DOGNETTECHNOLOGIES

Catalogo dei Servizi di Cybersecurity 2026

Ethical Hacking and Linux Extreme

DOGNETTECHNOLOGIES

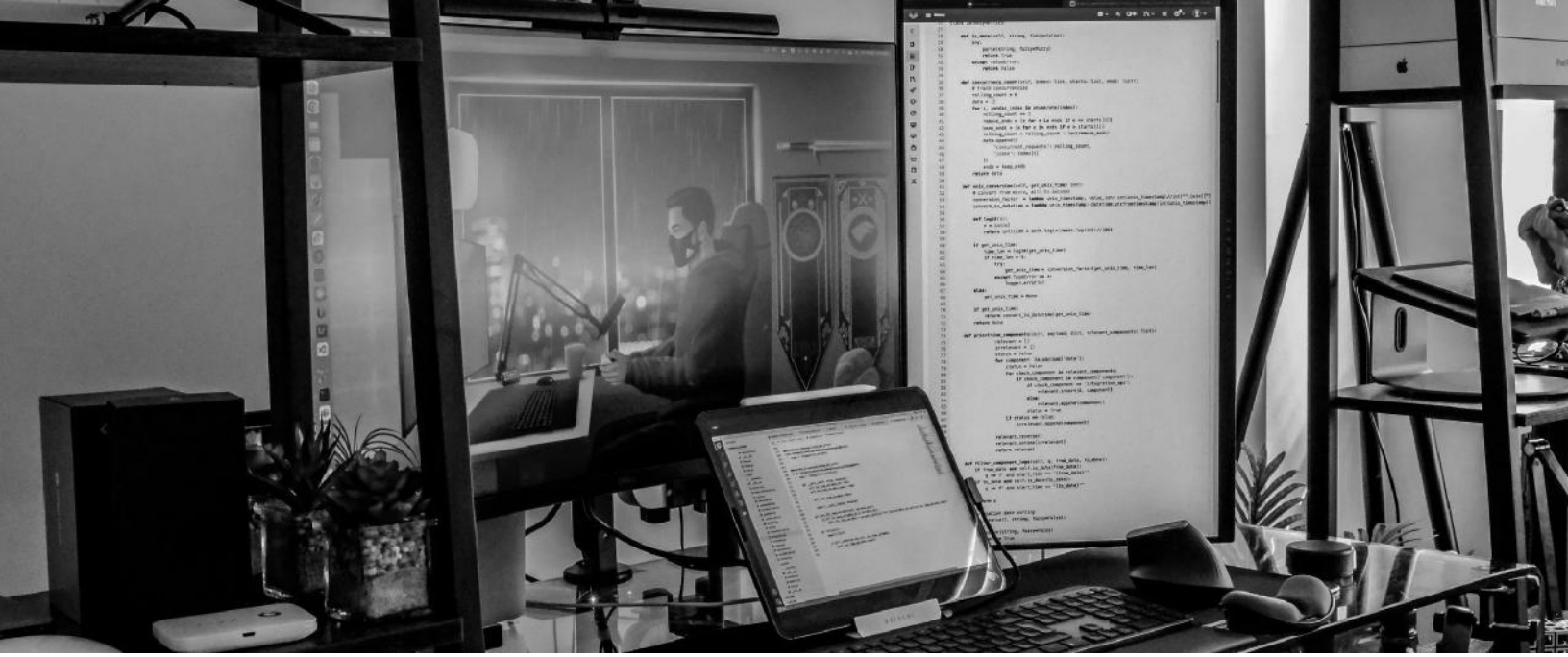
Indice

Introduzione

Dognet Technologies offre soluzioni all'avanguardia per garantire la sicurezza informatica della tua azienda. Con un team di esperti dedicati e una metodologia comprovata, trasformiamo le tue esigenze di sicurezza in realtà affidabili e robuste. Garantiamo un aumento della resilienza e una gestione delle vulnerabilità imbattibile. Siamo un team di esperti con alle spalle progetti importanti per grandi aziende, abbiamo ottenuto certificazioni ampiamente riconosciute che garantiscono il nostro operato.

