DOGNET TECHNOLOGIES SRL

Descrizioni Tecnica dei Servizi

Revisione interna — Marzo 2026

ETHICAL HACKING AND LINUX EXTREME

Table of Contents

Vulnerability Assessment & Penetration Test

▸ ETHICAL HACKING

Panoramica del Servizio

Il servizio di Vulnerability Assessment e Penetration Testing (VAPT) di Dognet Technologies è una soluzione integrata e completa per l'identificazione, l'analisi e la mitigazione delle vulnerabilità di sicurezza informatica presenti negli asset tecnologici aziendali. A differenza degli approcci superficiali orientati alla mera conformità formale, il nostro servizio si distingue per la completezza metodologica e l'accuratezza tecnica nell'individuazione delle reali esposizioni al rischio cyber. Non ci limitiamo a generare report standardizzati per soddisfare requisiti normativi pro forma: ci impegniamo a identificare e sfruttare concretamente ogni vulnerabilità presente, simulando attacchi reali condotti da threat actor motivati e competenti.

Metodologie e Framework di Riferimento

Il nostro approccio metodologico si fonda sull'integrazione sinergica di framework riconosciuti a livello internazionale. Adottiamo le linee guida OWASP (Open Web Application Security Project) per la valutazione della sicurezza applicativa, con particolare riferimento all'OWASP Testing Guide, all'OWASP Top 10, all'OWASP Mobile Security Testing Guide (MSTG) e all'OWASP API Security Project. Utilizziamo il framework MITRE ATT&CK per modellare i comportamenti degli attaccanti reali, mappando tattiche, tecniche e procedure (TTP) utilizzate da gruppi APT e threat actor avanzati. Integriamo inoltre la metodologia OSSTMM (Open Source Security Testing Methodology Manual) per un approccio scientifico e ripetibile alla misurazione della sicurezza operativa.

Competenze e Certificazioni del Team

I nostri security specialist possiedono certificazioni professionali di alto livello: CEH (Certified Ethical Hacker), PWASP (Practical Web Application Security and Penetration Testing), CISSP (Certified Information Systems Security Professional) ed eCPPT (eLearnSecurity Certified Professional Penetration Tester). Questa combinazione garantisce visione strategica e architettonica della sicurezza abbinata alle competenze operative necessarie per eseguire penetration test completi su infrastrutture complesse, incluse tecniche di pivoting, post-exploitation e lateral movement.

Ambito di Copertura

Il servizio VAPT copre l'intero spettro degli asset tecnologici aziendali: applicazioni web (OWASP Top 10 e oltre), applicazioni mobile (Android e iOS, secondo OWASP MSTG), infrastrutture di rete (vulnerability scanning, exploitation, privilege escalation, lateral movement), API REST/SOAP/GraphQL e microservizi (OWASP API Top 10), ambienti cloud su AWS, Azure e GCP (IAM misconfiguration, network exposure, privilege escalation), dispositivi IoT e sistemi OT/ICS (SCADA, PLC, protocolli industriali Modbus, DNP3, OPC).

Processo di Esecuzione

Il processo segue fasi strutturate e metodiche: reconnaissance e OSINT per mappare la superficie esposta e identificare asset, dipendenti e tecnologie in uso; vulnerability scanning automatizzato autenticato e non autenticato con strumenti professionali; analisi manuale approfondita per identificare business logic flaw, catene di attacco multi-step e vulnerabilità non rilevabili automaticamente; exploitation controllata con proof-of-concept per ogni vulnerabilità critica che dimostra la sfruttabilità reale; e produzione del report finale.

Deliverable

Report completo con executive summary per il management non tecnico; findings dettagliati con descrizione tecnica, severity CVSS 3.1, prove di sfruttabilità e remediation specifica; matrice di prioritizzazione per la remediation; e retesting gratuito sui finding critici e alti dopo la correzione da parte del team tecnico del cliente.

Tiger Team e BlackOps

▸ ETHICAL HACKING — ALTAMENTE RISERVATO

Panoramica del Servizio

Il servizio Tiger Team rappresenta la forma più avanzata e realistica di security testing, combinando penetration testing cyber con operazioni di physical security testing per simulare attacchi condotti da threat actor sofisticati che non si limitano al perimetro digitale, ma sfruttano ogni vettore disponibile—fisico, umano e tecnologico—per raggiungere i loro obiettivi. A differenza dei tradizionali penetration test limitati al perimetro di rete, questo servizio simula scenari di attacco realistici dove avversari determinati—spie industriali, insider threat, gruppi APT, sabotatori—combinano tattiche convenzionali e non convenzionali per compromettere confidenzialità, integrità e disponibilità di asset critici.

Le operazioni includono intrusione fisica controllata in facility, compromissione di infrastrutture fisiche di sicurezza, social engineering avanzato, utilizzo di tecnologie non convenzionali come droni per ricognizione, e deployment di hardware malevolo direttamente in ambienti protetti come i Centri Elaborazione Dati.

Framework Legale e Vincoli Operativi

Data la natura estremamente sensibile delle attività, operiamo entro un framework legale rigorosissimo. Ogni engagement richiede contratti legali estremamente dettagliati che specificano scope preciso, limitazioni esplicite, finestre temporali, aree geografiche, asset in-scope e out-of-scope, e rules of engagement. I contratti includono clausole di non perseguibilità penale per le azioni autorizzate, confidentiality agreement bilaterali e indemnity clause. Prima dell'inizio delle operazioni, notifichiamo preventivamente le autorità competenti (Forze dell'Ordine, eventualmente intelligence services per facility critiche) per prevenire malintesi e interventi non necessari. Otteniamo autorizzazioni scritte esplicite dai vertici aziendali del cliente (CEO, CISO, Security Director, Legal Counsel) e manteniamo chain of custody rigorosa per tutte le evidenze raccolte.

Obiettivo: Prevenzione, Non Spionaggio

Il servizio Tiger Team è finalizzato esclusivamente alla prevenzione e detection di minacce reali. Simuliamo tecniche utilizzabili da spie industriali o gruppi APT per identificare vulnerabilità fisiche e procedurali, testare l'efficacia dei controlli di sicurezza fisica, l'awareness del personale, le capability di detection e response, e la resilienza complessiva dell'organizzazione contro attacchi sofisticati multi-vector. Non estraiamo proprietà intellettuale, non violiamo vincoli etici e ogni informazione ottenuta durante l'engagement è trattata con massima confidenzialità.

Physical Penetration Testing

Conduciamo operazioni di intrusione fisica controllata per testare controlli di accesso, sorveglianza e procedure di risposta. Le tecniche includono: lock picking e bypass di sistemi di controllo accessi (badge reader, biometria, serrature elettroniche); tailgating e piggybacking per testare l'awareness del personale; badge cloning RFID/NFC; identificazione di blind spot nelle telecamere e vulnerabilità nei sensori di movimento; operazioni notturne per testare i controlli in orari con ridotta presenza di personale; simulazione di delivery personnel (corrieri, tecnici manutentori) per testare le procedure di verifica identità dei visitatori.

Compromissione del CED e Hardware Malevolo

Una volta ottenuto accesso fisico ad aree sensibili come il Centro Elaborazione Dati, simuliamo la compromissione diretta dell'infrastruttura IT critica: installazione di Bad USB device, Raspberry Pi configurati come implant persistenti connessi alla rete interna per command-and-control remoto, hardware keylogger su workstation amministrative, e altri dispositivi che permetterebbero a un attaccante reale di mantenere accesso permanente anche dopo la discovery del vettore di intrusione iniziale.

Deliverable

Report operativo completo con timeline dell'operazione, tecniche fisiche e cyber utilizzate, analisi dei gap di detection e risposta, valutazione dell'awareness del personale, e roadmap di remediation che copre controlli di sicurezza fisica, procedure operative e investimenti in tecnologie di detection. Include raccomandazioni specifiche per security policy, formazione del personale e miglioramento dei sistemi di sorveglianza.

Hardening dei Sistemi

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio di System Hardening di Dognet Technologies è un intervento tecnico specializzato finalizzato alla riduzione sistematica della superficie d'attacco dei sistemi Linux attraverso l'applicazione rigorosa di best practice di sicurezza, configurazioni ottimizzate e implementazione di controlli difensivi stratificati. Operiamo principalmente su distribuzioni Debian, Ubuntu e Oracle Linux, applicando metodologie consolidate che trasformano installazioni standard vulnerabili in sistemi fortificati resistenti agli attacchi più sofisticati. Il nostro approccio non si limita a modifiche superficiali o checklist generiche: interviene profondamente su ogni layer del sistema operativo, dal kernel ai servizi applicativi, garantendo una postura di sicurezza robusta, misurabile e auditabile.

