MJL cooperation

# PROGETTO S9/L5

*Joel Landry MOUAFO*

# Indice

# Traccia del progetto

Con riferimento alla figura del progetto, 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 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 € Esercizio Traccia e requisiti DDoS dall'esterno che rende 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 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 .

4. Soluzione completa : 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 necessario/facoltativo magari integrando la soluzione al punto 2)

# *Introduzione*

Abbiamo una rappresentazione dell'architettura di rete di un'applicazione di e-commerce, evidenziando i flussi di dati tra diverse componenti e i possibili vettori di attacco. Faremo una security Operation rispondendo agli quesiti di **azioni preventive,impatti sul business, response, soluzione completa contro l’attacco e i modifiche delle’infrastruttura  per evitare altri attacchi.**

Torna all'indice

# Azioni preventive

# Azioni preventive

Gli **attacchi SQLi** sono un tipo di attacco informatico in cui un hacker inserisce del codice dannoso nei campi di input di un sito web per far eseguire commandi non autorizzati al database e gli **attacchi XSS** sono problemi di sicurezza del codice dannoso in una parte sel sito che memorizza i dati come un commento o un profilo utente.

Per difendere quelli attacchi sarebbe possibile implementare azioni preventive come il filtraggio e validazione input,sanitizzazione degli output, inserire patch di sicurezza , firewall applicativi...

- **Filtraggio e validazione input**: verificare e filtrare tutti i dati in ingresso per rimuovere contenuti dannosi (codice javascript corrotti)
- **Sanitizzazione degli output**: monitorare la visualizzazione dagli utenti siano sicuri per prevenire XSS.