Scopri i nostri servizi:

Visita il nostro spazio virtuale su Slack



Ethical Hacking

Caratteristiche Fondamentali

Questa categoria raccoglie tutti i servizi orientati alla simulazione offensiva: attivita in cui i nostri specialisti assumono il punto di vista dell'attaccante per identificare e sfruttare concretamente le vulnerabilita presenti negli asset aziendali, prima che lo faccia qualcun altro.
Gli interventi spaziano dal classico Vulnerability Assessment e Penetration Test su reti, sistemi e applicazioni web, fino ad analisi piщ verticali come l'Active Directory Assessment — che mappa i percorsi di escalation privilege verso il domain controller — e il Web Assessment, focalizzato su portali, e-commerce e API secondo la metodologia OWASP. Per chi sviluppa software internamente, la Code Review analizza il codice sorgente prima del rilascio, intercettando injection flaw, debolezze crittografiche e business logic vulnerability che gli scanner automatici non vedono. Le sessioni Red Team e Purple Team portano la simulazione al livello successivo: non piщ il singolo test tecnico, ma la verifica della capacita difensiva complessiva dell'organizzazione, con mappatura MITRE ATT&CK di ogni tecnica utilizzata. Per contesti ad alto rischio и disponibile il servizio Tiger Team, che combina penetration test cyber con physical security testing in operazioni multi-vettore. Completano la categoria l'analisi di dispositivi IoT e hardware embedded, la sicurezza delle reti wireless e dei protocolli radio, e il servizio OSINT, che mappa tutto cit che un attaccante put raccogliere sull'azienda prima ancora di lanciare un attacco.

Elenco completo dei nostri servizi di ethical hacking

- Vulnerability Assessment & Penetration Test (VAPT)
  Identificazione e sfruttamento controllato delle vulnerabilita presenti su reti, sistemi, applicazioni e cloud. Report con severity CVSS, proof-of-concept e remediation specifica. Retesting gratuito sui finding critici.

- Web Assessment
  Analisi di sicurezza approfondita su applicazioni web, portali aziendali, e-commerce e API. Segue la metodologia OWASP Testing Guide. Individua vulnerabilita di business logic non rilevabili da scanner automatici.

- Active Directory Assessment
  Analisi tecnica dell'infrastruttura identitaria Microsoft (AD, Azure AD, ambienti ibridi). Mappatura di attack path con BloodHound, analisi di Kerberoasting, DCSync, escalation privilege e percorsi verso il domain controller.

- Revisione del Codice (Code Review)
  Analisi del codice sorgente per identificare vulnerabilita di sicurezza (injection, autenticazione, crittografia, business logic) prima del rilascio in produzione. Supporto per Java, Python, PHP, JavaScript, Go, C/C#.

- Sessioni Red Team / Purple Team
  Simulazione di attacchi reali multi-vettore (cyber + social engineering) per testare la capacita difensiva complessiva. Il modello Purple Team esegue le tecniche MITRE ATT&CK in coordinamento con il team interno per migliorare la detection.

- Tiger Team & BlackOps
  Operazioni avanzate che combinano penetration test cyber e physical security testing (intrusione fisica controllata, badge cloning, hardware implant in CED). Per organizzazioni con requisiti di sicurezza elevati. Per questo servizio e' necessario stipulare contratti legali dedicati e agire in un perimetro ben definito.

- Hardware & IoT Security Assessment
  Analisi di sicurezza su dispositivi connessi: firmware, interfacce fisiche (UART, JTAG), protocolli radio (Zigbee, BLE, LoRaWAN), API di gestione. Critico per manifatturiero, healthcare, smart building.

- Radio & WiFi Security Analysis
  Verifica dei protocolli WiFi enterprise (WPA2/WPA3, 802.1X), analisi di rogue access point, Evil Twin, resistenza agli attacchi di deautenticazione. Analisi di protocolli radio specifici con hardware SDR.