Framework e Standard di Riferimento

Il processo si fonda sui CIS Benchmarks (Center for Internet Security), standard globalmente riconosciuti e validati dalla community internazionale di security professional. Implementiamo i controlli CIS di Livello 1 (baseline security essenziale senza impatti operativi significativi) e Livello 2 (sicurezza avanzata per ambienti ad alto rischio), personalizzando l'applicazione in base al profilo di rischio specifico e ai requisiti operativi del cliente. Integriamo inoltre i requisiti PCI-DSS per ambienti che gestiscono dati di carte di pagamento, garantendo conformità ai requisiti 2.2 (configurazioni sicure), 2.3 (cifratura del traffico amministrativo) e agli altri controlli correlati.

Hardening del Kernel Linux

Interveniamo direttamente sui parametri del kernel attraverso sysctl, configurando protezioni avanzate contro attacchi di rete, memory corruption e privilege escalation: kernel.dmesg_restrict e kernel.kptr_restrict per prevenire information disclosure, kernel.yama.ptrace_scope per limitare il debugging non autorizzato, kernel.unprivileged_bpf_disabled per ridurre la superficie eBPF. Configuriamo protezioni contro SYN flood, ICMP redirect, IP forwarding non necessario e source routing. Implementiamo ASLR completo, protezioni contro buffer overflow e disabilitiamo i moduli kernel non necessari con blacklist e firma dei moduli dove applicabile.

Filesystem, Account e Autenticazione

Il filesystem viene protetto con partitioning sicuro (separazione di /tmp, /var, /home su partizioni dedicate con mount option noexec, nosuid, nodev), file integrity monitoring con AIDE o Tripwire, e mandatory access control con AppArmor (Debian/Ubuntu) o SELinux (Oracle Linux) in modalità enforcing. L'autenticazione è rafforzata con PAM configurato per complessità delle password, history, aging e account lockout; sudo con least privilege e logging completo; SSH hardening con chiavi pubbliche, disabilitazione root login e cipher aggiornati; e 2FA dove richiesto dal profilo di rischio.

Servizi, Network, Container e Deliverable

I servizi critici (SSH, Apache/Nginx, MySQL/PostgreSQL, BIND) ricevono hardening specifico per disabilitare version disclosure, rimuovere funzionalità non necessarie e configurare TLS ottimale. Il network è protetto con iptables/nftables a default-deny policy, rate limiting anti-DoS e logging del traffico sospetto. Per ambienti container (Docker/Kubernetes) implementiamo

user namespace, seccomp profile, capability dropping e pod security standard. I deliverable includono baseline configuration documentation completa, automation script Ansible/Bash per deployment ripetibile, compliance mapping verso CIS e PCI-DSS, e runbook operativi per la maintenance continuativa.

Architettura e Progettazione

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio di Architettura e Progettazione di Dognet Technologies offre a PMI e startup una soluzione enterprise-grade, performante, sicura ed economicamente sostenibile per la realizzazione di ambienti IT moderni basati su virtualizzazione open source. Progettiamo infrastrutture complete che combinano virtualizzazione (VM KVM e container LXC), storage distribuito ad alte prestazioni, networking software-defined, backup automatizzato e monitoring proattivo—eliminando la dipendenza da soluzioni proprietarie costose come VMware e offrendo flessibilità, scalabilità e TCO drasticamente inferiore. Ogni architettura è progettata con approccio security-by-design: hardening completo dello stack, encryption at rest e in transit, separazione dei piani di rete e accesso amministrativo con 2FA.

Scenari Architetturali Supportati

Progettiamo architetture per molteplici scenari: infrastrutture hybrid cloud che integrano cluster Proxmox on-premise con cloud pubblici (AWS, Azure, GCP) per workload bursting, backup off-site e disaster recovery geograficamente distribuito; architetture edge computing distribuite con nodi Proxmox in location remote (filiali, siti industriali) gestiti centralmente con capacità di operare autonomamente in caso di disconnessione; siti di disaster recovery con cluster secondari, replicazione automatizzata e RTO/RPO conformi ai requisiti di business continuity; e architetture modulari per PMI in crescita, progettate per espansione incrementale di compute, storage e networking senza disruption operativa.

Cluster Proxmox High-Availability e Storage Ceph

Progettiamo cluster Proxmox VE ottimizzati per alta disponibilità: dimensionamento su workload specifici, quorum distribuito con QDevice per prevenire split-brain, live migration senza downtime, fencing mechanisms (IPMI, PDU smart, watchdog) per isolamento di nodi failed, e resource scheduling con affinity/anti-affinity rules. Integriamo Ceph come storage backend distribuito con block storage RBD, object storage RADOS Gateway e CephFS: topology ottimale con separazione SSD/SATA/NVMe per differenti workload, policy di replica 3x con failure domain a livello host o rack, pool con erasure coding per dati cold, e performance tuning con PG autoscaling e scrubbing schedulato.

Software-Defined Networking e Deliverable

Il networking è basato su Open vSwitch con VLAN segmentation per separazione di management, VM, storage e backup; bonding LACP per fault tolerance e aggregazione di bandwidth; firewall distribuito per micro-segmentation e enforcement di least-privilege network policy; e VXLAN per multi-site connectivity e hybrid cloud. I deliverable includono documentazione architetturale completa (network diagram, storage topology, security architecture), specifiche tecniche per l'approvvigionamento hardware, runbook operativo, piano di disaster recovery con procedure testate, e contratto di supporto continuativo.

Baseline e Deployment

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio di Baseline e Deployment fornisce virtual machine e container Linux pre-configurati, hardened e compliance-ready che eliminano la necessità di partire da distribuzioni vanilla insicure richiedendo settimane di hardening manuale. Creiamo golden image e template ottimizzati per sicurezza, performance e conformità normativa, pronti per deployment immediato in qualsiasi ambiente virtualizzato. Ogni baseline è meticolosamente configurata secondo gli standard richiesti dal cliente—NIS2, PCI-DSS, CIS Benchmarks, ISO 27001, NIST—garantendo che ogni istanza deployata parta da una postura di sicurezza robusta e auditabile. I deliverable sono forniti in formati universalmente compatibili con tutti i principali hypervisor, accompagnati da automation script per provisioning scalabile.

Distribuzioni Linux Supportate

Creiamo baseline hardened per le principali distribuzioni Linux enterprise: Debian e Ubuntu LTS per workload production critici che richiedono stabilità e supporto esteso; Oracle Linux per ambienti enterprise con Oracle Database (compatibilità RHEL binaria e Unbreakable Enterprise Kernel); Red Hat Enterprise Linux, Rocky Linux, AlmaLinux, CentOS Stream; SUSE Linux Enterprise Server; e qualsiasi distribuzione specifica richiesta dal cliente. Ogni distribuzione viene configurata da installazioni minimal per ridurre al massimo la attack surface.

Framework di Compliance e Profili Specializzati

Progettiamo baseline allineate ai principali framework: NIS2, PCI-DSS (Requisiti 2, 8, 10), CIS Benchmarks Livello 1 e 2, ISO 27001 Annex A, NIST SP 800-53, GDPR technical requirements, HIPAA Security Rule e SOC 2 Type II. I profili specializzati disponibili includono: OS minimal (foundation per installazioni custom), web server (Apache/Nginx con ModSecurity WAF), database server (MySQL/PostgreSQL/Oracle con audit logging e encryption at rest), application server (Java/Tomcat, Python, Node.js, PHP-FPM), container-specific (Docker/LXC con attack surface minimale), bastion/jump host (2FA, session recording, command restriction), e baseline completamente custom con stack applicativi pre-installati e pre-configurati.

Deliverable

Template VM/container nei formati richiesti (OVF, QCOW2, Docker image, LXC template); automation script per provisioning scalabile; documentazione completa del hardening implementato con compliance mapping verso i framework applicabili; script di validation per continuous compliance checking; e procedure di aggiornamento per il mantenimento della postura di sicurezza nel tempo.