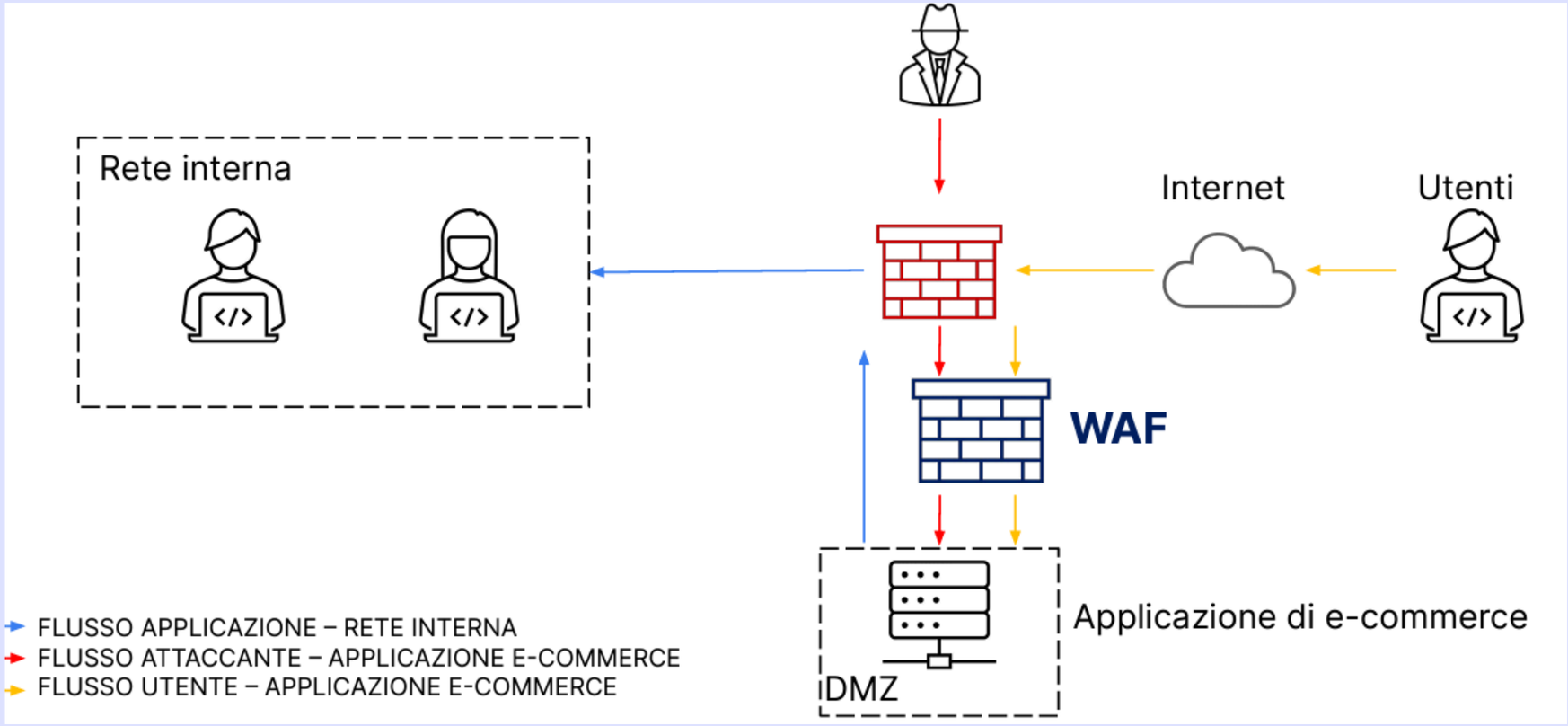
# Azioni preventive

- **Patch di sicurezza:** mantenere aggiornati tutti i software, inclusi server web e data base per correggere eventuali vulnerabilità.
- **Firewall applicativi (WAF)** implementa un web application Firewall per monitorare e filtrare traffico HTTP danoso. A differenza dei fairewall standard, sono dedicati per proteggere le web App da attacchi XSS e SQLi.

