	XSOAR	1	3.000 €
SIEM	Elastic security	1	3.000 €
BACKUP SOFTWARE	Acronis Backup	1	1.000 €
RAID 5	LSI megaRAID	1	300 €
HDD	Seagate IronWolf 4TB	4	1000 €
UPS	CyberPower	1	500 €
	<b>TOTALE</b>	<b>10</b>	<b>10.300 €</b>