- OSINT — Open Source Intelligence
  Mappatura della superficie di attacco esterna: asset esposti, dipendenti, tecnologie, credential nei breach pubblici, dark web monitoring. Indispensabile prima di qualsiasi test e come audit preventivo della propria esposizione.

Intelligence, Risk & Compliance

Caratteristiche Fondamentali

Questa categoria affronta la dimensione strategica e normativa della sicurezza informatica, fornendo alle organizzazioni gli strumenti per comprendere il proprio livello di esposizione reale, soddisfare i requisiti regolatori e prendere decisioni informate sugli investimenti in sicurezza. La Valutazione del Rischio segue le metodologie ISO 27005 e NIST RMF per produrre una mappa del rischio comprensibile sia per il management che per i team tecnici, identificando le aree di maggior esposizione su cui concentrare le risorse. Il servizio di Cyber Threat Intelligence va oltre i semplici feed di indicatori di compromissione: fornisce intelligence contestualizzata su threat actor, campagne attive e TTP rilevanti per il settore del cliente, integrandosi direttamente con SIEM, firewall ed EDR per una detection più efficace. La Gestione delle Vulnerabilità è un programma continuativo — non un'attività una tantum — che combina scanning periodico, prioritizzazione basata sul rischio reale tramite EPSS score, e tracking della remediation con KPI misurabili nel tempo. La Valutazione GDPR analizza la conformità al Regolamento 679/2016 integrando la prospettiva giuridica con quella tecnica, producendo documentazione utilizzabile durante eventuali ispezioni del Garante. Infine, il servizio di Governance e Compliance accompagna le organizzazioni nei percorsi verso NIS2, PCI-DSS e ISO 27001, con un approccio integrato che implementa i controlli condivisi tra i framework una volta sola, riducendo tempi e costi rispetto a percorsi separati.

Elenco completo dei nostri servizi di CTI

- Valutazione del Rischio
  Identificazione, analisi e prioritizzazione dei rischi cyber secondo ISO 27005 e NIST RMF. Mappa del rischio comprensibile per management e team tecnici. Base documentale per audit ISO 27001, NIS2 e PCI-DSS.

- Cyber Threat Intelligence (CTI)
  Intelligence su minacce rilevanti per il settore del cliente: feed IoC integrabili in SIEM/firewall/EDR, threat actor profiling, dark web monitoring, alerting su campagne attive. Quattro livelli: strategica, tattica, operazionale, tecnica.

- Gestione delle Vulnerabilita
  Programma continuativo di scanning, prioritizzazione basata su rischio reale (CVSS + EPSS + criticita business), remediation tracking con SLA, KPI periodici per management e compliance NIS2/PCI-DSS.

- Valutazione GDPR
  Gap analysis della conformita al Regolamento Europeo 679/2016: trattamenti, basi giuridiche, misure di sicurezza (art. 32), documentazione obbligatoria, gestione dei diritti degli interessati. Report utilizzabile per audit del Garante.

- Governance & Compliance (NIS2 / PCI-DSS / ISO 27001)
  Percorso strutturato verso la conformita ai principali framework normativi. Gap analysis, implementazione dei controlli, documentazione completa, supporto durante audit. Approccio integrato per chi и soggetto a piщ standard contemporaneamente.