CTI — Cyber Threat Intelligence

▸ **INTELLIGENCE**

Panoramica del Servizio

Il servizio di Cyber Threat Intelligence (CTI) di Dognet Technologies fornisce intelligence azionabile, tempestiva e contestualizzata sulle minacce cyber che possono impattare la sicurezza e la continuità operativa delle organizzazioni clienti. A differenza di semplici feed di Indicator of Compromise (IoC) generici, il nostro approccio integra quattro tipologie di intelligence—strategica, tattica, operazionale e tecnica—per fornire una comprensione olistica del threat landscape, degli attori malevoli, delle loro motivazioni, capacità e tecniche. Trasformiamo dati grezzi provenienti da molteplici fonti in intelligence processata, validata, arricchita e immediatamente utilizzabile per decisioni strategiche, ottimizzazione delle difese, threat hunting proattivo e risposta rapida agli incidenti.

Approccio Multi-Layer alla Threat Intelligence

Il servizio articola la CTI su quattro livelli complementari che rispondono alle esigenze di stakeholder differenti. La Strategic Intelligence fornisce al C-level e al risk management una visione ad alto livello delle tendenze delle minacce, dell'evoluzione del panorama globale e settoriale e delle implicazioni geopolitiche che influenzano il rischio cyber. La Tactical Intelligence supporta CISO e security architect nella comprensione delle TTP degli attaccanti mappate su MITRE ATT&CK, per ottimizzare architetture difensive e capability di detection. La Operational Intelligence alimenta i SOC e i team di incident response con informazioni su campagne attive, operazioni ransomware e phishing campaign targeting il settore del cliente. La Technical Intelligence fornisce IoC concreti—IP malevoli, domini C2, hash malware, URL di phishing—direttamente integrabili in SIEM, firewall, IDS/IPS ed EDR per detection e blocking automatizzati.

Fonti, Processing e Integrazione

La qualità della threat intelligence dipende dalla diversificazione delle fonti. Utilizziamo OSINT sistematico (security blog, advisory vendor, CVE database, exploit database, social media), commercial threat intelligence feed con IoC curati e threat actor profiling, dark web monitoring sistematico su forum underground e marketplace criminali, e infrastrutture proprietarie di honeypot e honeynet per catturare attacchi in-the-wild. Il processo di processing normalizza, arricchisce e correla i dati grezzi; l'analisi esperta elimina i falsi positivi e contestualizza le minacce rispetto al profilo del cliente; la dissemination distribuisce intelligence nei formati appropriati per ciascun stakeholder—executive summary, technical bulletin e feed machine-readable STIX/TAXII.

Deliverable

Feed IoC aggiornati e integrabili nelle tecnologie di sicurezza esistenti; threat actor profile per gli attori rilevanti per il settore del cliente; report periodici di threat landscape; alerting immediato su campagne attive che impattano il settore; e sessioni di threat briefing per management e team di sicurezza.

Valutazione del Rischio

▸ **INTELLIGENCE**

Panoramica del Servizio

La Valutazione del Rischio è un servizio strategico che consente alle organizzazioni di comprendere in modo chiaro, misurabile e oggettivo il proprio livello di esposizione alle minacce cyber. Dognet Technologies supporta le aziende nell'identificazione, analisi e prioritizzazione dei rischi informatici che impattano su infrastrutture, applicazioni, processi e persone. Attraverso un approccio metodologico strutturato, analizziamo gli asset critici, le vulnerabilità presenti, le minacce realistiche e le potenziali conseguenze operative, economiche e reputazionali di un incidente di sicurezza. La valutazione non si limita all'aspetto tecnico: integra anche fattori organizzativi, procedurali e umani, fornendo una visione completa del rischio reale.

Il servizio è basato su standard riconosciuti a livello internazionale: ISO/IEC 27001, ISO 27005, NIST Risk Management Framework e principi DevSecOps. Ogni rischio viene classificato in base a probabilità, impatto e livello di esposizione, consentendo una gestione consapevole e prioritaria delle attività di mitigazione.

Metodologia e Processo

Il processo segue le fasi previste dalla ISO 27005 e dal NIST RMF: identificazione e classificazione degli asset in base alla criticità per il business; analisi delle minacce realistiche per il settore e il profilo dell'organizzazione; identificazione delle vulnerabilità tecniche, organizzative e procedurali; valutazione della likelihood di ogni scenario di rischio; calcolo dell'impatto su confidenzialità, integrità, disponibilità e continuità operativa; e definizione del risk rating combinato. Il risultato è una mappa del rischio comprensibile sia per il management che per i team tecnici e di governance.

Applicazioni e Deliverable

La Valutazione del Rischio è un elemento chiave per: definire una strategia di cybersecurity basata sul rischio reale; supportare processi di compliance e audit (NIS2, ISO 27001 e PCI-DSS richiedono tutti una valutazione formale del rischio); ridurre l'impatto di incidenti concentrando gli investimenti sulle aree di maggior esposizione; e migliorare la resilienza operativa con un piano di trattamento strutturato e prioritizzato. I deliverable includono mappa del rischio completa, report esecutivo per il management, report tecnico dettagliato per i team IT, piano di trattamento con azioni di remediation e timeline, e documentazione del rischio residuo accettabile come evidenza per audit e certificazioni.

Valutazione GDPR

▸ GOVERNANCE E COMPLIANCE

Panoramica del Servizio

Il servizio di Valutazione GDPR di Dognet Technologies è dedicato all'analisi del livello di conformità al Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali. Supportiamo aziende e professionisti nell'identificazione dei gap normativi, tecnici e organizzativi che possono esporre l'organizzazione a sanzioni—fino al 4% del fatturato globale annuo—rischi legali e danni reputazionali. Il nostro approccio integra la prospettiva giuridica con quella tecnica di cybersecurity, perché la protezione dei dati personali non è solo una questione di documentazione: richiede misure di sicurezza informatica concrete e verificabili.

Aree di Analisi

Il servizio copre: analisi dei trattamenti di dati personali e dei flussi informativi; verifica delle basi giuridiche e della correttezza dei consensi raccolti; ruoli e responsabilità interne (Titolare, Responsabili, Autorizzati, DPO); adeguatezza delle misure di sicurezza tecniche e organizzative per garantire riservatezza, integrità, disponibilità e resilienza dei dati; documentazione obbligatoria (Registro dei Trattamenti, Informative privacy, Procedure di data breach, DPA con fornitori cloud e SaaS); processi di gestione dei diritti degli interessati (accesso, rettifica, cancellazione, portabilità); e modalità di conservazione, cancellazione e minimizzazione.

Integrazione GDPR e Cybersecurity

Particolare attenzione viene dedicata all'integrazione tra GDPR e sicurezza informatica: valutiamo l'allineamento tra le misure di protezione dei dati richieste dall'art. 32 del Regolamento e i controlli tecnici effettivamente implementati nell'infrastruttura IT—cifratura at rest e in transit, controllo degli accessi, logging e monitoring, gestione delle vulnerabilità, incident response e business continuity. Quando necessario, supportiamo la valutazione di impatto sulla protezione dei dati (DPIA) per i trattamenti ad alto rischio.

Deliverable

Report strutturato con livello di conformità attuale, non conformità e rischi associati con severity e probabilità di contestazione da parte del Garante, e azioni correttive prioritarie con stima dell'effort. Il report costituisce una base solida per audit, ispezioni del Garante e percorsi di adeguamento normativo. Il servizio è personalizzato in base alla dimensione dell'azienda, al settore e alla complessità dei trattamenti.

Revisione del Codice

▸ ETHICAL HACKING

Panoramica del Servizio

Il servizio di Code Review di Dognet Technologies è un'analisi tecnica approfondita del codice sorgente applicativo finalizzata all'identificazione sistematica di vulnerabilità di sicurezza, difetti architetturali e pratiche di sviluppo insicure prima che le applicazioni vengano rilasciate in produzione o esposte a utenti reali. A differenza dei controlli automatizzati—indispensabili ma strutturalmente limitati—la nostra revisione combina strumenti statici e dinamici con l'analisi critica condotta da specialisti certificati, capaci di comprendere il contesto applicativo, le logiche di business e i flussi di dati che determinano il rischio reale di ogni vulnerabilità identificata.

L'obiettivo non è produrre una lista di warning da linter, ma restituire al team di sviluppo una mappa precisa delle esposizioni al rischio, con severity reale, proof-of-concept dove applicabile e remediation guidance concreta che non si limiti al "usa una libreria aggiornata" ma indichi come e perché effettuare ogni correzione nel contesto specifico del codebase analizzato.

