EXPOSURE & REMEDIATION MANAGEMENT

REMEDIA [ExpOps]

Tutta l'esposizione. Una sola regìa.

Aggrega vulnerabilità e finding da oltre 60 fonti — VM, AppSec, cloud, OT, pentest e segnalazioni — in un unico repository normalizzato e deduplicato. Prioritizzato sul rischio reale, assegnato in automatico, orchestrato fino alla chiusura verificata.

Aggrega. **Prioritizza.** **Rimedia.** **Dimostra.**

— IL PROBLEMA

Non ti serve un altro scanner. Ti serve una regìa.

Gli strumenti di rilevazione li hai già — spesso più d'uno, per dominio. Quello che manca è governare un output che arriva da decine di fonti in formati diversi e non confrontabili.

Fonti frammentate

Scanner infrastrutturali, AppSec, cloud, OT, pentest e segnalazioni: ogni strumento parla una lingua diversa.

Priorità non condivisa

Il CVSS da solo non dice quali falle sono davvero sfruttate né quanto conta l'asset colpito.

Remediation non tracciata

Chi risolve cosa, entro quale SLA, con quale verifica? La chiusura non è dimostrabile.

Conformità da provare

PCI, ISO 27001, NIS2 e DORA chiedono evidenza della postura. Ricostruirla a mano è fragile.

REMEDIA non sostituisce i tuoi strumenti: li integra. Una piattaforma alimentata da tutte le tue fonti — in produzione, multi-tenant.

COME FUNZIONA

Da decine di fonti a un'unica pipeline governata.

SAAS | EXPOSURE MGMT | MULTI-TENANT | IT / EN

REMEDIA ingerisce qualsiasi fonte, normalizza ogni finding su uno schema unico — CVE, CVSS, asset, business unit, ambiente — lo arricchisce con l'intelligence sugli exploit e ne governa il ciclo di vita fino alla chiusura verificata.

Due flussi, due costi

- ✓ **Fonti strutturate** (API, CSV, XML, JSON, SARIF) → parser deterministici, nessun costo AI.
- ✓ **Report non strutturati** (PDF, DOCX) → Parsing AI con revisione di un analista.

LA PIPELINE DI NORMALIZZAZIONE

01
Ingestione
60+ connettori, upload report, inserimento manuale

02
Parsing AI
Estrazione dei finding dai PDF non strutturati

03
Normalizzazione
Schema unico + enrichment NVD / KEV / EPSS

04
Deduplica
Merge cross-scanner dei duplicati

05
Prioritizzazione
VBR 2.0: exploit, EPSS, CVSS, asset, esposizione

06
Orchestrazione
Owner, campagne, SLA e tracking

Primo valore già in pochi giorni: un repository unico e consultabile.

COPERTURA

60+ connettori. Tutta la superficie, un solo posto.

VM / Infrastruttura

Tenable · Rapid7 · Qualys · CrowdStrike · Defender · Nessus · OpenVAS

AppSec — SAST/DAST/SCA

Snyk · Checkmarx · Veracode · GitHub AS · Semgrep · SonarQube

Cloud / CNAPP

Wiz · Orca · Prisma Cloud · Lacework · Sysdig · Defender for Cloud

Container / K8s

Trivy · Grype · Prisma Compute · Anchore · Kubescape

OT / ICS / IoT

Nozomi · Claroty · Dragos · Armis · Tenable OT

CMDB / CAASM

ServiceNow · BMC Helix · Device42 · Lansweeper · Tanium · Axonius

ITSM / Ticketing

Jira · ServiceNow · Zendesk · PagerDuty · Opsgenie · BMC Helix

Threat Intel / EASM

CISA KEV · EPSS · OSV · Cyberfero Early Warning · Shodan · Censys

Patch / Deploy

Ansible · Automox · BigFix · Intune

Fonti strutturate via API o file; pentest e report non strutturati via Parsing AI. Nuovi connettori aggiunti su richiesta.

