CYBERFERO

VULNERABILITY & EXPOSURE REMEDIATION MANAGEMENT

REMEDIA

All your exposure.
One single control room.

Aggregates vulnerabilities and findings from 130+ integrations (VM, AppSec, cloud, OT, EDR, CMDB, pentests), prioritises them on real risk and orchestrates remediation through to verified closure. Delivered as a managed service by Cyberfero.

Aggregate. Prioritise. Remediate. Prove.

CYBERFERO.COM · INFO@CYBERFERO.COM · +39 0522 1685330

THE PROBLEM

You don't need another scanner. You need a control room.

Detection tools are not in short supply: there is often more than one per domain. What is missing is a way to govern output coming from dozens of sources, in different formats and with incomparable priorities.

Fragmented sources

Infrastructure scanners, AppSec, cloud, OT, EDR, pentests and manual reports: each with its own console and language.

No shared priority

CVSS alone does not tell you what to fix first. Without context (real exploitation, exposure, criticality) teams work on noise.

Untracked remediation

Who fixes what, by when, with which patch? Between spreadsheets and emails the status gets lost.

Compliance to prove

NIS2, DORA, ISO 27001 and PCI require continuous evidence, not a yearly report.

REMEDIA does not replace your tools: **it integrates them** and becomes the single point for prioritisation, remediation and proof.

HOW IT WORKS

From dozens of sources to one governed pipeline.

Every finding goes through the same pipeline: normalised, deduplicated across tools, enriched with intelligence and context, assigned and tracked until closure is verified at the source.

01
Ingestion
130+ API integrations, on-prem push, CSV/XML/SARIF import, CIS/STIG benchmarks

02
AI Parsing
Unstructured PDF/DOCX pentest reports turned into findings

03
Normalisation
One schema, full descriptions, plugin output

04
Deduplication
Same CVE on the same host from several sources = one finding

05
Prioritisation
Client risk formula: CVSS, EPSS, KEV, VPR, context

06
Orchestration
Owners, campaigns, tickets, patches, SLAs and escalation

07
Verification
Closure confirmed by the source, retest, history and audit

First value within days: a **single, searchable repository** of your whole exposure.

COVERAGE

130+ integrations. Your whole surface, in one place.

VM / Infrastructure

Tenable · Qualys · Rapid7 · CrowdStrike Spotlight · ConnectSecure · Defender · Greenbone · Nuclei

AppSec — SAST/DAST/SCA

Snyk · Checkmarx · Veracode · GitHub Advanced Security · GitLab · Semgrep · SonarQube · Burp · Invicti

Cloud / CNAPP / Container

Wiz · Orca · Prisma Cloud · Defender for Cloud · AWS Inspector · Sysdig · Aqua · Trivy · Prowler

OT / ICS / IoT

Nozomi · Claroty · Armis · Tenable OT · Forescout

CMDB / CAASM / Identity

ServiceNow · BMC Helix · Device42 · Lansweeper · Axonius · Intune · Entra ID · Okta · Zoho One

EDR / XDR

CrowdStrike Falcon · SentinelOne · Microsoft Defender · Sophos · Elastic · Check Point

ITSM / Ticketing

ServiceNow · Jira · BMC Helix ITSM · Freshservice · Zendesk · Zoho Desk · PagerDuty · Opsgenie

Patch / Deploy

ConnectSecure · Automox · Intune · Ansible · BigFix · Qualys Patch · Check Point Harmony

Threat Intel / EASM / Pentest

CISA KEV · EPSS · MISP · Recorded Future · Mandiant · Shodan · Censys · HackerOne · Cobalt · Bugcrowd

Structured sources via API or on-prem push; unstructured reports (PDF, DOCX) via AI Parsing. New connectors released continuously.

PRIORITISATION

What to fix first, based on real risk.

