



VT del firewall

Progetto di Architettura di Rete per Theta Co.

Proposta Tecnica e Preventivo

Presentato da: VT Firewall S.r.l.

17 ottobre 2025

Rif: PRI-THETA-2025-V1.0

Sommario Esecutivo

Obiettivo del Progetto:



Dotare la Compagnia Theta di un'infrastruttura di rete resiliente e all'avanguardia, per **proteggere i dati** critici, supportare la crescita e adattarsi alle future sfide tecnologiche.



Scopo:



Supportare 120 postazioni utente

Progettare e configurare i sei piani dell'immobile

Garantire la massima sicurezza e protezione dei dati



Approccio Strategico e Visione architeturale



Architettura basata sulla Segregazione Dati:

L'architettura è stata definita per segregare i dati in base alla loro criticità su un'infrastruttura di rete a più livelli, garantendo una protezione modulare e rafforzata.



Piani ad Alto Rischio e Legati ai Dati



Identificazione dei Piani con Dati Sensibili:

- Piano Terra: IT e Infrastruttura
- Primo Piano: Risorse Umane e Legale
- Secondo Piano: Commerciale e Marketing
- Terzo Piano: Produzione e Logistica
- Quarto Piano: Ricerca e Sviluppo (R&S)
- Quinto Piano: Amministrazione, Finanza e Controllo

Ogni piano è stato analizzato per definire i livelli di rischio e i requisiti di sicurezza specifici.



Principi Fondamentali della Sicurezza

Obiettivo: Illustrare le strategie chiave adottate per garantire la robustezza e l'integrità dell'infrastruttura di rete, con particolare attenzione alla protezione dei dati sensibili e alla prevenzione delle minacce.

Segregazione & Controllo Accessi



- Segregazione di Rete (VLAN): Isolamento logico dei dipartimenti e dei dati sensibili, prevenendo la diffusione laterale di eventuali compromissioni.



- Firewall Dedicati (Perimetrali e Interni): Controlli di accesso granulari e rafforzati, implementati sia al perimetro della rete sia all'interno, a livello di ciascun piano.



Monitoraggio e Protezione Avanzata



- **Sistema IDS/IPS Integrato:** Monitoraggio continuo del traffico di rete e prevenzione proattiva delle minacce su più livelli dell'architettura.

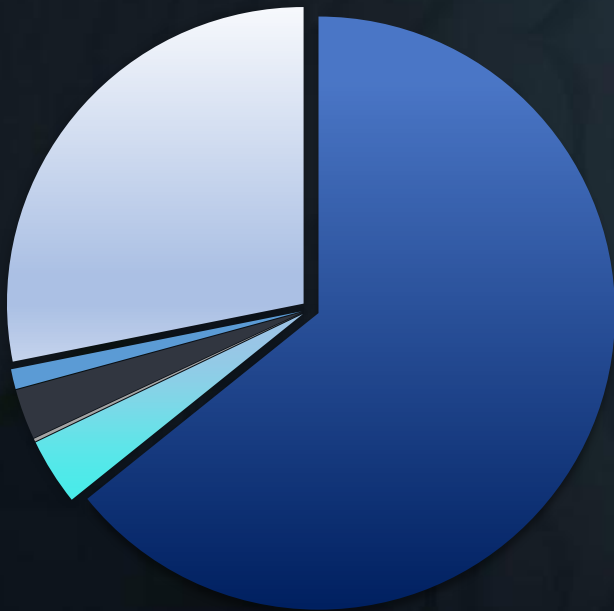
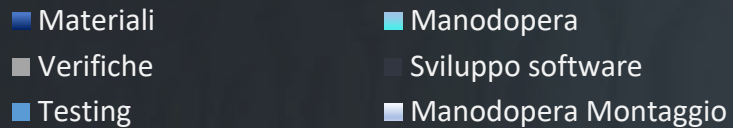


- **DMZ (Zona Demilitarizzata) per Servizi Esposti:** Isolamento sicuro delle risorse accessibili dall'esterno (es. Web Server), minimizzando la superficie di attacco.



Costo Totale Progetto

Il budget complessivo è stato allocato strategicamente per coprire tutte le fasi e i componenti necessari all'implementazione dell'infrastruttura di sicurezza.