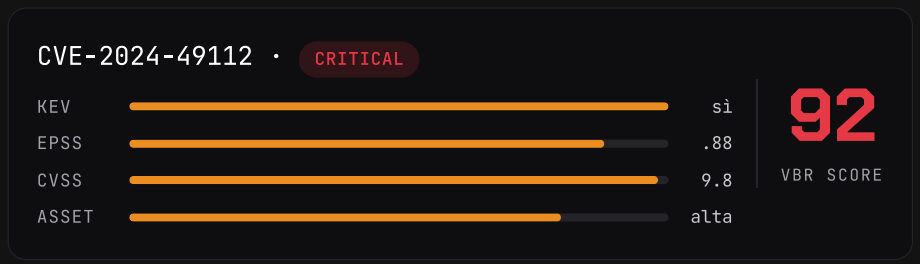
FUNZIONALITÀ

Il motore: prioritizza e orchestra la remediation.

CORE

Prioritizzazione VBR 2.0

Vulnerability-Based Risk: combina maturità dell'exploit (CISA KEV, ransomware, Metasploit, Exploit-DB), probabilità EPSS, gravità CVSS, criticità dell'asset ed esposizione a Internet. L'urgenza reale, non solo il punteggio tecnico.



Orchestrazione remediation

Campagne per tema, regole e playbook automatici, patch management con push e verifica verso Ansible, Automox, BigFix e Intune.

SLA policy-driven + escalation

Stati e scadenze per severità e policy (KEV, esposti), escalation automatica al contatto, digest periodici agli owner.

Deduplica cross-scanner

Un unico finding quando più strumenti riportano la stessa CVE sullo stesso asset: niente doppioni, niente rumore.

Assegnazione al Server Owner

Hostname → owner dalla CMDB o dal mapping manuale, con portale sicuro dedicato.

GOVERNANCE & INSIGHT

Misura la postura. Dimostra la conformità.

Analytics & metriche

MTTR, velocità (nuovi vs risolti), aging, rispetto degli SLA, scorecard per Business Unit e Server Owner.

Conformità multi-framework

PCI-DSS 4.0, CIS v8, ISO 27001:2022, NIS2, DORA, NIST CSF 2.0, GDPR e SOC 2. Report firmabile in PDF.

Risk graph & attack path

Vista relazionale del blast-radius: dove un singolo fix riduce di più il rischio sull'intero parco di asset.

CAASM & EASM

Gap di copertura degli asset e superficie esterna esposta (Shodan/Censys + crt.sh, DNS, InternetDB).

Report executive per il vertice

Risk score, trend e priorità in un report automatico, commentato dagli analisti Cyberfero, schedulabile ed esportabile in PDF white-label con il logo del cliente — la stessa fonte di dati che alimenta la vista operativa dei tecnici.

- MTTR & VELOCITÀ
- RISPETTO SLA
- SCORECARD BU / OWNER
- CONFORMITÀ 8 FRAMEWORK

L'INTERFACCIA

Per i team tecnici: una sola coda di lavoro.

DASHBOARD OPERATIVA · MULTI-TENANT

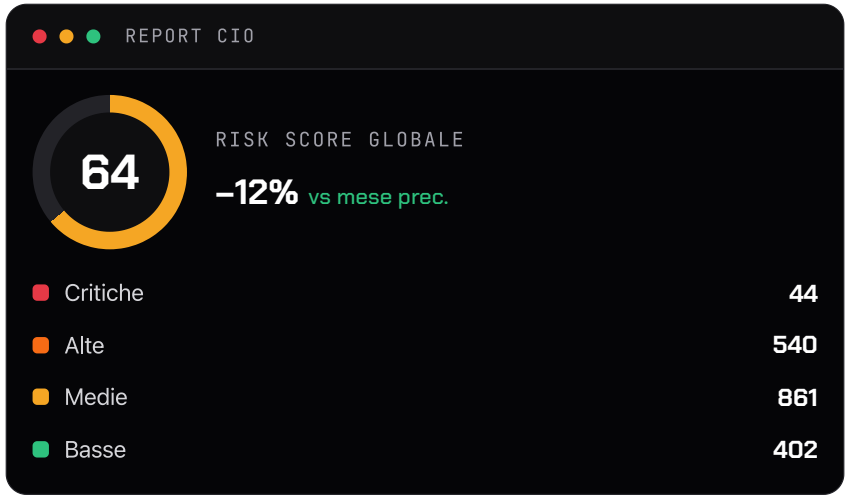
VULN. APERTE	CRITICHE	KEV SFRUTTATE	RISPETTO SLA
1.847	44	12	86%
▼ 312 (30gg)	▲ 6	priorità assoluta	▲ +9%