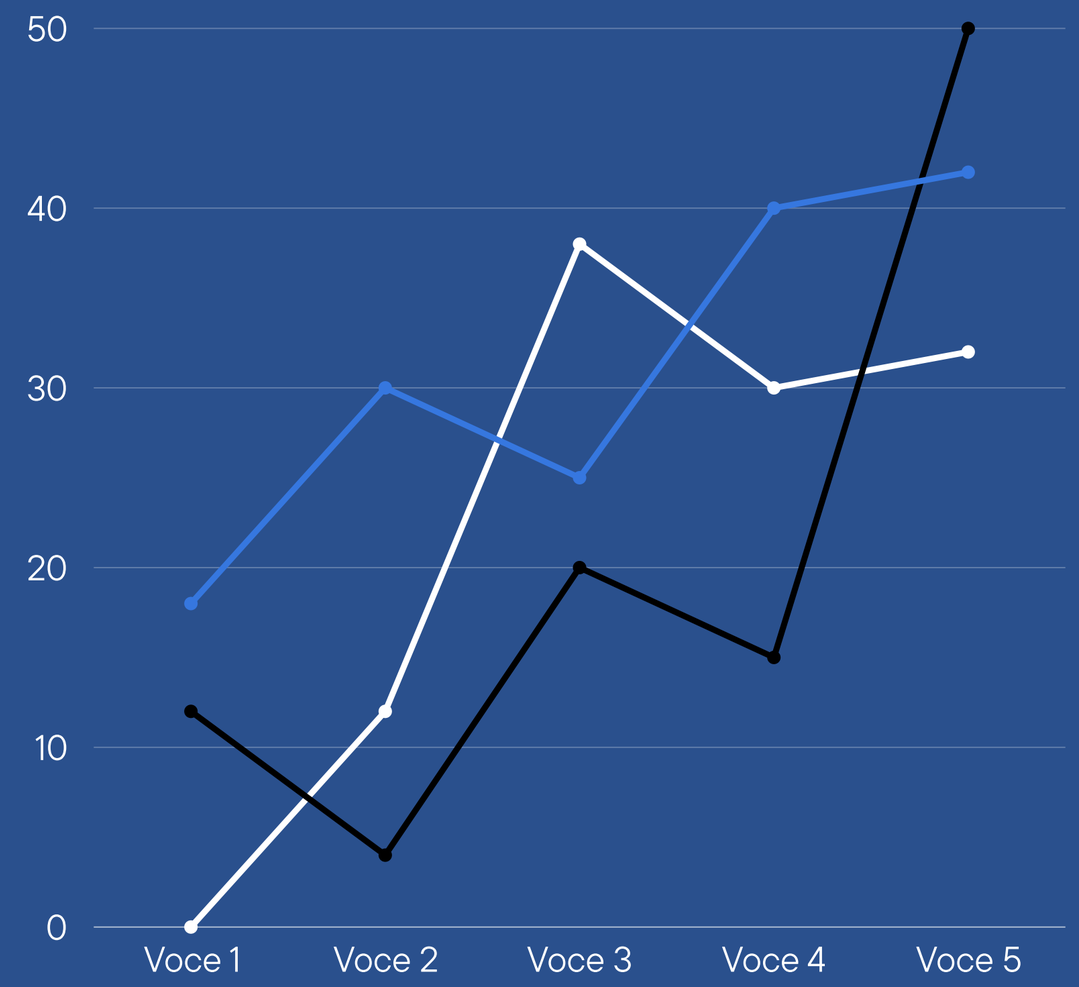
Nella rappresentazione della rete, aggiunggiamo un firewall applicativo tra Internet e l'applicazione di e-commerce nella DMZ tale che l'applicazione di e-commerce deve essere disponibile per gli utenti per effettuare acquisti sulla piattaforma. La figura seguite è la rappresentazione dell'architettura di rete:

