// AI-POWERED SECURITY PLATFORM · v1.4

CyberLens

L’Ecosistema Integrato per la Cyber Resilience Strategica

CyberLens non è solo un tool di analisi, ma il punto d’incontro tra **Compliance normativa**, **Intelligence offensiva** e **Difesa attiva**. Progettata per le sfide di sicurezza del 2026, la piattaforma trasforma la complessità dei dati in una roadmap d’azione chiara e automatizzata.

Compliance Full-Stack

Gestione nativa NIS2 e DORA, ogni controllo tecnico allineato agli obblighi legali europei.

Intelligence sulle Minacce

OWASP Top 10 (2025) e MITRE ATT&CK;® per visibilità totale su tattiche e tecniche degli avversari.

ATT&CK; to D3FEND

Mappatura automatica da ogni tecnica ATT&CK; ai corrispondenti artefatti di difesa D3FEND™.

// AI-DRIVEN REMEDIATION: IL POAM INTELLIGENTE

Il vero cuore operativo di CyberLens è il motore AI che trasforma i risultati in un **Plan of Action and Milestones (POAM) dinamico**:

01 **Prioritizzazione Predittiva**
L’AI valuta CVSS, contesto aziendale e criticità degli asset per stabilire cosa risolvere per primo.

02 **Suggerimenti Tecnici**
Ogni vulnerabilità è accompagnata da istruzioni di mitigazione precise e testate.

03 **Timeline di Implementazione**
Stime accurate dei tempi di risoluzione per ottimizzare il carico IT e rispettare le scadenze di compliance.

30'	M1→M7	100%	NIS2+
da dominio a report PDF	moduli integrati	automazione AI	compliance documentata

NIS2 · DORA · OWASP Top 10 2025 · MITRE ATT&CK® · D3FEND™ · EPSS/NVD

// 01 — IL PROBLEMA

Il Vulnerability Assessment tradizionale si è evoluto.

Le organizzazioni italiane affrontano un paradosso: la normativa europea (NIS2, DORA) impone valutazioni periodiche della sicurezza, ma i VA tradizionali sono incompatibili con le realtà operative delle PMI e dei team IT interni.

2–4 settimane

Tra scansione, analisi manuale e redazione del report. Nel frattempo le vulnerabilità restano esposte.

Costi proibitivi

Consulenti specializzati, licenze enterprise e ore di analisi rendono il VA accessibile solo alle grandi organizzazioni.

Report illeggibili

Liste di CVE senza contesto né priorità. Il management non capisce, il team tecnico non sa da dove iniziare.

CyberLens risolve tutto questo. 30 minuti, costo radicalmente inferiore. Executive Summary leggibile, POAM operativo, documentazione NIS2/DORA pronta per l'audit. Mentre i tool tradizionali segnalano i problemi, CyberLens **chiude il cerchio**: individua la falla, mappa la difesa e pianifica la risoluzione, riducendo il **Mean Time to Remediate (MTTR)**.

// Dashboard CyberLens — Indice di Rischio, metriche CVE/Kill Chain/D3FEND e Score Breakdown

// 02 — ARCHITETTURA

Pipeline modulare M1→M7.

Ogni modulo è indipendente e produce output strutturato per il successivo. Puoi usare la pipeline completa o singoli moduli dalla CLI o dashboard web.