Framework e Standard di Riferimento

Il processo di revisione adotta come riferimento primario l'OWASP Code Review Guide, integrando le classificazioni OWASP Top 10 e OWASP Top 10 Proactive Controls per garantire che ogni categoria di vulnerabilità rilevante venga sistematicamente verificata. Utilizziamo il Common Weakness Enumeration (CWE) per la classificazione standardizzata delle debolezze identificate, facilitando la comunicazione con team di sviluppo e stakeholder tecnici. Per applicazioni che gestiscono dati sensibili o operano in contesti regolamentati, mappiamo i findings verso i requisiti di sicurezza NIST SP 800-53 e, dove applicabile, PCI-DSS, NIS2 e GDPR.

Copertura e Tipologie di Vulnerabilità

La revisione copre l'intero spettro delle vulnerabilità di sicurezza applicativa rilevabili a livello di codice sorgente:

- Injection flaws: SQL Injection, Command Injection, LDAP Injection, XPath Injection, template injection lato server—con analisi dei flussi di input dall'entry point fino alle query o ai comandi eseguiti, identificando ogni punto in cui la sanitizzazione è assente, insufficiente o bypassabile.
- Authentication e Session Management: implementazioni di autenticazione con debolezze crittografiche, gestione errata di token, session fixation, insufficient session expiry, password storage con algoritmi inadeguati (MD5, SHA1 non salted, bcrypt con cost factor insufficiente).
- Autorizzazione e Access Control: IDOR (Insecure Direct Object Reference), privilege escalation per logiche di autorizzazione errate, mancanza di controlli lato server su operazioni privilegiate, mass assignment nelle API REST.
- Cryptographic Failures: utilizzo di algoritmi deprecati (DES, 3DES, RC4, MD5 per integrità), lunghezze di chiave insufficienti, IV statici o prevedibili, padding oracle vulnerabilities, gestione non sicura di materiale crittografico.

- Sensitive Data Exposure: logging di dati sensibili (password, PAN, token), hard-coded credentials, API key e segreti committati nel codice, trasmissione di dati sensibili senza cifratura.
- Security Misconfigurations: dipendenze con CVE note, configurazioni di framework non sicure per default, CORS misconfiguration, header di sicurezza assenti o errati, error handling verboso che espone stack trace e informazioni architetturali.
- Business Logic Flaws: vulnerabilità specifiche della logica applicativa che gli scanner automatici non possono identificare—race conditions, bypass di workflow, manipolazione di prezzi e quantità, elusione di controlli antifrode.

Linguaggi e Stack Supportati

Il nostro team copre un ampio spettro di tecnologie: Java (Spring Boot, Jakarta EE), Python (Django, Flask, FastAPI), PHP (Laravel, Symfony, WordPress custom), JavaScript/TypeScript (Node.js, Express, NestJS, React, Angular), Go, C/C++ per componenti embedded e applicazioni ad alte prestazioni, C# (.NET Core, ASP.NET), Ruby on Rails. Per applicazioni mobile, analizziamo codice Swift, Kotlin e Java per iOS e Android, includendo la sicurezza delle comunicazioni verso backend API.

Processo di Esecuzione

La revisione si articola in fasi sequenziali e parallele ottimizzate per massimizzare la profondità dell'analisi in tempi contenuti. La fase di setup prevede l'acquisizione sicura del codebase (repository Git, accesso read-only, file system isolato), la mappatura dell'architettura applicativa, l'identificazione dei trust boundary e dei flussi di dati sensibili, e la configurazione degli strumenti di analisi statica (SAST) calibrati sul framework specifico.

L'analisi automatizzata con strumenti SAST (SonarQube, Semgrep con ruleset custom, Bandit per Python, SpotBugs per Java, ESLint security plugin, phpcs-security-audit) produce un primo inventory di finding grezzi che vengono poi sottoposti a triage manuale per eliminare i falsi positivi—che negli strumenti SAST possono raggiungere il 60-80%—e per assegnare severity reale basata sul contesto applicativo.

La revisione manuale si concentra su aree ad alto rischio identificate durante il triage: flussi di autenticazione, logiche di autorizzazione, gestione delle sessioni, operazioni crittografiche, interazioni con database e sistemi esterni, e componenti che gestiscono input untrusted. Ogni finding critico viene corredato da un proof-of-concept che dimostra la sfruttabilità reale.

Deliverable

Il report finale include: executive summary con risk rating complessivo e top findings per il management non tecnico; findings detail con descrizione tecnica, CWE reference, severity CVSS 3.1, prove di sfruttabilità e remediation specifica con esempi di codice corretto; heatmap del codebase che evidenzia le aree a maggior concentrazione di rischio; e piano di remediation prioritizzato con stima dell'effort di correzione. Su richiesta, offriamo sessioni di walkthrough tecnico con il team di sviluppo per trasferire le competenze necessarie a prevenire le stesse categorie di vulnerabilità nei rilasci futuri.

Perché è Importante

Il 70% delle violazioni di dati origina da vulnerabilità applicative. Identificare e correggere queste debolezze in fase di sviluppo costa in media 6 volte meno rispetto alla correzione post-produzione e centinaia di volte meno rispetto alla gestione di un breach. La Code Review non è un controllo formale: è l'ultima linea di difesa prima che il codice diventi superficie d'attacco reale.

Web Assessment

▸ ETHICAL HACKING

Panoramica del Servizio

Il Web Assessment di Dognet Technologies è un'attività di security testing specializzata sulle applicazioni web—portali aziendali, piattaforme e-commerce, applicazioni SaaS, sistemi gestionali web-based, API REST e GraphQL—condotta da specialisti certificati con un approccio che replica fedelmente le tecniche utilizzate dagli attaccanti reali. Non si tratta di un semplice vulnerability scan automatizzato: è un'analisi manuale approfondita che identifica vulnerabilità di business logic, catene di attacco multi-step e debolezze architetturali invisibili agli scanner.

L'applicazione web è oggi la superficie d'attacco principale per la stragrande maggioranza delle organizzazioni. Secondo il Verizon Data Breach Investigations Report, le applicazioni web sono il vettore d'attacco primario nel 43% delle violazioni. Un Web Assessment sistematico permette di identificare e correggere queste esposizioni prima che vengano sfruttate da attori malevoli.

Metodologia e Framework

Il testing segue la OWASP Testing Guide (OTG) nella sua versione più aggiornata, coprendo sistematicamente tutte le categorie di vulnerabilità definite dall'OWASP Top 10 e dai controlli dell'OWASP Application Security Verification Standard (ASVS). Integriamo tecniche dal PTES (Penetration Testing Execution Standard) e mappiamo i finding verso il framework MITRE ATT&CK for Enterprise per contestualizzare ogni vulnerabilità nelle TTP di threat actor reali.

Aree di Testing

Il testing copre l'intera superficie applicativa attraverso le seguenti aree:

- Autenticazione e autorizzazione: bypass di meccanismi di login, brute force protection, account enumeration, reset password insicuro, autorizzazione verticale e orizzontale, IDOR, JWT manipulation, OAuth misconfiguration.
- Injection: SQL Injection (error-based, blind, time-based, out-of-band), NoSQL Injection, LDAP Injection, XML Injection, template injection (SSTI), OS Command Injection, HTTP Header Injection.
- Cross-Site Scripting (XSS): reflected, stored e DOM-based XSS, bypass di filtri e WAF, escalation verso account takeover e session hijacking.
- Cross-Site Request Forgery (CSRF) e Clickjacking: verifica della protezione CSRF su operazioni state-changing, analisi dei Content Security Policy e X-Frame-Options header.
- Insecure Direct Object Reference (IDOR) e Mass Assignment: accesso non autorizzato a risorse di altri utenti, manipolazione di parametri, mass assignment nelle API REST.
- Security Misconfiguration: header di sicurezza HTTP assenti o errati, CORS misconfiguration, directory listing, backup files esposti, error handling verboso, componenti obsoleti e vulnerabili.
- Business Logic Flaws: manipolazione di prezzi e quantità, bypass di step obbligatori nei workflow, race conditions, elusione di controlli antifrode, abuso di coupon e promozioni.