Progettazione e Attività Sistemistiche

Caratteristiche Fondamentali

Questa categoria comprende gli interventi tecnici diretti sull'infrastruttura IT aziendale, con l'obiettivo di costruire ambienti sicuri, stabili e gestibili nel tempo. Il punto di partenza e' spesso l'hardening dei sistemi Linux: un processo strutturato che riduce la superficie di attacco a livello di kernel, filesystem, autenticazione e servizi, seguendo i CIS Benchmarks e producendo script di automazione Ansible per rendere il risultato ripetibile e auditabile. Per chi vuole modernizzare l'infrastruttura server, il servizio di architettura e progettazione offre soluzioni enterprise-grade basate su Proxmox VE — con clustering ad alta disponibilita, storage Ceph distribuito e networking software-defined con VLAN microsegmentate — a un costo drasticamente inferiore rispetto alle piattaforme VMware. Il servizio di Baseline e Deployment produce template VM e container pre-hardened e compliance-ready, eliminando la necessita di riconfigurare ogni nuova istanza da zero. Per ambienti containerizzati Docker e LXC, interveniamo su sicurezza delle immagini, hardening del daemon e integrazione dello scanning nelle pipeline CI/CD. La gestione dei dispositivi di rete copre router, switch e firewall dei principali vendor, con hardening, monitoring continuo e documentazione aggiornata.
Chiude la categoria il servizio di Log Storage & Analysis, che progetta e implementa pipeline di raccolta e correlazione dei log necessarie sia per la detection degli incidenti che per soddisfare i requisiti di retention di GDPR, NIS2 e PCI-DSS.

Elenco completo dei nostri servizi di consulenza e attivita' sistemistiche

- Hardening dei Sistemi Linux
  Riduzione della superficie di attacco su Debian, Ubuntu, Oracle Linux. Kernel hardening, AppArmor/SELinux, SSH, PAM, firewall. Basato su CIS Benchmarks Livello 1 e 2. Automation script Ansible per deployment ripetibile.

- Architettura & Progettazione Infrastrutture
  Progettazione di ambienti IT moderni basati su virtualizzazione open source: cluster Proxmox HA, storage Ceph, Software-Defined Networking con VLAN microsegmentate, hybrid cloud. Alternativa enterprise a VMware a costi contenuti.

- Virtualizzazione Proxmox
  Installazione, configurazione sicura e gestione di infrastrutture Proxmox VE: clustering, live migration, backup con Proxmox Backup Server, hardening host, migrazione da VMware. Esperienza diretta su ambienti multi-nodo.

- Baseline & Deployment (Golden Image)
  Template VM e container Linux pre-configurati, hardened e compliance-ready (NIS2, PCI-DSS, CIS, ISO 27001). Pronti per deployment immediato. Eliminano settimane di hardening manuale su ogni nuova istanza.

- Container Docker & LXC
  Security review di immagini Docker (Trivy, Grype), hardening del daemon, seccomp/AppArmor profiles, capability dropping, scanning automatico in pipeline CI/CD. Configurazione sicura di LXC/LXD con user namespace isolation.

- Log Storage & Analysis
  Progettazione e implementazione di pipeline di log management scalabili (stack Elastic, Graylog, object storage). Regole di correlazione per detection automatica. Compliance con requisiti di retention GDPR, NIS2, PCI-DSS.

- Gestione Network Device
  Configurazione, hardening e manutenzione di router, switch, firewall, access point (Cisco, Fortinet, Palo Alto, MikroTik, pfSense). Gap analysis vs CIS Benchmarks, VLAN policy, monitoring continuo con alerting.

Le nostre fasce di servizi

Per le vostre esigenze, offriamo:

Servizi/Fasce	Essential	Pro	Deluxe
Vulnerability Assessment	Presente	Presente	Presente
Penetration Test / Red Team	Assente	Presente	Presente
Threat Intelligence	Limitato	Limitato	Presente
Canale Slack Dedicato	Assente	Limitato	Presente
Assistenza/Consulenza	Limitato	Presente	Presente
Governance	Assente	Assente	Presente
SYS Admin	Assente	Limitato	Presente

Le nostre fasce di servizi

Descrizione e contenuti:

Fascia Essential

VA COMPLETO:

- Il VA comprende 3 scansioni automatiche e servizio di early warnings mensile
- Valutazione del rischio

ASSISTENZA CONSULENZA LIMITATA:

