REPORT TECNICO – FUNZIONAMENTO E COSTI DEI SISTEMI DI SICUREZZA IMPLEMENTATI

Cliente: Nencini Sport S.P.A

Data: 10/07/2025

Consulente di Sicurezza Informatica: Andrea Giovannoni

---

1. Obiettivo del documento

Questo report descrive il funzionamento dei principali sistemi di sicurezza informatica implementati nell'infrastruttura e-commerce aziendale, illustrando come ciascun componente contribuisce alla protezione attiva e reattiva dei sistemi. Inoltre, fornisce una stima dei costi annuali orientativi per la loro adozione e gestione.

---

2. Architettura difensiva multilivello (Defence in Depth)

L'infrastruttura di sicurezza si basa su un modello a strati, progettato per garantire la protezione contro una vasta gamma di minacce, dalla superficie esterna (web) fino ai sistemi interni e ai dati sensibili.

Livello	Componente	Funzione primaria
Perimetrale	WAF, Firewall, CDN	Filtraggio e blocco traffico anomalo
Applicativo	CSP, validazione input, WAF	Prevenzione attacchi web (SQLi, XSS, LFI)

Infrastrutturale	Segmentazione, IDS/IPS	Isolamento logico, rilevamento intrusioni
Endpoint	EDR	Monitoraggio comportamentale, contenimento malware
Log & Correlazione	SIEM	Analisi eventi, allarmi, compliance
Automazione	SOAR	Orchestrazione risposte, riduzione MTTR

---

3. Descrizione operativa dei sistemi

3.1 WAF (Web Application Firewall)

- Posizionato tra Internet e la DMZ.
- Analizza il traffico HTTP/S in ingresso.
- Blocca automaticamente SQL Injection, XSS, attacchi LFI/RFI, scansioni automatizzate.
- Regole personalizzabili (firma + comportamento).
- Integra alert nel SIEM e attiva flussi SOAR se necessario.

3.2 Segmentazione di rete e Firewall ACL

- DMZ separata logicamente dalla rete interna.
- ACL configurate per limitare solo i flussi strettamente necessari (es. web → DB).

- Accesso amministrativo consentito esclusivamente tramite Bastion Host con MFA.

3.3 IDS/IPS (Suricata / Snort)

- Inserito tra DMZ e rete interna.
- Analizza il traffico in tempo reale, rileva exploit, scansioni, anomalie.
- In modalità IPS, blocca direttamente le connessioni pericolose.
- Eventi loggati e inviati al SIEM.

3.4 EDR (Endpoint Detection and Response)

- Installato su server critici in DMZ e backend.
- Analisi dei processi in tempo reale.
- Blocca attacchi fileless, ransomware, privilege escalation.
- In caso di compromissione, isola la macchina dalla rete (Network Quarantine) e avvisa il SOC tramite alert SIEM.

3.5 SIEM (Wazuh / ELK Stack)

- Centralizza i log di tutti i componenti (WAF, IDS/IPS, EDR, server, firewall).
- Applica regole di correlazione per identificare pattern di attacco.
- Fornisce dashboard di controllo in tempo reale.
- Automatizza invio alert critici al SOAR.

3.6 SOAR (TheHive + Cortex)

- Orchestratore della risposta automatica agli incidenti.
- Riceve input dal SIEM.
- Attiva playbook: es. isolamento IP, notifica team, disattivazione credenziali, chiusura porte firewall.
- Tiene traccia di ogni azione per fini di audit e post mortem.

---

4. Esempio operativo reale

Scenario: attacco XSS + esfiltrazione dati

1. Il WAF blocca la richiesta XSS → alert al SIEM.
2. L'EDR rileva attività sospette (esecuzione curl) → isola il server.
3. Il SOAR genera un incidente automatico, chiude le comunicazioni DMZ → DB.
4. Il SOC analizza e risolve, con ripristino del sistema da snapshot sicuro.
5. Il SIEM conserva tutti i log per audit e reportistica.

---

5. Benefici operativi

- Protezione proattiva da attacchi web, malware, minacce avanzate.
- Monitoraggio continuo e visibilità centralizzata (SIEM).
- Risposta automatica e riduzione drastica del MTTR.
- Conformità normativa: GDPR, ISO/IEC 27001, NIS2.
- Modularità: ogni componente è scalabile e aggiornabile.

---

6. Stima dei costi annuali orientativi

Componente	Configurazione	Costo stimato annuo
WAF (Cloudflare Business)	Protezione da attacchi web	€ 2.400
EDR (SentinelOne Complete)	15 endpoint	€ 2.400
SIEM (Wazuh con supporto professionale)	Rete media + cloud	€ 16.360
SOAR (TheHive Gold)	Licenza on-prem per 5 utenti	€ 15.400
Totale stimato	—	≈ € 36.560

Queste soluzioni rappresentano un bilanciamento tra sicurezza e avanzata e sostenibilità

Il sistema è pronto per operazioni live, testato, auditabile e allineato agli standard europei in materia di sicurezza.