- API Security: OWASP API Top 10—Broken Object Level Authorization, Broken Authentication, Excessive Data Exposure, Lack of Resources Limiting, Function Level Authorization, Mass Assignment, Security Misconfiguration.
- Gestione delle sessioni: session fixation, session prediction, insufficient session expiry, secure e httponly cookie flags, token entropy analysis.

Modalità di Testing

Offriamo tre modalità operative adattabili alle esigenze del cliente: Black Box (nessuna informazione preliminare, simula un attaccante esterno), Grey Box (accesso con credenziali utente standard, simula un attaccante con accesso limitato o un insider non privilegiato), White Box (accesso completo a documentazione, codice sorgente e credenziali amministrative, massimizza la copertura e la profondità dell'analisi). Per la maggior parte delle applicazioni business-critical raccomandiamo l'approccio Grey Box o White Box, che garantisce una copertura superiore nella stessa finestra temporale.

Deliverable

Il report include executive summary con risk rating complessivo; findings dettagliati con descrizione tecnica, severity CVSS 3.1, prove di sfruttabilità (screenshot, payload, request/response HTTP) e remediation specifica; matrice di prioritizzazione per la remediation; e retesting gratuito sui finding critici e alti dopo la correzione da parte del team di sviluppo.

Compromissione Hardware e IoT

▸ ETHICAL HACKING

Panoramica del Servizio

Il servizio di Hardware e IoT Security Assessment analizza la sicurezza di dispositivi fisici connessi—sensori industriali, telecamere IP, router, PLC, dispositivi medicali, sistemi embedded—identificando vulnerabilità nel firmware, nelle interfacce fisiche, nei protocolli di comunicazione e nelle API di gestione. Con miliardi di dispositivi IoT connessi e una media di 5,2 vulnerabilità per dispositivo rilevata dai principali vendor di sicurezza, l'IoT rappresenta uno dei vettori di compromissione più sottovalutati dalle organizzazioni.

Aree di Assessment

L'analisi copre quattro livelli distinti. A livello firmware: estrazione, decompilazione e analisi statica del firmware per identificare credenziali hard-coded, chiavi crittografiche embedded, backdoor, servizi non documentati e debolezze nel processo di aggiornamento (OTA security). A livello interfacce fisiche: analisi delle interfacce UART, JTAG, SPI, I2C per accesso non autorizzato, debug port aperte, possibilità di dump della memoria e modifica del boot process. A livello comunicazioni: analisi del traffico di rete (Zigbee, Z-Wave, BLE, WiFi, LoRaWAN, MQTT, CoAP), verifica della cifratura end-to-end, autenticazione dei messaggi e resistenza ad attacchi man-in-the-middle e replay. A livello applicativo: sicurezza delle API di gestione e delle interfacce web embedded, autenticazione, autorizzazione e aggiornamento sicuro del firmware.

Deliverable

Report tecnico con finding per ciascun livello di analisi, severity CVSS, dimostrazione pratica delle vulnerabilità sfruttabili e remediation roadmap strutturata per priorità. Il servizio è particolarmente critico per organizzazioni in settori manifatturiero, healthcare, energy e smart building, dove la compromissione di un dispositivo IoT può impattare sia la sicurezza informatica che la safety fisica.

Sessioni di RedTeam (Purple)

▸ ETHICAL HACKING

Panoramica del Servizio

Le sessioni di Red Team e Purple Team di Dognet Technologies simulano attacchi reali condotti da threat actor avanzati contro l'organizzazione nel suo complesso—non solo la tecnologia, ma anche le persone e i processi. A differenza di un penetration test che valuta la presenza di vulnerabilità tecniche specifiche, un'operazione Red Team valuta la capacità difensiva complessiva dell'organizzazione: quanto tempo impiega il team di sicurezza (Blue Team) a rilevare l'intrusione, a contenere il movimento laterale, a rispondere e a eradicare la presenza dell'attaccante.

Il modello Purple Team integra Red Team (attaccanti) e Blue Team (difensori) in un framework collaborativo: ogni tecnica offensiva viene eseguita in coordinamento con i difensori, che osservano in tempo reale come i loro strumenti di detection rispondono, identificando gap di visibilità e opportunità di miglioramento dei controlli di sicurezza. Questo approccio massimizza il trasferimento di conoscenza e accelera il miglioramento della postura difensiva.

Framework di Riferimento

Le operazioni sono strutturate seguendo il framework MITRE ATT&CK, che classifica oltre 400 tecniche e sotto-tecniche utilizzate da gruppi APT reali, organizzate nelle 14 tattiche della kill chain: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact. Ogni tecnica eseguita viene documentata con il codice ATT&CK corrispondente, permettendo al Blue Team di verificare la copertura dei propri controlli di detection contro tecniche specifiche.

Fasi dell'Operazione Red Team

La fase di Scoping e Threat Modeling definisce, in accordo con il cliente, gli obiettivi dell'operazione (flag), i vincoli operativi (regole di ingaggio), i threat actor da simulare (e.g., ransomware group, APT nation-state, insider malintenzionato) e il perimetro autorizzato. Questa fase è critica: operazioni mal definite producono risultati non actionable.

La Reconnaissance raccoglie informazioni sull'organizzazione attraverso tecniche OSINT—dipendenti su LinkedIn, tecnologie esposte, indirizzi IP, domini, certificati SSL, dati di breach precedenti—costruendo un profilo dell'organizzazione equivalente a quello che preparerebbe un attaccante motivato nelle settimane precedenti un attacco.

L'Initial Access replica i vettori di compromissione iniziale più utilizzati dagli attaccanti reali: phishing targeted (spear phishing con pretesti convincenti costruiti sui dati OSINT), exploitation di servizi esposti (VPN, RDP, applicazioni web), attacchi alla supply chain, e compromissione di credenziali ottenute da breach pubblici.

Una volta ottenuto il primo accesso, il Lateral Movement simula la progressione dell'attaccante all'interno della rete: privilege escalation, credential dumping, movimento laterale verso sistemi di interesse (domain controller, file server, database, backup), mantenendo persistenza attraverso tecniche di evasione degli antivirus e dei sistemi EDR.

L'Objective Achievement verifica il raggiungimento degli obiettivi definiti in scoping: accesso a dati sensibili, possibilità di deploy di ransomware, compromissione di sistemi critici, exfiltration di dati.

Sessioni Purple Team

Le sessioni Purple Team si affiancano all'operazione Red Team con workshop strutturati in cui il Red Team esegue una tecnica ATT&CK specifica mentre il Blue Team verifica se i propri strumenti (SIEM, EDR, NDR) l'hanno rilevata. Nei casi di mancata detection, le sessioni identificano le modifiche necessarie alle regole di detection, agli alert threshold e ai playbook di risposta. Ogni sessione si chiude con action items concreti per il team di sicurezza.

Deliverable

Report operativo completo con timeline dell'operazione, ogni tecnica ATT&CK utilizzata e il relativo esito (rilevata/non rilevata), analisi dei gap di detection e visibilità, valutazione del tempo medio di rilevamento e risposta (MTTD/MTTR), e roadmap di miglioramento dei controlli difensivi. Include raccomandazioni tecniche specifiche per SIEM rules, EDR policies e network segmentation.

Active Directory Assessment

▸ ETHICAL HACKING

Panoramica del Servizio

L'Active Directory Assessment di Dognet Technologies è un'analisi tecnica approfondita dell'infrastruttura identitaria Microsoft—Active Directory, Azure AD (Entra ID) e ambienti ibridi—che costituisce il cuore dell'autenticazione e dell'autorizzazione nella quasi totalità delle organizzazioni che utilizzano tecnologie Microsoft. Il 90% degli attacchi ransomware culmina con la compromissione del domain controller AD, perché chiunque controlli Active Directory controlla l'intera organizzazione.

Il nostro assessment valuta sistematicamente configurazioni, permessi, deleghe, relazioni di trust, account privilegiati e oggetti di Gruppo Policy che, se mal configurati, permettono a un attaccante con accesso iniziale limitato di escalare i privilegi fino al controllo completo del dominio.