M1 // OSINT	**OSINT Engine**	Ricognizione passiva e attiva della superficie esposta. SpiderFoot per OSINT, Nmap per porte e servizi, ZAP per DAST, Nikto, SSLScan per TLS.	SpiderFoot · Nmap · ZAP · Nikto · SSLScan
M2 // CVE	**CVE Intelligence**	Arricchisce ogni CVE con CVSS score, probabilità exploit EPSS, PoC pubblici da ExploitDB e GitHub. Identifica vulnerabilità da sfruttare immediatamente.	NVD · EPSS · ExploitDB · GitHub
M3 // ATT&CK;	**ATT&CK; Mapper**	Mappa le vulnerabilità sulle 14 fasi della kill chain MITRE ATT&CK; tramite CWE. Associa contromisure D3FEND a ogni tecnica rilevata.	MITRE STIX · D3FEND
M4 // AI	**AI Orchestrator**	Claude AI genera Executive Summary, POAM con timeline operativa e analisi dettagliata delle 5 CVE più critiche. Report PDF professionale in output.	Claude AI · POAM · Report
M6 // DIFF	**Diff Engine**	Confronta la superficie non autenticata con quella post-login. Identifica vulnerabilità esposte solo agli utenti autenticati e calcola il delta di rischio.	Auth diff · Risk delta
M7 // RED TEAM	**Red Team Engine**	Pentest autonomo basato sul profilo di rischio. Metasploit per exploit CVE, Nuclei per scanner automatico, Hydra per brute force, ffuf per fuzzing.	Metasploit · Nuclei · Hydra · ffuf

// 03 — OUTPUT

Report completi, pronti per l'audit.

Il report PDF viene generato automaticamente al termine della pipeline — nessun intervento manuale, nessuna configurazione. Pronto per essere consegnato al cliente, al management o all'auditor.

Executive Summary AI

Sintesi leggibile dal management con Risk Score, grade e raccomandazioni strategiche generate da Claude AI.

CVE con CVSS ed EPSS

Ogni CVE con severità CVSS, probabilità exploit EPSS, PoC pubblici e urgenza di remediation (Immediata/30gg/90gg).

Kill Chain MITRE ATT&CK;

Mapping sulle 14 fasi della kill chain con tecniche rilevate, tattiche e copertura complessiva.

Contromisure D3FEND

Per ogni tecnica ATT&CK; identificata, le contromisure D3FEND con priorità e effort stimato.

POAM Operativo

Piano azioni immediata, 30gg, 90gg e pianificata — con responsabili, deadline e stima effort per ogni azione.

OWASP Top 10 2025

Mapping dei finding ZAP sulle categorie OWASP con distribuzione per severità e dettaglio finding.

SSL/TLS Analysis

Certificati, protocolli abilitati, cipher suite deboli e configurazioni errate con evidenza tecnica.

Diff Auth/Unauth

Delta tra superficie pubblica e autenticata — identifica le vulnerabilità interne esposte post-login.

// SCALA RISK SCORE

0–20	A	Verde	Molto Basso
21–40	B	Azzurro	Basso
41–70	C	Giallo	Medio
71–85	D	Arancio	Significante
86–100	F	Rosso	Alto/Critico

// 04 — COMPLIANCE

NIS2, DORA e audit documentati automaticamente.

NIS2

Network and Information Security Directive 2

Obbliga le organizzazioni essenziali e importanti a implementare misure di gestione del rischio informatico con VA periodici documentati.

- Analisi e gestione del rischio (Art. 21)
- Misure tecniche documentate per audit
- Reporting incidenti entro 72 ore
- Valutazione periodica della sicurezza

DORA

Digital Operational Resilience Act

Impone al settore finanziario test di resilienza operativa digitale, inclusi penetration test con metodologie standardizzate (TLPT).

- TLPT Threat-Led Penetration Testing
- Gestione rischio ICT continuativa
- Mappatura dipendenze tecnologiche
- Reportistica strutturata per audit

VA

Vulnerability Assessment Periodico

Best practice e requisiti normativi richiedono scansioni frequenti. CyberLens le rende economicamente sostenibili su base mensile.

