EXPOSURE & REMEDIATION MANAGEMENT

REMEDIA [ExpOps]

All your exposure. One command center.

Aggregate vulnerabilities and findings from 60+ sources — VM, AppSec, cloud, OT, pentests and manual reports — into a single normalized, deduplicated repository. Prioritized on real risk, auto-assigned, orchestrated to verified closure.

Aggregate. **Prioritize.** **Remediate.** **Prove.**

— THE PROBLEM

You don't need another scanner. You need a command center.

You already have the detection tools — often more than one per domain. What's missing is governing an output that arrives from dozens of sources in different, non-comparable formats.

Fragmented sources

Infrastructure scanners, AppSec, cloud, OT, pentests and manual reports: every tool speaks a different language.

No shared priority

CVSS alone doesn't tell you which flaws are actually exploited, nor how much the affected asset matters.

Untracked remediation

Who fixes what, within which SLA, with what verification? Closure can't be proven.

Compliance to prove

PCI, ISO 27001, NIS2 and DORA demand evidence of your posture. Rebuilding it by hand is fragile.

REMEDIA doesn't replace your tools: it integrates them. One platform, fed by every source.

HOW IT WORKS

From dozens of sources to one governed pipeline.

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

REMEDIA ingests any source, normalizes every finding onto a single schema — CVE, CVSS, asset, business unit, environment — enriches it with exploit intelligence and governs its lifecycle to verified closure.

Two flows, two costs

- ✓ **Structured sources** (API, CSV, XML, JSON, SARIF) → deterministic parsers, no AI cost.
- ✓ **Unstructured reports** (PDF, DOCX) → AI Parsing with analyst review.

THE NORMALIZATION PIPELINE

01
Ingestion
60+ connectors, report upload, manual entry

02
AI Parsing
Finding extraction from unstructured PDFs

03
Normalization
Single schema + NVD / KEV / EPSS enrichment

04
Deduplication
Cross-scanner duplicate merging

05
Prioritization
VBR 2.0: exploit, EPSS, CVSS, asset, exposure

06
Orchestration
Owners, campaigns, SLAs and tracking

First value in days: one unified repository, searchable from the start.

COVERAGE

60+ connectors. Your whole surface, in one place.

VM / Infrastructure

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

ⓘ Structured sources via API or file; pentests and unstructured reports via AI Parsing. New connectors added on request.

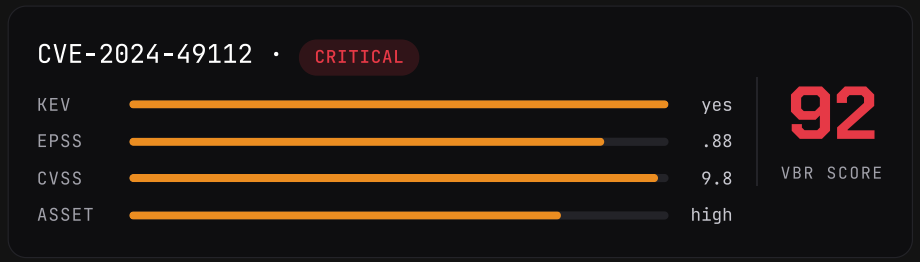
CAPABILITIES

The engine: prioritize and orchestrate remediation.

CORE

VBR 2.0 prioritization

Vulnerability-Based Risk: combines exploit maturity (CISA KEV, ransomware, Metasploit, Exploit-DB), EPSS probability, CVSS severity, asset criticality and internet exposure. Real urgency, not just the technical score.



Remediation orchestration

Themed campaigns, automatic rules and playbooks, patch management with push and verification to Ansible, Automox, BigFix and Intune.

Policy-driven SLAs + escalation

States and deadlines by severity and policy (KEV, exposed), automatic escalation to the contact, periodic digests to owners.

Cross-scanner deduplication

A single finding when multiple tools report the same CVE on the same asset: no duplicates, no noise.

Server Owner assignment

Hostname → owner from the CMDB or manual mapping, with a dedicated secure portal.

GOVERNANCE & INSIGHT

Measure your posture. Prove compliance.

Analytics & metrics

MTTR, velocity (new vs resolved), aging, SLA adherence, scorecards by Business Unit and Server Owner.

Multi-framework compliance

PCI-DSS 4.0, CIS v8, ISO 27001:2022, NIS2, DORA, NIST CSF 2.0, GDPR and SOC 2. Signable PDF report.

Risk graph & attack path

Relational view of the blast radius: where a single fix reduces risk most across the whole estate.

CAASM & EASM

Asset coverage gaps and exposed external surface (Shodan/Censys + crt.sh, DNS, InternetDB).

Executive report for leadership

Risk score, trends and priorities in an automatic report, commented by Cyberfero analysts, schedulable and exportable as a white-label PDF with the customer's logo — the same data source that feeds the engineers' operational view.