Vulnerabilità e Tecniche di Attacco Verificate

Il testing copre le principali catene di attacco documentate contro Active Directory, utilizzando le stesse tecniche adottate dai gruppi ransomware e APT:

- Kerberoasting: identificazione di account di servizio con SPN configurati, verifica della complessità delle password e della forza dei cifrari Kerberos utilizzati, assessment della resistenza agli attacchi offline di cracking degli hash TGS.
- AS-REP Roasting: identificazione di account con pre-autenticazione Kerberos disabilitata, vulnerabili all'estrazione di hash craccabili offline senza necessità di credenziali iniziali.
- Pass-the-Hash / Pass-the-Ticket: verifica delle configurazioni che permettono il riutilizzo di hash NTLM e ticket Kerberos per movimento laterale senza conoscere le password in chiaro.
- DCSync Attack: identificazione di account o gruppi con permessi Replicating Directory Changes che consentono l'estrazione di tutti gli hash del dominio simulando un domain controller.
- Golden Ticket e Silver Ticket: verifica delle condizioni che permettono la creazione di ticket Kerberos falsificati con validità arbitraria per persistenza a lungo termine.
- BloodHound Attack Paths: mappatura completa dei percorsi di privilege escalation attraverso l'analisi delle relazioni ACL, deleghe e appartenenze a gruppi—identificando ogni path che porta da un utente standard al domain admin.
- Misconfigured Delegations: Unconstrained Delegation, Constrained Delegation, Resource-Based Constrained Delegation—analisi delle configurazioni che permettono impersonation non autorizzata.
- AdminSDHolder e ACL Abuse: analisi delle Access Control List su oggetti critici (domain, AdminSDHolder, GPO) per identificare permessi eccessivi che permettono privilege escalation stealth.
- Azure AD / Entra ID: in ambienti ibridi, analisi delle configurazioni Azure AD Connect, Seamless SSO, PTA/PHS, privileged roles, Conditional Access policies e Service Principal permissions.

Strumenti Utilizzati

L'assessment utilizza strumenti professionali consolidati nella community di security: BloodHound/SharpHound per la mappatura delle relazioni AD e l'identificazione di attack path; Impacket suite per l'exploitation di protocolli Windows; PowerView e ADRecon per l'enumerazione e l'analisi delle configurazioni; PingCastle per la compliance assessment e il risk scoring dell'infrastruttura AD; Rubeus per l'analisi Kerberos; e tool custom sviluppati internamente per scenari specifici.

Deliverable

Report tecnico con: risk score complessivo dell'infrastruttura AD con benchmark rispetto a best practice Microsoft e CIS; attack paths critici visualizzati con grafi BloodHound annotati; finding dettagliati per ogni vulnerabilità con severity, impatto reale e passi di remediation specifici; hardening checklist prioritizzata; e sessione di walkthrough tecnico con il team IT per la pianificazione degli interventi correttivi.

Radio/WiFi Analysis

▸ ETHICAL HACKING

Panoramica del Servizio

Il servizio di Radio e WiFi Security Analysis valuta la sicurezza delle infrastrutture wireless aziendali e dei protocolli radio utilizzati nei contesti operativi—reti WiFi enterprise, reti guest, reti IoT wireless e protocolli radio specifici di settore (Zigbee, Z-Wave, BLE, DECT, LoRaWAN, reti PMR). Le reti wireless rappresentano un perimetro che per natura estende la superficie d'attacco oltre le mura fisiche dell'organizzazione, accessibile da parcheggi, spazi comuni e, in alcuni casi, da centinaia di metri di distanza con hardware specializzato.

Aree di Analisi

Per le reti WiFi, il testing copre: verifica dei protocolli di autenticazione implementati (WPA2/WPA3-Enterprise con 802.1X vs WPA2-Personal), analisi della configurazione RADIUS, test di resistenza ad attacchi di deautenticazione e Evil Twin (rogue access point), verifica della segmentazione tra reti corporate e guest, analisi dei meccanismi PMKID e handshake per valutare la resistenza agli attacchi offline di cracking, e verifica della copertura e dei segnali non autorizzati (rogue AP interni).

Per i protocolli radio specifici, effettuiamo sniffing e analisi del traffico con hardware SDR (Software Defined Radio), verifica della presenza di cifratura e autenticazione dei messaggi, identificazione di replay attack, e analisi della superficie di attacco specifica del protocollo in uso nel contesto operativo del cliente.

Deliverable

Report con mappa della copertura wireless, finding tecnici per ogni vulnerabilità identificata, severity e impatto operativo reale, e remediation con specifiche tecniche di configurazione per le piattaforme enterprise in uso (Cisco, Aruba, Ruckus, Ubiquiti).

Gestione Network Device

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio di Gestione Network Device copre la configurazione, l'hardening, il monitoraggio e la manutenzione continuativa dei dispositivi di rete attivi—router, switch, firewall, access point, load balancer e altri appliance di rete—garantendo che l'infrastruttura di connettività sia sicura, performante e allineata alle policy di sicurezza aziendale. I dispositivi di rete sono spesso il componente meno aggiornato e monitorato dell'infrastruttura IT, nonostante rappresentino il perimetro di controllo primario del traffico aziendale.

Operiamo su apparati dei principali vendor (Cisco, Juniper, Fortinet, Palo Alto, MikroTik, HPE Aruba) e su soluzioni open source (pfSense, OPNsense, VyOS), adattando il servizio alla realtà tecnologica del cliente senza imporre sostituzioni non necessarie.

Attività Incluse

Il servizio comprende: auditing della configurazione attuale con gap analysis rispetto ai CIS Benchmarks per i dispositivi in uso; hardening delle configurazioni (disabilitazione servizi non necessari, protocolli di gestione sicuri, SNMPv3, accesso amministrativo con autenticazione a due fattori, logging centralizzato); gestione del ciclo di vita dei firmware con patching programmato; implementazione e manutenzione di policy di segmentazione e VLAN; configurazione di monitoring continuo con alerting su eventi anomali (link down, tentativi di autenticazione falliti, variazioni di configurazione non autorizzate); e documentazione aggiornata della topologia e delle configurazioni.

Deliverable

Inventory documentato dei dispositivi gestiti, report mensile sullo stato di salute e sicurezza dell'infrastruttura, log di tutte le modifiche effettuate e configurazioni baseline archiviate con versionamento per rollback rapido in caso di malfunzionamenti.

LOG Storage & Analysis

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio di Log Storage & Analysis progetta, implementa e gestisce l'infrastruttura di raccolta, archiviazione, correlazione e analisi dei log generati da tutti i componenti dell'infrastruttura IT—sistemi operativi, applicazioni, dispositivi di rete, firewall, endpoint, ambienti cloud. I log sono la memoria dell'infrastruttura: senza una strategia strutturata di log management, qualsiasi evento di sicurezza—intrusione, data breach, malfunzionamento critico—diventa impossibile da investigare, rilevare tempestivamente o dimostrare a un auditor.

In un contesto normativo che richiede retention di log per periodi definiti (GDPR, NIS2, PCI-DSS richiedono tipicamente 12-24 mesi con accesso rapido agli ultimi 90 giorni), la gestione strutturata dei log è sia un requisito di compliance che uno strumento operativo di sicurezza.

Architettura e Implementazione

Progettiamo stack di log management scalabili e adatti alla dimensione del cliente: da soluzioni self-hosted basate su stack Elastic (Elasticsearch, Logstash, Kibana) o Graylog, fino a configurazioni ibride con storage su object storage cloud-compatible (S3-compatible, Backblaze B2) per la retention a lungo termine a costo contenuto. Integriamo con il modulo MicroSIEM di SentinelCore per le PMI che adottano la nostra piattaforma, o con SIEM enterprise esistenti (Splunk, IBM QRadar, Microsoft Sentinel) per organizzazioni con infrastrutture più complesse.

Il servizio include: definizione della strategia di log collection (quali sorgenti, quale formato, quale retention per categoria); deployment e configurazione degli agent di raccolta; normalizzazione e parsing dei log in formato strutturato; implementazione di regole di correlazione per detection automatica di pattern anomali; e dashboard operative per il monitoring quotidiano da parte del team IT.

Deliverable

Architettura documentata della pipeline di log, playbook di analisi per i pattern di sicurezza più comuni, report mensile degli eventi significativi rilevati e dashboard configurate per il monitoring autonomo da parte del team interno.

Container Docker & LXC

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio Container Docker & LXC supporta le organizzazioni nella progettazione, implementazione sicura e gestione operativa di infrastrutture containerizzate basate su Docker, Docker Compose, LXC/LXD e, per ambienti più complessi, Kubernetes. La containerizzazione offre vantaggi significativi in termini di portabilità, isolamento e velocità di deployment—ma introduce una superficie d'attacco specifica che richiede competenze di sicurezza dedicate, spesso assenti nei team di sviluppo e operations tradizionali.