Ripartizione Dettagliata dei Costi:



Materiali (€ 96.315,14): Questa voce rappresenta la componente più significativa, includendo l'acquisto di hardware, licenze software essenziali e gli elementi fisici dell'infrastruttura.



Manodopera (€ 45.180): Copre le ore lavorative necessarie per l'installazione fisica, la configurazione iniziale e l'integrazione di tutti i sistemi di sicurezza.



Sviluppo Software (€ 3.900): Include eventuali costi per lo sviluppo o la personalizzazione di script e l'ottimizzazione del Web Server per test specifici.



Testing (€ 1.550): Allocated per le attività di verifica, test di vulnerabilità (VAPT) e simulazioni di attacco per assicurare la robustezza del sistema.

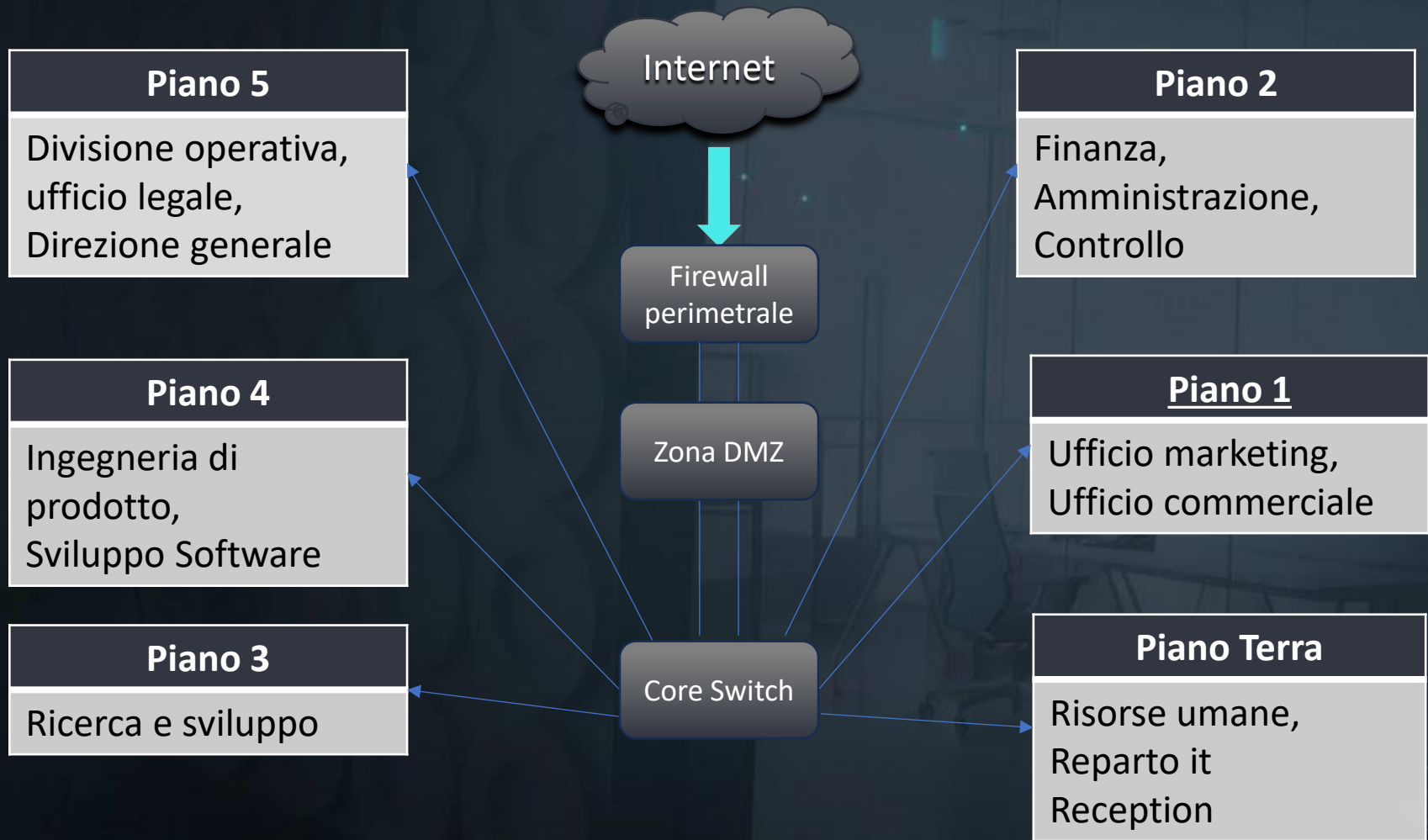


Verifiche (€ 225): Costi relativi alle ispezioni e alle verifiche finali della conformità del sistema rispetto ai requisiti e agli standard stabiliti.