# Azioni preventive

Torna all'indice



# Impatti sul business




Torna all'indice

# Impatti sul business

Un attacco di tipo **DDoS(Distributed Denial Of Service)** è un tentativo di rendere un servizio online non disponibile per gli utenti legittimi ,sovraccaricando il sito web o il server con un enorme volume di traffico internet. Nel nostro caso ,l'applicazione web subisce un attacco DDoS dall'essterno che la rende non raggiungibile per **10  minuti**, l'impatto sul business può essere significativo.
Se ogni minuti gli utenti spendono in media **1500 €**, l'interruzione di **10 minuti** può causare una perdita di:
**1500 € X 10 = 15000 €.**

Torna all'indice

# Impatti sul business

**Azioni preventive:**

- **Monitoring e alerting:** aiuterà a monitorare costantemente il traffico e impostare alert per rilevare e rispondere rapidamente agli attacchi.
- **Limitazione della larghezza di banda**: limitare la larghezza di banda per prevenire sovraccarichi sull'applicazione web.

Torna all'indice

# Response

Torna all'indice

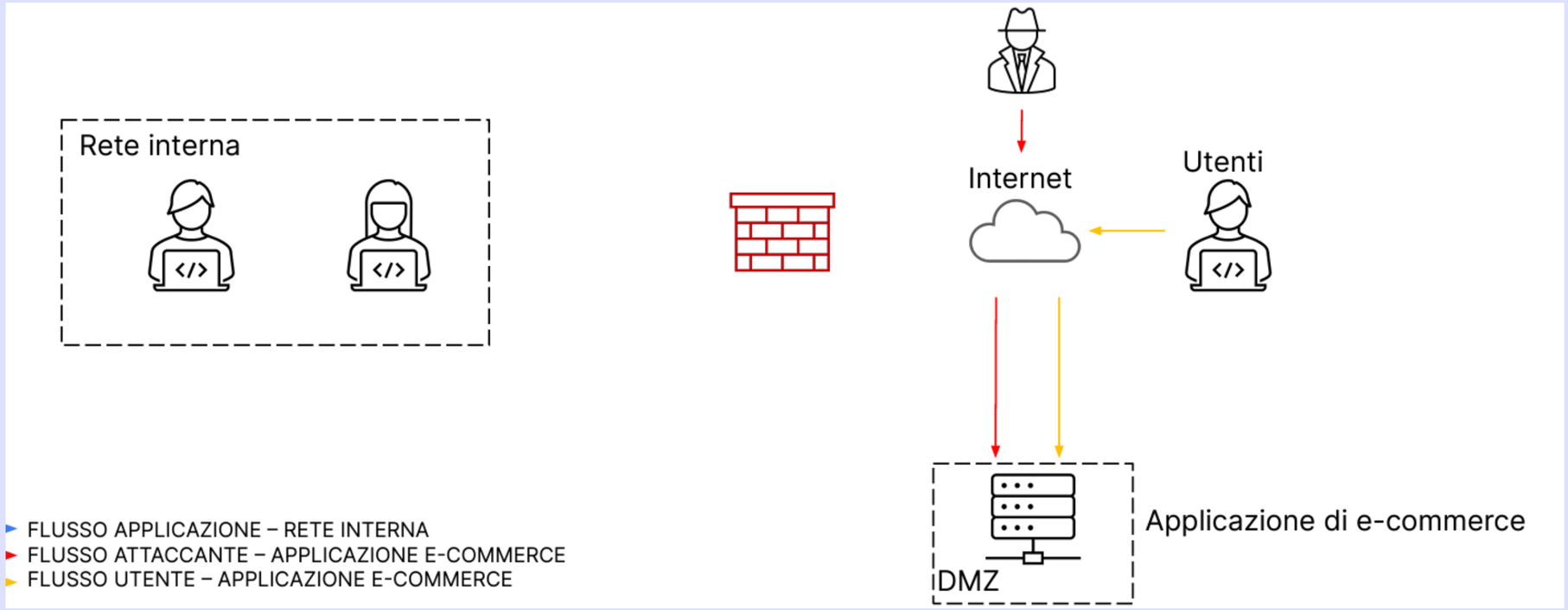
# Response

Siamo stati infettata da un malware e la nostra priorità è che il malware non si propaghi sulla nostra rete. Per quello possiamo procedere all’isolamento immediato rimuovendo anche l’accesso agli attaccanti e avviare un’analisi forense per identificare e risolvere la vulnerabilità attraverso un modulo di risposta agli incidenti. Cosi fatto l’attacante non potrà più connessa alla rete interna. La macchina infetta sarà direttamente collegata ad internet.