Il NIST e i principali framework di sicurezza cloud identificano la container security come area critica: immagini con vulnerabilità note, configurazioni di runtime non sicure, container in esecuzione con privilegi eccessivi e daemon Docker esposti in rete sono tra le cause più frequenti di compromissione in ambienti cloud-native.

Attività Incluse

Il servizio comprende: security review delle immagini Docker (vulnerability scanning con Trivy, Grype, Docker Scout; verifica dell'utilizzo di immagini base minimali e aggiornate; identificazione di segreti e credenziali embedded nei layer); hardening della configurazione del Docker daemon (TLS authentication, user namespace remapping, seccomp profiles, AppArmor profiles); implementazione di runtime security policies (no-new-privileges, read-only filesystem dove applicabile, capability dropping, resource limits); configurazione della segregazione di rete tra container con network policy appropriate; e definizione di un processo di image lifecycle management con scanning automatico nelle pipeline CI/CD.

Per LXC/LXD, configuriamo profili di sicurezza, limitazione delle capabilities, user namespace isolation e storage volume management con encryption at rest dove richiesto dal profilo di rischio.

Deliverable

Assessment della configurazione attuale con gap analysis, playbook di hardening implementato e documentato, configurazione dello scanning automatico delle immagini nelle pipeline di rilascio, e formazione operativa al team DevOps sui principi di container security.

Virtualizzazione PROXMOX

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio di Virtualizzazione Proxmox copre la progettazione, l'installazione, la configurazione sicura e la gestione operativa di infrastrutture di virtualizzazione basate su Proxmox VE—la piattaforma open source enterprise-grade per la gestione di macchine virtuali (KVM) e container Linux (LXC). Proxmox rappresenta oggi la scelta più adottata dalle PMI italiane che vogliono consolidare l'infrastruttura server su hardware on-premise riducendo i costi di licenza rispetto alle soluzioni VMware, mantenendo funzionalità enterprise come clustering, high availability, live migration e backup integrato.

Dognet Technologies ha maturato esperienza diretta nell'implementazione di infrastrutture Proxmox multi-nodo per clienti in diversi settori, con configurazioni che spaziano da ambienti single-node per uffici di piccole dimensioni fino a cluster ad alta disponibilità con storage condiviso Ceph per organizzazioni con requisiti di business continuity stringenti.

Attività Incluse

Il servizio comprende: sizing e progettazione dell'infrastruttura hardware in base ai requisiti di carico, ridondanza e budget; installazione e configurazione del cluster Proxmox con network bonding, VLAN tagging e separazione del traffico di storage, management e produzione; hardening dell'host Proxmox (accesso amministrativo con 2FA, certificati TLS, firewall host, audit logging, disabilitazione di servizi non necessari); configurazione dello storage (local LVM, directory, ZFS per integrità dei dati con snapshot e compressione, Ceph distribuito per cluster multi-nodo); implementazione di Proxmox Backup Server per backup incrementali cifrati con retention policy; migrazione di workload fisici (P2V) e da altre piattaforme di virtualizzazione; e monitoring dell'infrastruttura con alerting su risorse critiche.

Deliverable

Documentazione completa dell'architettura implementata, runbook operativo per le attività di routine (snapshot, backup, aggiornamenti, espansione del cluster), piano di disaster recovery con procedure di ripristino testate, e accesso a un contratto di supporto continuativo per interventi su malfunzionamenti e aggiornamenti critici.

Gestione Vulnerabilità

▸ CONSULENZA SISTEMISTICA

Panoramica del Servizio

Il servizio di Gestione delle Vulnerabilità di Dognet Technologies è un programma continuativo e strutturato per l'identificazione, la classificazione, la prioritizzazione e la remediation delle vulnerabilità di sicurezza presenti negli asset tecnologici dell'organizzazione—server, workstation, applicazioni, dispositivi di rete, asset cloud. A differenza di un singolo vulnerability scan occasionale, un programma di vulnerability management è un processo ciclico che garantisce visibilità continua sul livello di esposizione dell'organizzazione e dimostra miglioramento misurabile della postura di sicurezza nel tempo.

L'assenza di un programma strutturato di vulnerability management è uno dei gap più diffusi nelle PMI italiane: secondo le nostre analisi, oltre il 65% delle aziende con meno di 250 dipendenti non ha mai effettuato una scansione sistematica della propria infrastruttura. Questo significa che vulnerabilità critiche con exploit pubblicamente disponibili rimangono presenti per mesi o anni, offrendo agli attaccanti vettori di compromissione banalmente sfruttabili.

Componenti del Programma

Il programma si articola in quattro componenti funzionali integrati. Asset Discovery e Inventory: identificazione e catalogazione continua di tutti gli asset tecnologici—inclusi shadow IT, dispositivi non gestiti e asset cloud non inventariati—per garantire che nessun sistema rimanga fuori dalla copertura del programma. Un asset non inventariato è un asset non monitorato, e quindi una potenziale porta d'ingresso invisibile.

Vulnerability Scanning: scansioni programmate con frequenza adattata al profilo di rischio (settimanale per asset critici esposti, mensile per infrastruttura interna, ad ogni rilascio per applicazioni web) con strumenti professionali come Nessus, OpenVAS/Greenbone, Qualys o il modulo SentinelCore per ambienti PMI. Le scansioni autenticate forniscono una visibilità nettamente superiore rispetto a quelle non autenticate, identificando vulnerabilità di configurazione e software obsoleto non rilevabili dall'esterno.

Risk-Based Prioritization: il volume di vulnerabilità identificate in un'infrastruttura di medie dimensioni rende impossibile la remediation immediata di tutto. La prioritizzazione basata sul rischio reale—che integra severity CVSS, exploitability (EPSS score), esposizione dell'asset, criticità del business e presence of working exploits—permette al team IT di concentrare le risorse sulle vulnerabilità che rappresentano il rischio maggiore, non semplicemente quelle con lo score CVSS più alto.

Remediation Tracking e Reporting: workflow strutturato di assegnazione delle vulnerabilità ai responsabili, tracking dello stato di remediation con SLA differenziati per severity, gestione delle eccezioni con giustificazione e data di scadenza, e KPI periodici che dimostrano il miglioramento della postura di sicurezza nel tempo—indispensabili per il management, per i clienti e per i requisiti NIS2.

Integrazione con SentinelCore

Per i clienti che adottano la piattaforma SentinelCore di Dognet Technologies, il programma di vulnerability management è nativamente integrato con il modulo di scanning, il MicroSIEM per la correlazione degli eventi e il modulo Intellidog per il threat intelligence enrichment—che

contestualizza ogni vulnerabilità con informazioni su exploit attivi in the wild, TTPs dei gruppi che la sfruttano e indicatori di compromissione correlati.

Requisiti Normativi

Un programma strutturato di vulnerability management è esplicitamente richiesto da NIS2 (art. 21, misure di gestione dei rischi), PCI-DSS (Requisiti 6 e 11), ISO 27001 (Annex A 8.8), e dalle linee guida ENISA per la sicurezza delle reti e dei sistemi informativi. Il servizio di Dognet Technologies produce la documentazione necessaria a dimostrare la compliance a questi framework durante audit interni ed esterni.

Deliverable

Report mensile di vulnerability status con trend, KPI di remediation, eccezioni attive e vulnerabilità critiche aperte; dashboard operativa aggiornata in tempo reale; supporto alla pianificazione dei patch window; e reportistica per il management con esposizione del rischio residuo e progressione nel tempo.

OSINT — Open Source Intelligence

▸ INTELLIGENCE

Panoramica del Servizio

Il servizio OSINT (Open Source Intelligence) di Dognet Technologies raccoglie, analizza e struttura informazioni pubblicamente disponibili su un'organizzazione, un individuo, un dominio o un'infrastruttura tecnologica, con l'obiettivo di mappare la superficie di attacco esterna, identificare esposizioni non consapevoli e supportare attività di threat intelligence, due diligence e indagini di sicurezza. L'OSINT è la prima fase di qualsiasi attacco sofisticato: gli attaccanti passano settimane o mesi a raccogliere informazioni prima di lanciare un'operazione. Conoscere cosa è visibile dall'esterno è il primo passo per ridurre la superficie esposta.