TOTALE STIMATO: 142.170,14 €



Rete



Architettura della Zona Demilitarizzata (DMZ)

Dettagli sulla configurazione di sicurezza per il perimetro esterno.



Strategia "Defense in Depth"

- **Isolamento Completo**
- **Contenimento:** Evita propagazione attacchi da Web Server.



Componenti Chiave DMZ

- **Web Server DVWA**
- **Firewall (Esterno)**
- **IPS (Interno DMZ)**



Connessione Rete Interna

- **Punto di Filtraggio Aggiuntivo (IPS)**
- **Router Core**

Posizionamento Strategico IDS

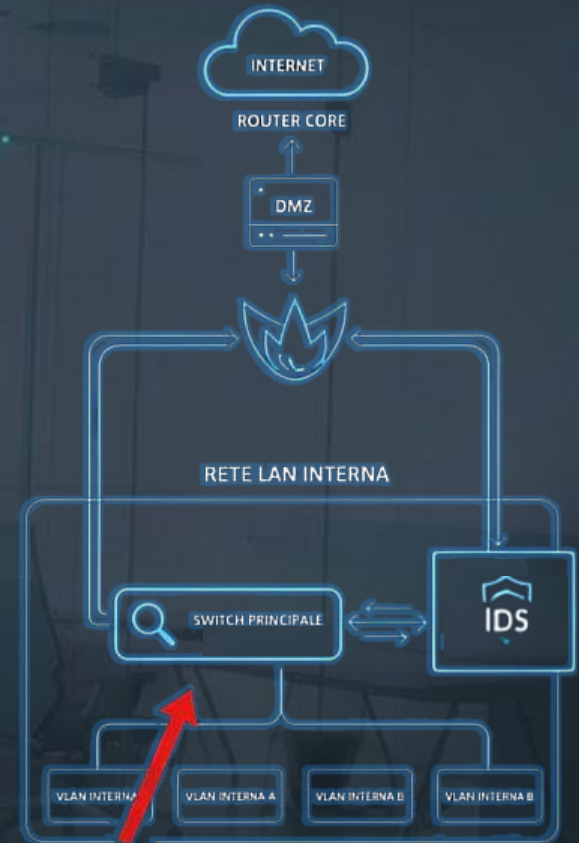
Punti Chiave del Posizionamento IDS:

Connessione allo Switch Più Esterno:

- L'IDS è direttamente collegato allo switch principale del piano terra,
- **Monitoraggio del Traffico di Confine**
- **Rilevamento Precoce**

Funzione di Sicurezza Cruciale:

- Agisce come un sensore sentinella, allertando o bloccando (se configurato come IPS) le minacce al "confine" della rete interna, complementando la protezione del firewall.
- Contribuisce in modo significativo alla strategia di "Difesa in Profondità", aggiungendo un livello di ispezione interna dopo il firewall perimetrale.



Punto Chiave di Monitoraggio
Traffico in Entrata



Configurazione Segmentazione Logica

Architettura per l'isolamento e la Scalabilità della rete



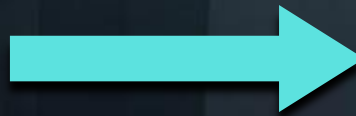
Strategia di Segmentazione Logica

- Implementata basandosi sull'analisi della sensibilità dei dati.
- Richiede una configurazione precisa a livello del Router per gestire il traffico inter-VLAN.
- Garantisce l'isolamento dei reparti e la protezione dei dati critici.