- L'assistenza è limitata in caso di attacco e la consulenza è telefonica, o al limite, nel canale slack solo su invito per un periodo limitato di tempo. Non è 24x24 7x7 ma solo negli orari d'ufficio dal lun al ven fino a 20 ore mensili

THREAT INTELLIGENCE LIMITATA:

- domain threat intelligence 2 volte l'anno

Fascia Pro

PT2 E ASSISTENZA/CONSULENZA COMPLETA:

- Indica 1 pentest l'anno e le simulazioni di red/blu team completi.
- Assistenza e consulenza 24x24 7x7 tramite telefono o canale slack (su invito) su qualsiasi questione Assistenza SysAdmin, SIEM e progettazione IDS/IPS no a 40 ore mensili.

VA LIMITATA:

- Il VA è limitato nel senso che ci sono solo le scansioni automatiche 2 volte l'anno, non 3.

THREAT INTELLIGENCE LIMITATA:

- Domain Threat Intelligence e a 1 Ramsonware Risk Indicator all'anno

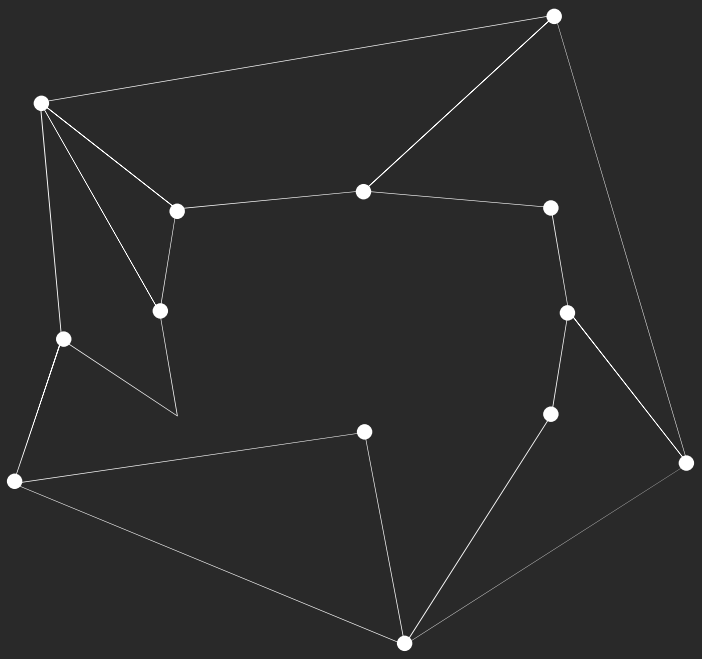
Fascia Deluxe

- Indica 1 Pentest o 1 RedTeam l'anno
- Vuln Assessment 3 volte l'anno + early warnings settimanale + 1 valutazione del rischio
- CTI comprende 1 domain threat intelligence +1 Ramsonware Risk Indicator + 1 GDPR validator all'anno
- Canale slack dedicato riservato con consulenza/assistenza per qualsiasi questione 24x24 7x7
- Governance, stesura policy e verifica annuale dell'efficacia
- Assistenza SysAdmin, SIEM e progettazione IDS/IPS su richiesta (consulenza/assistenza) fino 80 ore mensili
- Accesso ai nuovi servizi come SOC e log analysis

NOTA BENE

Il monte ore compreso nel piano è il limite massimo di ore fatturabili al prezzo di 25€/h.
Superato il limite si applica il prezzo standard in base al tipo di servizio oggetto dell'assistenza.
Se le ore non vengono utilizzate verrà fatturato solo il 50% dell'importo non l'intero monte ore previsto dalla fascia associata.

I prezzi potrebbero subire delle maggiorazioni in base alla grandezza dell'infrastruttura e alla superficie d'attacco.



Contatti

“Dognet ha trasformato il nostro approccio alla sicurezza. Affidabili e professionali!” – Cliente Soddisfatto

Visita: www.dognet.tech

Email: info@dognet.tech

Telefono: 351-5568240
352-0321176

dognet TECHNOLOGIES