Il nostro servizio è applicabile in tre contesti distinti: OSINT difensivo (analisi della propria esposizione pubblica per ridurre la superficie d'attacco), OSINT investigativo (raccolta di informazioni su soggetti terzi per due diligence, investigazioni di sicurezza o supporto legale), e OSINT come fase preparatoria a un penetration test o a un'operazione Red Team.

Fonti e Tecniche

Il processo OSINT sistematizza la raccolta da fonti eterogenee, organizzandole in categorie funzionali:

- Infrastruttura tecnica: enumerazione DNS (A, MX, TXT, SPF, DMARC, DKIM), certificate transparency logs (crt.sh, Censys), Shodan e FOFA per la mappatura dei servizi esposti su IP pubblici, Wayback Machine per l'analisi dello storico del sito, analisi dei meta-dati dei documenti pubblicati per identificare informazioni tecniche (versioni software, nomi utente, percorsi interni).
- Presenza digitale: analisi del sito web, social media aziendali e personali, profili LinkedIn di dipendenti (struttura organizzativa, stack tecnologico, ruoli chiave), GitHub e altri repository pubblici per codice sorgente, credenziali e segreti accidentalmente committati, offerte di lavoro che rivelano tecnologie in uso.
- Data breach e credential exposure: ricerca nei database di breach pubblici (HaveIBeenPwned, DeHashed, Leak-Lookup) per identificare indirizzi email e credenziali aziendali compromesse in breach precedenti, ancora utilizzabili per credential stuffing se non cambiate.
- Dark web e forum underground: ricerca su marketplace e forum del dark web per verificare la presenza di dati aziendali in vendita, discussion su vulnerabilità specifiche dei prodotti in uso, o menzioni dell'organizzazione in contesti criminali.
- Geospatial e physical: analisi di immagini satellitari, Street View e fotografie pubbliche per identificare informazioni sulla sede fisica, infrastrutture visibili esternamente, badge e accessi fotografati accidentalmente.

Strumenti e Workflow

Il processo utilizza strumenti consolidati nella community OSINT: Maltego per la visualizzazione grafica delle relazioni tra entità, theHarvester, Recon-ng e SpiderFoot per la raccolta automatizzata, Amass per l'enumerazione avanzata dei domini, Shodan e Censys per la ricerca di asset esposti, OSINT Framework come riferimento metodologico, e tool custom sviluppati da Dognet per casi d'uso specifici. Tutti i dati raccolti vengono organizzati in un grafo di relazioni che rende immediatamente visibile la struttura delle connessioni tra entità.

Casi d'Uso Principali

Due diligence pre-acquisizione o pre-partnership: analisi dell'esposizione pubblica e della reputazione digitale di un soggetto prima di stringere relazioni commerciali o investire. Analisi della superficie di attacco esterna: mappatura completa di tutto ciò che un attaccante può vedere della propria organizzazione, base per la prioritizzazione degli interventi di riduzione della superficie. Supporto a incident response: raccolta di informazioni sull'attaccante, sui domini di C2 utilizzati e sulle infrastrutture malevole per supportare la risposta all'incidente e potenzialmente l'attribuzione. Protezione VIP e brand protection: monitoring continuo per rilevare tentativi di impersonazione, domini typosquatting, account social fraudolenti e menzioni negative.

Deliverable

Report OSINT strutturato con: executive summary dell'esposizione identificata; grafo delle relazioni tra entità; finding dettagliati per categoria (infrastruttura, persone, breach, dark web); risk rating per ogni esposizione; e remediation actions specifiche e actionable per ridurre la superficie identificata.

Governance e Compliance: NIS2 — PCI-DSS — ISO 27001

▸ GOVERNANCE E COMPLIANCE

Panoramica del Servizio

Il servizio di Governance e Compliance di Dognet Technologies supporta le organizzazioni nel percorso verso la conformità ai principali framework normativi e standard di sicurezza informatica—NIS2, PCI-DSS e ISO 27001—attraverso un approccio concreto e operativo che trasforma i requisiti regolatori in controlli tecnici e organizzativi implementabili, verificabili e mantenibili nel tempo. Non vendiamo checklist da spuntare per superare un audit: costruiamo sistemi di gestione della sicurezza che funzionano e che reggono all'esame di auditor accreditati perché riflettono controlli realmente implementati, non solo documentati.

In un contesto in cui la Direttiva NIS2 è diventata obbligatoria per un'ampia platea di organizzazioni italiane, in cui le sanzioni per non conformità possono raggiungere il 2% del fatturato globale, e in cui i partner commerciali e i clienti enterprise richiedono sempre più spesso certificazioni ISO 27001 come prerequisito contrattuale, la compliance non è più un'opzione ma un requisito competitivo.

NIS2 — Direttiva sulla Sicurezza delle Reti e dei Sistemi Informativi

La Direttiva NIS2 (recepita in Italia con D.Lgs. 138/2024) estende gli obblighi di sicurezza informatica a oltre 10.000 organizzazioni italiane nei settori essenziali e importanti, imponendo misure di gestione del rischio, obblighi di notifica degli incidenti e responsabilità diretta del management. Il nostro percorso NIS2 si articola in: gap analysis rispetto ai requisiti dell'art. 21 (misure di gestione dei rischi di cybersecurity); implementazione dei controlli mancanti (politiche di sicurezza, gestione degli incidenti, continuità operativa, sicurezza della supply chain, autenticazione multi-fattore, cifratura, vulnerability management); preparazione della documentazione richiesta per la notifica all'autorità competente (ACN); e formazione del management sulle responsabilità personali previste dalla direttiva.

PCI-DSS — Payment Card Industry Data Security Standard

Lo standard PCI-DSS v4.0 è obbligatorio per qualsiasi organizzazione che gestisce, processa o memorizza dati di carte di pagamento, indipendentemente dalle dimensioni. La non conformità espone a sanzioni contrattuali da parte dei circuiti di pagamento, all'aumento delle commissioni di processing e, in caso di breach, a responsabilità dirette per le frodi generate. Il nostro percorso PCI-DSS include: scoping dell'ambiente dei dati di carta (CDE), gap analysis rispetto ai 12 requisiti PCI-DSS v4.0, implementazione tecnica dei controlli mancanti (segmentazione di rete, crittografia, logging, vulnerability management, penetration testing), preparazione della documentazione per il Self-Assessment Questionnaire (SAQ) o per il Report on Compliance (RoC) con QSA accreditato.

ISO 27001:2022 — Sistema di Gestione della Sicurezza delle Informazioni

La certificazione ISO 27001 è lo standard internazionale per i Sistemi di Gestione della Sicurezza delle Informazioni (ISMS) e rappresenta la dimostrazione più riconosciuta a livello globale di un approccio maturo e sistematico alla sicurezza informatica. Il nostro percorso di implementazione ISO 27001 copre: definizione dello scope dell'ISMS e del contesto organizzativo; valutazione del rischio informatico secondo la metodologia ISO 27005; selezione e implementazione dei controlli dell'Annex A (aggiornato nella versione 2022 con 93

controlli organizzati in 4 domini); sviluppo della documentazione obbligatoria (politiche, procedure, statement of applicability); preparazione e supporto durante l'audit di certificazione con ente accreditato; e mantenimento del sistema con audit interni e riesame della direzione.

Approccio Integrato

Per organizzazioni soggette a più framework, implementiamo un approccio di compliance integrata che mappa i requisiti comuni tra NIS2, PCI-DSS e ISO 27001, implementando controlli condivisi una volta sola ed evitando la duplicazione degli sforzi. La maggior parte dei controlli tecnici—vulnerability management, logging e monitoring, gestione degli accessi privilegiati, cifratura, incident response—è richiesta da tutti e tre i framework con requisiti largamente sovrapponibili. Un'implementazione integrata riduce i costi e i tempi rispetto a percorsi separati per ogni standard.

Deliverable

Gap analysis documentata con mapping verso i requisiti normativi applicabili; piano di implementazione con milestones, responsabilità e budget stimato; set completo di policy, procedure e documentazione tecnica; evidence package per audit interni ed esterni; formazione del personale sui requisiti e sulle responsabilità; e supporto continuativo per il mantenimento della conformità e la gestione degli audit periodici.

Seguiteci sui social

- https://www.linkedin.com/company/dognet-technologies
- https://www.instagram.com/dognettechnologies
- https://youtube.com/shorts/5j2p7vyWW4k?si=tkkS3gRqkt2Utic
- https://www.facebook.com/people/Dognet-Technologies/6157003660737