Gestione Dinamica degli Indirizzi IP (DHCP)

- Adozione del protocollo DHCP per i 120 host aziendali.
- Configurato direttamente sul Router L3 (o su un Server DHCP dedicato) per servire le subnet di ciascuna VLAN.
- Assicura un'allocazione efficiente e automatica degli IP.



Dettagli di Configurazione Router (VLAN & DHCP).



Disattivazione Interfaccia Fisica

- Comando: interface GigabitEthernet0/0
- Comando: no ip address
- Obiettivo: Instradamento solo tramite Sub-interfacce

```
interface GigabitEthernet0/0  
># no ip address
```



Creazione Sub-interfacce Logiche

- Per ogni VLAN (es. VLAN 30): interface Gig0/0.30
- encapsulation dot1Q 30 (Tagging VLAN)
- ip address 192.168.30.1 255.255.255.0 (Default Gateway per VLAN 30)



Configurazione e DHCP Relay

- Su ogni Sub-interfaccia (es. interface Gig0/0.30)
- ip helper-address 192.168.10.10 (indirizzo IP del Server DHCP)
- Obiettivo: Inoltra richieste DHCP al Server Centrale.

```
ip helper-address 192.168.10.10
```

Piattaforma di Virtualizzazione e Ruoli delle VM

Piattaforma di Virtualizzazione:



VirtualBox

- Utilizzata come hypervisor principale...
- **Benefici:** Ottimizzazione dell'hardware...

Macchine Virtuali Chiave e Loro Funzioni:



pfSense (Firewall/Router Virtuale)

- **Ruolo:** Utilizzato come firewall interno
- **Funzioni:** Filtraggio avanzato del traffico



Kali Linux (Piattaforma di Penetration Testing)

- **Ruolo:** Ambiente dedicato all'esecuzione dei test
- **Funzioni:** Toolkit completo per vulnerability assessment



Metasploitable (Web Server DVWA)

- **Ruolo:** Server web deliberatamente vulnerabile
- **Funzioni:** Simula un'applicazione web con vulnerabilità comuni

Integrazione e Monitoraggio della Sicurezza di Rete (Suricata)

Dettagli Implementativi del Sistema di Rilevamento delle Intrusioni (IDS)

- **Sistema:** Network Intrusion Detection System (NIDS).
- **Tool:** Pacchetto Suricata (versione 7.0.8_1).
- **Piattaforma:** Integrato in pfSense.
- **Accesso:** Tramite il menu dei servizi di pfSense per configurazione e monitoraggio centralizzato.

Configurazione e Aggiornamento dei Set di Regole

Strategia di Difesa e Scelta delle Regole

- **Base Difensiva:** Utilizzo di set di regole aggiornati per massima copertura minacce.

- **Regole Installate:** **Emerging Threats Open Rules (ETOpen)**, risorsa open source essenziale.

Dettagli Configurazione e Aggiornamento

- **URL Custom per Download:**
<https://rules.emergingthreats.net/open/suricata-5.0.0/emerging.rules.tar.gz>
Assicura la corretta localizzazione della risorsa.
- **Frequenza Aggiornamenti:** Regolari.
- **Ultimo Aggiornamento:** **15 ottobre 2025** (confermato da timestamp firme MD5).

Stato Operativo dell'Interfaccia LAN

Abilitazione e Monitoraggio

Abilitazione e Stato Servizio



Interfaccia: LAN (vtnet1)

- **Stato Servizio:** Attivo (monitoraggio in corso).

Modalità Operativa (IDS Puro)



- **Blocking Mode:** Disabilitata
- **Configurazione:** Solo registrazione, nessun blocco attivo sul flusso di dati.

Analisi dei Log di Allerta Recenti

Overview: 500 Alert Entries dal Log View Suricata

1. Avviso QUIC 2. Failed Decrypt



- **Evento:** Tentativi di decifratura falliti di pacchetti QUIC.
- **Context:** Comune con traffico QUIC crittografato non ispezionabile.
- **Valutazione:** Solitamente **NON è una minaccia diretta**, ma indica una limitazione nell'ispezione profonda.

2. Avviso IPv4 Total Length Error



- **Evento:** Pacchetti IP con dimensione totale inferiore alla dimensione dell'header IPv4.
- **Context:** Classificato come "Decoder Event".
- **Valutazione:** Richiede **ULTERIORI INDAGINI**.
 - Possibili cause: Fuzzing di rete, tentativi di evasione IDS, pacchetti malformati.