- MTTR & VELOCITY
- SLA ADHERENCE
- BU / OWNER SCORECARD
- 8-FRAMEWORK COMPLIANCE

— THE INTERFACE

For technical teams: one single work queue.

OPERATIONAL DASHBOARD · MULTI-TENANT

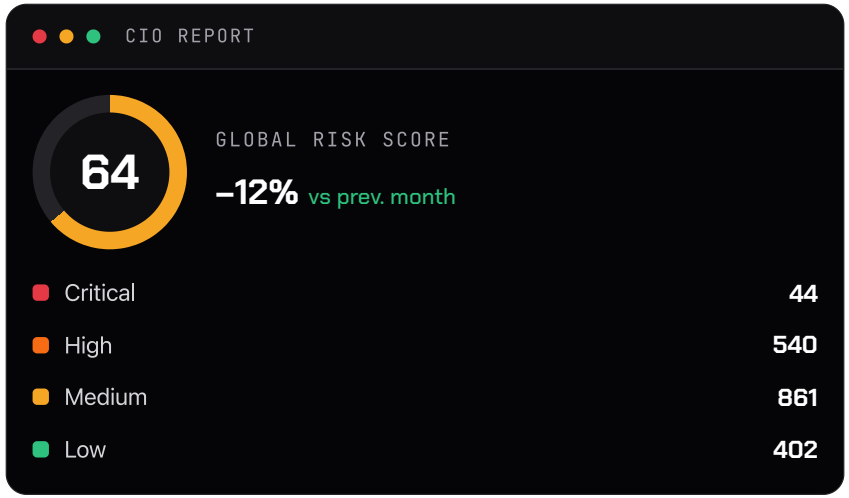
OPEN VULNS	CRITICAL	EXPLOITED KEV	SLA ADHERENCE
1,847	44	12	86%
▼ 312 (30d)	▲ 6	top priority	▲ +9%

VULNERABILITY REPOSITORY

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

THE LEADERSHIP VIEW

The same data, read by leadership.



MTTR and velocity

Mean time to close, new vs resolved, aging: posture as a trend, not a snapshot.

Compliance across 8 frameworks

PCI-DSS 4.0, CIS v8, ISO 27001, NIS2, DORA, NIST CSF 2.0, GDPR and SOC 2 in a signable report.

Schedulable white-label PDF

Commented by Cyberfero analysts and exportable with the customer's logo.

One repository, two readings: operational view for engineers, executive summary for leadership. Multi-tenant: every subsidiary in its own space, with the group Fleet at a glance.

PLATFORM & SECURITY

Enterprise-ready. And part of a suite.

REMEDIA [ExpOps]

OPERATIONAL LIFECYCLE

Ingestion, normalization, deduplication, VBR prioritization, owner assignment, orchestration, tracking and reporting.

VulnApproval [Risk]

RISK ACCEPTANCE

When a vulnerability can't be fixed in time, REMEDIA forwards the request: an approval workflow through to leadership sign-off.

Detection → Prioritization → Remediation → Risk acceptance → Suppression

THE PLATFORM

Multi-tenant & Fleet

Groups, subsidiaries and shared scope; Fleet view across all tenants.

SSO + mandatory MFA

Entra ID and Google, TOTP MFA for everyone, staff / customer roles.

Public REST API

Full endpoints, export, keys and OpenAPI for integrations.

Granular audit log

Every action tracked: who, what, when — evidence for audit.

WHY CYBERFERO

A managed service, not another license.

Integrates, doesn't duplicate

Connects to your scanners via API and adds pentests, cloud, AppSec, OT and manual findings on top. No assessment coverage paid for twice.

People, not just software

Cyberfero analysts validate AI Parsing, tune prioritization and comment a monthly report. Under ISO 27001 scope, with a 24/7 SOC.

Predictable cost

One-off build + a light recurring service: no hidden integration costs, no project to redo for every new source.

SOLUTION	CATEGORY	INGESTS PENTESTS	MANAGED SERVICE	PER-ASSET PRICING
Nessus · Qualys	VA / VM scanner	✗	✗	Yes
Vulcan · Brinqa · Nucleus	RemOps (product)	✓	✗	Yes
REMEDIA · Cyberfero	Managed ExpOps	✓	✓	Yes

POSITIONING FROM PUBLIC BENCHMARK SOURCES; NOT AN OFFICIAL QUOTE FROM THE CITED VENDORS.

NEXT STEPS

REMEDIA [ExpOps]

Let's see it run on your data.

01

Live demo on remedia.cyberfero.com to the CISO and CIO.

02

Half-day workshop to validate requirements and scope.

03

Kick-off: a unified repository to consult from the very first phase.

+39 0522 1685330

info@cyberfero.com

www.cyberfero.com

Via Statuto 3, Reggio Emilia