Torna all'indice

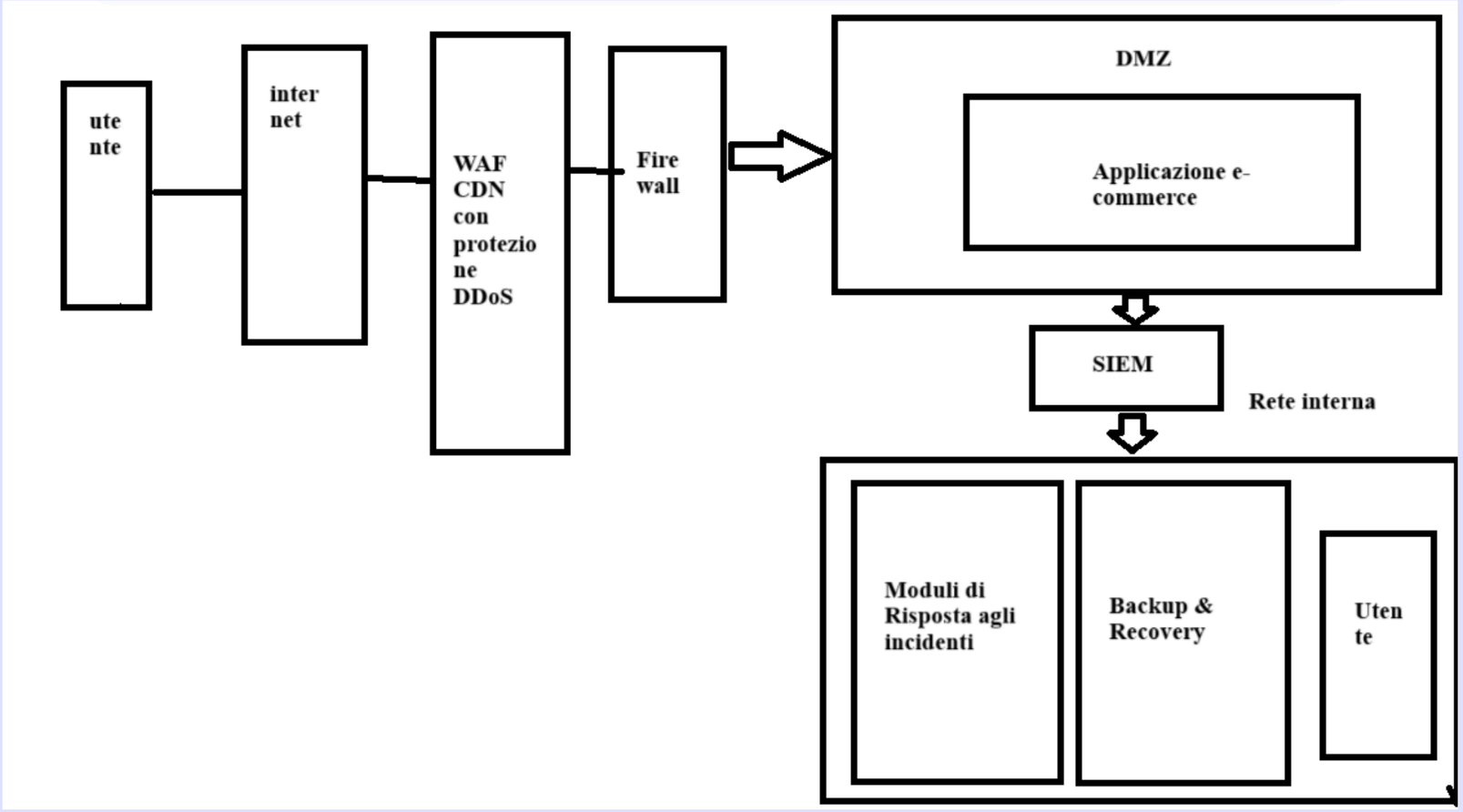
# Response

Torna all'indice



# Soluzione completa

# soluzione completa



# soluzione completa

Nella figura precedente abbiamo una representazione di architettura di rete più sicura con soluzione complete per gli incidenti di sicurezza con diversi componenti.

- **WAF(Web Application Firewall)** posizionato tra Internet e la DMZ. Protegge l'applicazione web da **attacchi SQLi e XSS.**
- **CDN( Content Delevery Network)** con protezione DDoS mitiga gli attacchi DDoS e distribuisce i contenuti per un accesso più veloce.
- **Firewall** controlla il traffico in ingresso e in uscita tra internet e la DMZ
- **SIEM(Security Information and Event Management)** per il monitoraggio centralizzato degli eventi di sicurezza, rilevamento delle minacce e risposta