Audit di Sicurezza del Web Server DVWA

Analisi tecnica delle vulnerabilità rilevate nella configurazione di sicurezza del Web Server posizionato in DMZ

Metodologia di Testing e Sviluppo di TOOL Custom

Illustrare l'approccio proattivo di VT Firewall S.r.l. nel testing dell'infrastruttura, attraverso una metodologia di verifica mirata e lo sviluppo di strumenti di analisi.

Obiettivi e Contesto del Testing



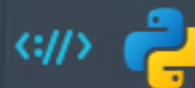
- **Convalida Pre-Produzione:** Testing in ambiente simulato per convalidare le politiche di sicurezza e identificare vulnerabilità.
- **Focus sul Web Server (DVWA):** Priorità al Web Server Metasploitable in DMZ, esposto a rischi esterni.
- **Tool Custom:** Sviluppo di strumenti Python specifici per requisiti di progetto e analisi approfondita.

Scanner Custom per la Scansione delle Porte



- **Funzionalità:** Questo tool, sviluppato in Python, accetta in input un indirizzo IP e un range di porte da scansionare (es. 1-1024), restituendo lo stato di accessibilità di ciascuna porta (Aperta/Chiusa).
- **Obiettivo di Sicurezza:** Permette di verificare se porte di servizio note e potenzialmente insicure siano esposte in modo inopportuno, specialmente sul Web Server Metasploitable.

Analizzatore dei Verbi HTTP



- **Funzionalità:** Progettato per inviare richieste specifiche a un determinato path del WebServer e verificarne le risposte.
- **Obiettivo di Sicurezza:** Questo strumento è fondamentale per individuare l'abilitazione di verbi HTTP potenzialmente pericolosi, la cui presenza non necessaria rappresenta una significativa vulnerabilità di configurazione.



Scansione delle Porte: Metodologia e Risultati

Configurazione del Test

La scansione è stata condotta utilizzando il Port Scanner proprietario di VT Firewall S.r.l., indirizzata all'IP 192.168.50.16 per validare l'efficacia delle regole di filtraggio implementate.

Porte Analizzate

- Servizi standard ad alto rischio (SSH, Telnet)
- Servizi web (HTTP/HTTPS)
- Porta alta casuale (44444)

Esito Positivo

I servizi standard risultano correttamente **non accessibili**, confermando l'efficacia del filtraggio su porte di default.

❑ **Nota:** Il server non espone servizi non necessari su porte a basso numero, indicando una configurazione baseline corretta.

RISCHIO CRITICO: Porta 44444 Aperta

Rilevamento

Porta 44444 risulta **Aperta** con "Accesso consentito" su un servizio sconosciuto

Potenziali Minacce

- **Backdoor:** Accesso remoto non autorizzato
- **Servizio non documentato:** Applicazione di gestione esposta

Azioni Immediate

Blocco immediato della porta 44444 su Firewall e ACL del Router fino a identificazione completa

Raccomandazione Tecnica

È imperativo eseguire un **Service Fingerprinting** approfondito per identificare lo scopo del servizio in ascolto. La presenza di porte alte aperte è un indicatore tipico di compromissione o configurazione errata che richiede bonifica immediata.

RISULTATI SCANSIONE VERBI HTTP

Obiettivo e Metodologia del Test

- **Strumento:** Tool personalizzato in Python.
- **Target:** Web Server DVWA (IP: 192.168.20.10).
- **Scopo:** Identificare l'abilitazione di metodi HTTP potenzialmente pericolosi su quattro percorsi chiave.

Analisi dei Risultati per Path

Path di Root (/)

Risultato: Tutti i metodi, inclusi PUT e DELETE, sono attivi (Stato 200 - OK)

Implicazione: Massima esposizione sulla directory principale.

Pagina di Login (/dvwa/login.php)

Risultato: Il server risponde positivamente a tutti i metodi

Implicazione: I metodi pericolosi sono attivi anche su pagine di autenticazione.

Path Base DVWA (/dvwa/)

Risultato: Reindirizzamento (302 - Found) per tutti i verbi.