REPOSITORY VULNERABILITÀ

CVE	SEV.	VBR	ASSET	OWNER
CVE-2026-41089	CRIT	96	SRV-DC-01	CC
CVE-2024-49112	CRIT	92	SRV-DC-01	CC
CVE-2024-5535	CRIT	78	APP-SAP-02	MR

LA VISTA DEL VERTICE

Lo stesso dato, letto dalla direzione.



MTTR e velocità

Tempo medio di chiusura, nuovi vs risolti, aging: la postura come tendenza, non come fotografia.

Conformità su 8 framework

PCI-DSS 4.0, CIS v8, ISO 27001, NIS2, DORA, NIST CSF 2.0, GDPR e SOC 2 in un report firmabile.

PDF white-label schedulabile

Commentato dagli analisti Cyberfero ed esportabile con il logo del cliente.

Un solo repository, due letture: vista operativa per i tecnici, sintesi esecutiva per il vertice. Multi-tenant: ogni consociata nel proprio spazio, con la Fleet di gruppo a colpo d'occhio.

PIATTAFORMA & SICUREZZA

Enterprise-ready. E parte di una suite.

REMEDIA [ExpOps]

CICLO DI VITA OPERATIVO

Ingestione, normalizzazione, deduplica, prioritizzazione VBR, assegnazione owner, orchestrazione, tracking e reporting.

VulnApproval [Risk]

ACCETTAZIONE DEL RISCHIO

Quando una vulnerabilità non è sanabile nei tempi, REMEDIA inoltra la richiesta: workflow di approvazione fino alla firma del vertice.

Detection → Prioritizzazione → Remediation → Risk acceptance → Soppressione

LA PIATTAFORMA

Multi-tenant & Fleet

Gruppi, consociate e perimetro condiviso; vista Fleet su tutti i tenant.

SSO + MFA obbligatoria

Entra ID e Google, MFA TOTP per tutti, ruoli staff / cliente.

API REST pubblica

Endpoint completi, export, chiavi e OpenAPI per integrazioni.

Audit log granulare

Ogni azione tracciata: chi, cosa, quando — evidenza per audit.

PERCHÉ CYBERFERO

Un servizio gestito, non un'altra licenza.

Integra, non duplica

Si collega ai tuoi scanner via API e somma a quei dati pentest, cloud, AppSec, OT e segnalazioni manuali. Niente copertura di assessment pagata due volte.

Persone, non solo software

Analisti Cyberfero validano il Parsing AI, tarano la prioritizzazione e commentano un report mensile. Sotto perimetro ISO 27001, con SOC 24/7.

Costo prevedibile

Sviluppo una tantum + presidio ricorrente leggero: nessun costo nascosto di integrazione, nessun progetto da rifare a ogni nuova fonte.

SOLUZIONE	CATEGORIA	INGERISCE PENTEST	SERVIZIO GESTITO	PREZZO PER-ASSET
Nessus · Qualys	Scanner VA / VM	✗	✗	Sì
Vulcan · Brinqa · Nucleus	RemOps (prodotto)	✓	✗	Sì
REMEDIA · Cyberfero	ExpOps gestito	✓	✓	Sì

POSIZIONAMENTO DA FONTI PUBBLICHE DI BENCHMARK; NON COSTITUISCE QUOTAZIONE UFFICIALE DEI VENDOR CITATI.

PROSSIMI PASSI

REMEDIA [ExpOps]

Vediamolo in azione sui tuoi dati.

01

Demo dal vivo su remedia.cyberfero.com al CISO e al CIO.

02

Workshop di mezza giornata per validare requisiti e perimetro.

03

Avvio: un repository unico consultabile già dalla prima fase.

+39 0522 1685330

info@cyberfero.com

www.cyberfero.com

Via Statuto 3, Reggio Emilia