Client risk formula

- Configurable weights for CVSS, EPSS, KEV, ransomware, exploit maturity, Tenable VPR, asset criticality and internet exposure
- Multipliers for the client's real environments (production, test, DR...)
- Client severity: VBR or VPR thresholds applied to critical, high, medium and low across the platform

Intelligence that anticipates

- Cyberfero Early Warning: advisories on products in use, even without a CVE
- Early exposure: hosts exposed to a new CVE before the scanner detects it
- Detection gaps: CVEs known to the scanner but not detected, with per-host diagnosis
- End of life (EOL) from the software inventory and Patch Tuesday with sector signal

Context that cuts the noise

- Risk graph and attack paths with chokepoints and crown jewels
- Control validation: verified EDR mitigations lower the priority
- Inferred owners for hosts without one, with confidence level
- Structured handling of false positives, exceptions and expiries

Not just CVSS: technical severity, likelihood of exploitation, business context and threat intelligence in one score.

REMEDIATION

From priority to closure, without manual hand-offs.

Remediation by action

Findings grouped by CVE, product, solution, owner, BU or asset: one patch closes hundreds of findings. You also see how many attack paths each action breaks.

Campaigns and playbooks

Rules that create dynamic campaigns (one per owner, BU or environment) with goals, deadlines, reminders and automatic attachment of new findings.

SLAs and escalation

Deadlines by severity, also in business days, automatic reminders and escalation; quiet hours for notifications.

Two-way ticketing

Single or bulk tickets on ServiceNow, Jira, BMC Helix, Zoho Desk and more; status flows back and the ticket closes when the finding is resolved.

Patching with impact analysis

Patches pushed to the patch management tool and verified at the next scan; first, an impact summary (production/test, domain controllers, reboots, reversibility).

Server Owner portal

Expiring personal link: owners see only their systems, install the update where allowed, report what they cannot fix and add their own photo.

Every step is tracked: who did what, when, with what outcome.

RISK ACCEPTANCE AND DATA QUALITY

Exceptions governed, not forgotten.

Risk acceptance

Maker-checker workflow with justification, expiry and estimated residual risk; acceptance pack generated automatically and, with VulnApproval, formal approval.

Suppression at the source

Decisions taken in REMEDIA are pushed back to VM systems that support it, so the same finding disappears elsewhere too.

Verified automatic closure

A finding no longer reported by the source closes by itself; for large volumes REMEDIA spot-checks the source before closing, with no manual approval.

Pentest retest

Upload the retest report and REMEDIA compares: what was fixed, what is still open, what is new.

Unscanned hosts

A host missing from a scan does not close its findings: it is flagged as «not reported», with the reason.

Silent and decommissioned assets

Assets that stop reporting, «decommissioned» states read from the CMDB and cascading closure of their findings.

The data you decide on is reliable: no phantom closures, no orphan findings.

GOVERNANCE AND COMPLIANCE

Measure your posture. Prove compliance.

Executive Summary

KPIs, trends and an AI-generated narrative ready for management and the board; scheduled white-label PDF reports.

Analytics and dashboards

MTTR, remediation velocity, aging, SLA compliance; personal and shareable dashboards with widgets built from any filter.

14 compliance frameworks

PCI DSS 4.0, ISO/IEC 27001 and 27002, NIS2, DORA, NIST CSF 2.0 and SP 800-53, CIS Controls v8, GDPR art. 32, SOC 2, HIPAA, Cyber Essentials, AI Act / ISO 42001, CIS/STIG hardening.

Evidence and attestations

Owner per control, exceptions with expiry, evidence pack and signable compliance report.

AI Exposure

Inventory of AI tools in use (shadow AI included) with owner, status, review and AI Act record.

Immutable audit log

Hash-chained record of every action, exportable to your SIEM, with configurable retention.

From the same data: the work queue for engineers, the numbers for leadership, the evidence for auditors.

AI IN REMEDIA

AI that works on your data.

Remediation assistant

Explains the vulnerability, proposes the fix plan and saves it in the finding.

Natural-language query

«Exploited criticals on exposed production servers»: the question becomes a filter, no query language needed.

AI routines

A goal in plain language, a cadence and limits: at each run REMEDIA proposes the actions and why.

AI pentest parsing

Unstructured reports turned into normalised, comparable findings.