Implicazione: Conferma che i metodi sono pienamente abilitati a livello di applicazione

Risorsa Inesistente (/risorsa)

Risultato: Gestione parzialmente corretta (404 per GET/POST, ma 405 per PUT/DELETE).

Implicazione: Sebbene il server limiti i metodi su risorse non esistenti, questo non mitiga il rischio su quelle valide.



RISCHIO CRITICO RILEVATO: Esposizione di Metodi Pericolosi

I test hanno confermato che il Web Server abilita e risponde con successo ai metodi **DELETE** e **PUT** su risorse critiche.

'PUT' Abilitato

- Consente a un attaccante di creare o sovrascrivere file sul server.
- **Vulnerabilità:** Caricamento di codice malevolo (defacement, backdoor).

'DELETE' Abilitato

- Consente l'eliminazione di risorse, un rischio diretto.
- **Vulnerabilità:** Compromissione dell'integrità dei dati e disponibilità del servizio.

La configurazione attuale del Web Server è classificata come ad **ALTO RISCHIO**. La risposta positiva dei metodi PUT e DELETE su percorsi funzionanti rappresenta una minaccia critica che richiede un intervento immediato

Sintesi del Progetto

- ✓ VT Firewall S.r.l. ha completato con successo la fase di progettazione e testing dell'infrastruttura di rete per la Compagnia Theta.
- ✓ Il progetto ha implementato un'architettura "Defense in Depth" su un edificio di sei piani, garantendo che i 120 host e i dispositivi critici (Firewall, NAS, Web Server, 3 IDS/IPS) siano posizionati strategicamente in una topologia logica isolata e sicura.
- ✓ La segmentazione logica (VLAN) sarà applicata prioritariamente ai reparti con la gestione di dati critici: Amministrazione e Finanza, Ricerca e Sviluppo, e Direzione Generale.



Raccomandazioni e strategie Post-Test

Azioni chiave per rafforzare la sicurezza



Hardening del Web Server:

- Disabilitare servizi di rete non essenziali (FTP/21, Telnet/23, SSH/22) esposti in DMZ.
- Obiettivo: Minimizzare la superficie di attacco esposta.



Filtraggio Avanzato Verbi HTTP:

- Configurare il server web/Firewall per consentire solo i verbi GET e POST.
- Bloccare PUT/DELETE su path sensibili (es. phpMyAdmin) per prevenire manipolazioni.



Politiche Firewall "Deny All":

- Applicare il principio del "Deny All" di default.
- Permettere solo traffico strettamente necessario verso la DMZ.
- Bloccare ogni tentativo di accesso o scansione verso la LAN interna.

Prossimi passi

Delinare la roadmap per il mantenimento, l'ottimizzazione continua e l'adeguamento dell'infrastruttura di sicurezza per garantire protezione di lungo termine.



Implementazione Prioritaria e Verifica



- ✓ Applicazione Immediata delle Raccomandazioni date
- ✓ Eseguire Nuovi Cicli di Testing



Monitoraggio Continuo e Gestione Incidenti



- Integrazione SIEM
- Sviluppare e testare un IRP dettagliato per gestire efficacemente eventuali violazioni o attacchi.



Aggiornamento, Formazione e Conformità






- Manutenzione Proattiva
- Formazione del Personale
- Audit e Conformità

Prossimi Passi & Chiamata all'Azione:

"Il nostro team è a vostra completa disposizione per discutere ulteriormente i dettagli della proposta e per aiutarvi a definire i prossimi passi ideali.

Proponiamo di:

- ✓  **Fissare un incontro di follow-up dedicato** entro la prossima settimana per un approfondimento tecnico o per rispondere a eventuali domande specifiche.
- ✓  **Preparare una proposta dettagliata e personalizzata** che includa un cronoprogramma e un preventivo basato sulle vostre esigenze specifiche.
- ✓  **Organizzare una demo tecnica** della soluzione per il vostro team, qualora desideriate vederla in azione con un caso d'uso reale.

Siamo pronti ad avviare la fase di implementazione non appena avremo il vostro prezioso feedback e la vostra approvazione, garantendovi un supporto costante e professionale