- Report PDF professionale per audit
- Storico scansioni e trend nel tempo
- POAM con deadline e responsabili
- Evidenza remediation completate

// 05 — PER CHI

[PMI · Aziende]

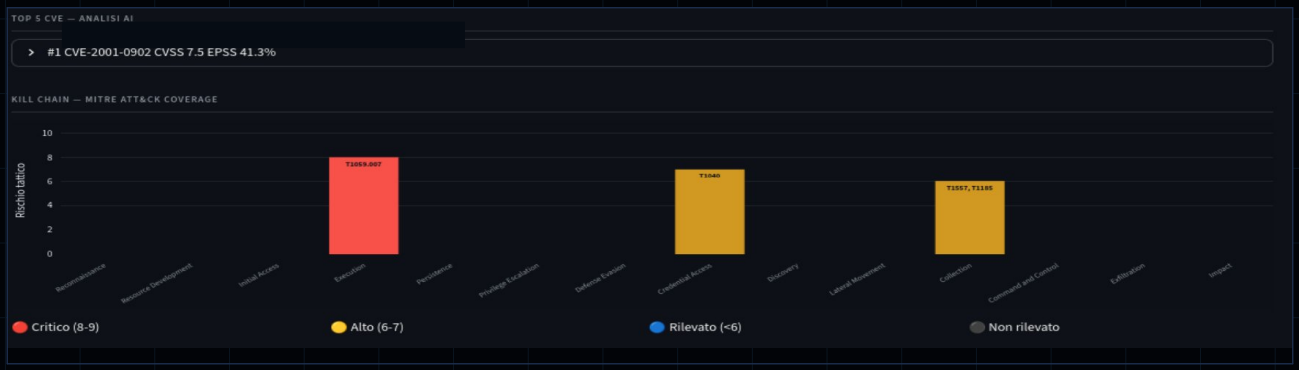
Sicurezza enterprise a costo accessibile.

- Report leggibile dal management
- Compliance NIS2/DORA documentata
- POAM con priorità chiare
- Scansioni mensili sostenibili

[MSSP · System Integrator]

Scala il business con AI integrata.

- White label con il tuo brand
- API per integrazione sistemi
- Multi-tenant: gestisci tutti i clienti
- Margini elevati su servizio ad alto valore



// Kill Chain MITRE ATT&CK; Coverage — rischio tattico per fase, tecniche rilevate e copertura della kill chain

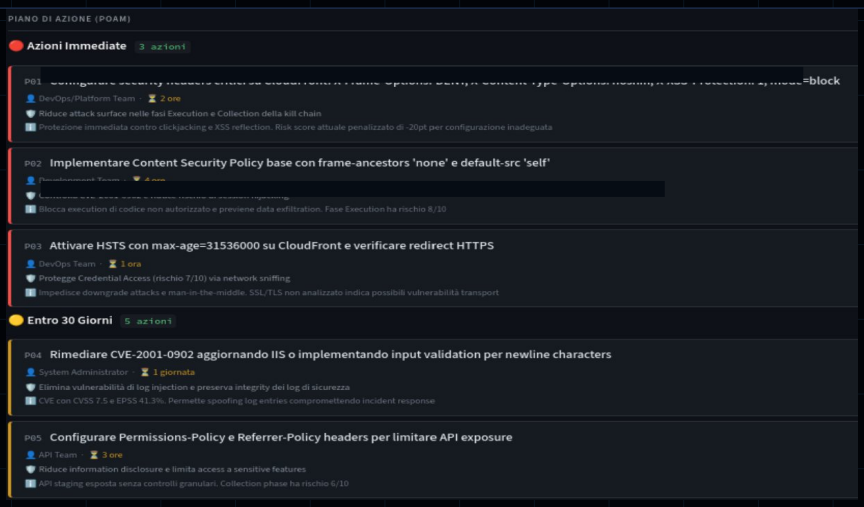
// INIZIA OGGI

Demo gratuita sul tuo dominio reale.

In 30 minuti vedi un report completo sulla tua superficie d'attacco. Nessun impegno, nessuna installazione. Solo risultati concreti.

[Richiedi demo gratuita]

// EMAIL	// WEB	// SEDE
info@cyberlens.it	www.cyberlens.it	Italia ■■



// POAM — Piano di Azione con priorità operative: azioni immediate, 30gg e 90gg con responsabili e effort stimato