Client's choice of AI engine

Anthropic, Azure OpenAI, AWS Bedrock, Google Vertex or any OpenAI-compatible endpoint: data stays where the client decides.

API and MCP server

Public REST API with scoped keys and an MCP server with OAuth 2.1 to connect corporate AI assistants.

AI speeds up analysis; risk decisions stay with people.

PLATFORM AND SECURITY

Enterprise-ready. And part of a suite.

Multi-tenant and Fleet

Groups and subsidiaries with a Fleet view, inherited settings and separate perimeters.

SSO and mandatory MFA

Microsoft Entra ID, Google, Okta and other OIDC providers; MFA for all users; IP restriction per tenant.

Roles and segregation

Staff, client administrators and viewers; each company sees only its own data.

Italian and English

UI, notifications, reports and manual in both languages.

Cyberfero suite

Integrates with Continuous VA, Penetration Testing, Early Warning & Advisory Monitoring and VulnApproval.

Continuous delivery

Frequent releases with release notes published in the platform.

Run by Cyberfero, an ISO 27001 certified MSSP with a 24/7 SOC.

COMPARISON

REMEDIA and the leading market platforms.

	REMEDIA	TENABLE ONE	QUALYS ETM	RAPID7 EXPOSURE COMMAND	NUCLEUS	BRINQA	ARMORCODE	SEEMPLICITY	ZAFRAN
Scanner-agnostic (no scanner to adopt)	✓	◐	◐	◐	✓	✓	✓	✓	✓
Declared connectors	130+	~50	n.d.	500+	200+	260+	350+	hundreds	n.d.
Cross-tool deduplication and normalisation	✓	✓	✓	✓	✓	✓	n.d.	✓	✓
Real-risk prioritisation (EPSS, KEV, context)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Two-way ticketing, campaigns and SLAs	✓	✓	n.d.	◐	✓	◐	n.d.	✓	✓
Integrated patch management (push and verify)	✓	◐	✓	◐	n.d.	◐	◐	◐	✓
Attack path / exposure graph	✓	✓	n.d.	✓	n.d.	◐	✓	n.d.	✓
Built-in AI (assistant, natural language)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Explicit NIS2 and DORA mapping	✓	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.
Managed service included (analysts + platform)	✓	SaaS	SaaS	◐	◐	SaaS	SaaS	SaaS	SaaS
Italian-language UI and support	✓	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.

Cisco Vulnerability Management (formerly Kenna) has been end-of-sale since 10/03/2026, with support until 30/06/2028 and no new connectors: REMEDIA is an alternative for those who need to migrate.

✓ documented · ◐ partial (e.g. separate module, separate service or vendor ecosystem only) · n.d. not stated in the public sources reviewed · SaaS = self-service platform, no managed service included

Sources: vendors' public documentation and web pages, October 2026. Connector counts are as declared by each vendor. «n.d.» does not mean the feature is missing. Trademarks belong to their owners; this comparison is not an offer from the vendors named.

WHY CYBERFERO

A managed service, not another licence.

Integrates, doesn't duplicate

Connects to the tools you already have and adds up their data: no scanner to replace, no assessment paid twice.

People, not just software

Cyberfero analysts tune prioritisation, validate AI Parsing, follow the campaigns and review progress with you.

Predictable cost

A clear service fee, no hidden integration costs and no project to redo for every new source.

130+
integrations

14
compliance frameworks

7
patch management tools

24/7
Cyberfero SOC

IT · EN
UI, reports and manual

Do I have to replace my scanners?

No: REMEDIA aggregates and governs them.

Do I need to install anything?

Not for cloud sources; an on-prem push agent is available for private networks.

How long does it take to start?

A few days for the first single, searchable repository.

NEXT STEPS



REMEDIA

Let's see it in action on your data.

01
Live demo
A session on a demo tenant with realistic data.

02
Proof of Concept
We connect your sources and show you your real exposure.

03
Service start
Connectors, owners, SLAs and reports set up with our team.

+39 0522 1685330 · info@cyberfero.com · www.cyberfero.com/remedia · Via Statuto 3, Reggio Emilia, Italy