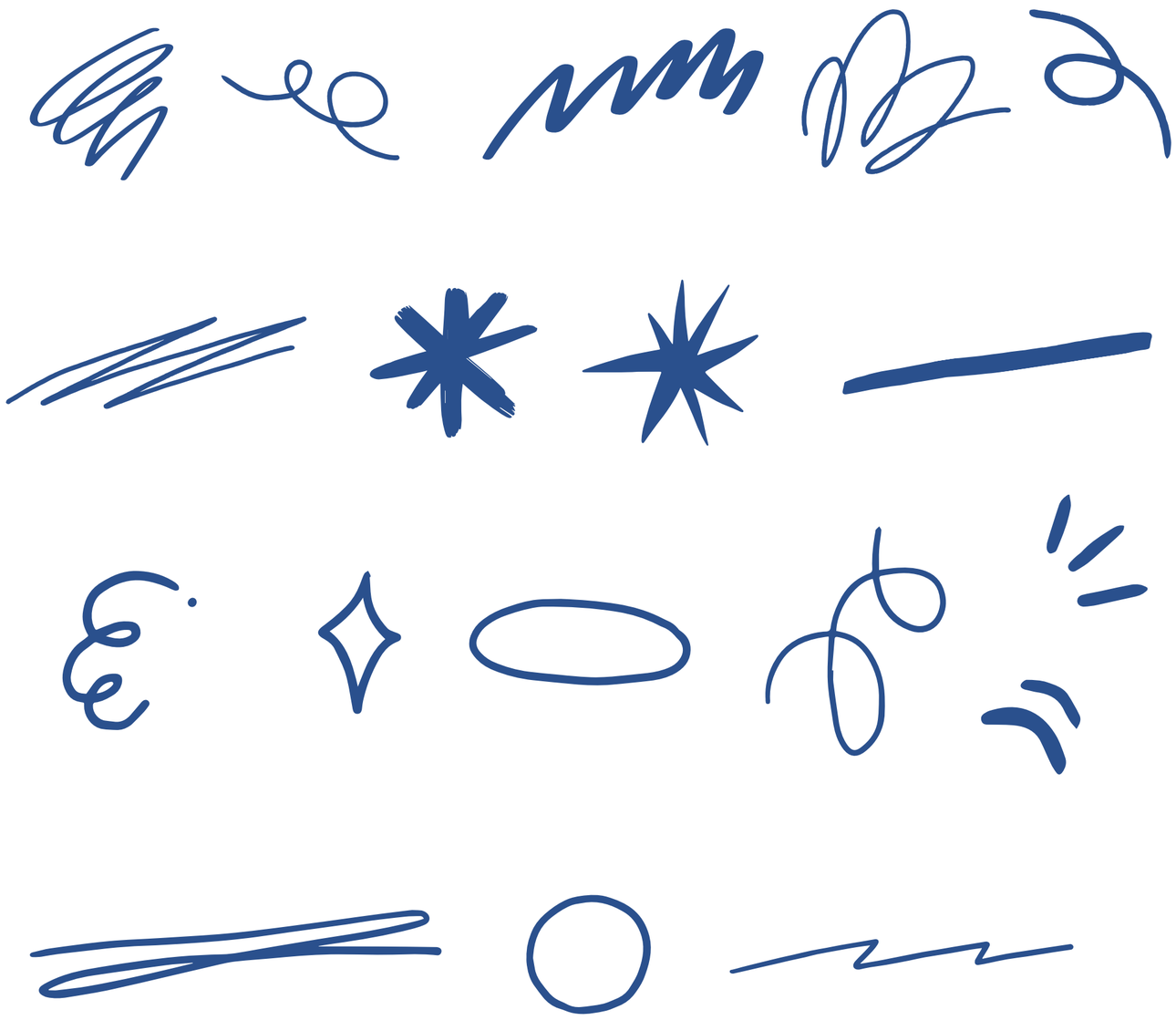
Torna all'indice

# soluzione completa

- **Moduli di risposta agli incidenti** per l’isolamento e risposta per gestire gli incidenti di sicurezza in tempo reale.
- **Backup & Recovery**: Piani di backup regolari e strategie di disaster recovery per garantire il pipristino rapido in caso di compromissione
- **Segmentazione della rete** implementata tra DMZ e  rete interna per limitare il movimento laterale degli attaccanti e migliorare la sicurezza complessiva.

Torna all'indice

# Conclusione

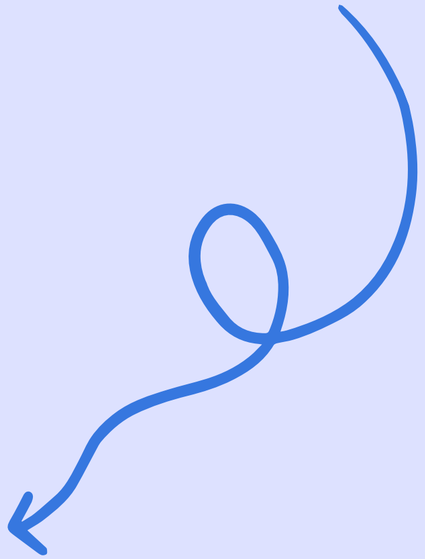


# conclusione

Torna all'indice

L’architettura aggiornata offre una protezione più robusta contro le minacce alla sicurezza, minimizzando l’impatto degli attacchi sul business e garantendo la continuità operativa attraverso l’inserimento degli elementi come WAF, CDN,SIEM e moduli di risposta agli incidenti.

# Grazie per l'attenzione!



Torna all'indice