PENTESTERRA

AUTOMATED SECURITY TESTING PLATFORM

External perimeter. Internal network. Cloud. Source code. One platform.

Your scanner found vulnerabilities. Do you know which ones can be exploited *right now*?

Most security tools hand you a list and walk away. They don't tell you what's actually reachable, what chains together into a real attack path, or what it means for your business. Pentesterra does all three — continuously, across every segment of your environment.

Four Security Disciplines. One Platform.

Security teams typically buy separate tools for each discipline. Pentesterra covers all four — and connects them into a single picture of your real risk.

Module	What it is	What most tools do	What Pentesterra does
VM	Vulnerability Management	List findings, assign CVSS score	Triage, prioritize, and track with verified status per finding
ASM	Attack Surface Management	Scan external perimeter only	Discover and monitor external AND internal assets continuously
BAS	Breach and Attack Simulation	Simulate attack scenarios in isolation	Build confirmed attack chains from real findings across all sources
ANPTT	Automated Network Penetration Testing	Schedule periodic scans	Continuously verify exploitability and generate PoC per finding

This is not another ASM or another VM. It is a platform where findings from all four disciplines connect into one graph of what an attacker could actually do to your organization **today**.

What Sets Pentesterra Apart

External and Internal. Every Segment.

Cloud-based security tools scan your public perimeter. They cannot reach what is inside.

Pentesterra deploys lightweight scanner nodes directly inside your network. No VPN. Black-box scanning. No agents on every host. Each node operates independently and reports back to the platform. Multiple nodes run in parallel: a large subnet scan that takes days on a single machine takes hours across a node cluster.

Covered: external perimeter, internal subnets, VLANs, cloud VPCs, contractor networks, air-gapped segments.

Automated Verification. Not “Found” but Proven.

Every finding goes through an automated verification pipeline before it reaches your team:

1. **Discovery** - vulnerability detected across all surfaces
2. **Enrichment** - matched against the knowledge base
3. **Verification** - safe targeted check runs against your actual environment
4. **PoC generation** - exact reproducing request, curl command, and step-by-step reproduction guide generated automatically
5. **Chain placement** - finding is placed in the attack graph, blast radius scored

Each finding carries a machine status that only moves forward:

Unconfirmed > Potential > Detected > Verified > Exploited

Security gets evidence. Engineering gets a reproducible PoC. No debate about whether the finding is real.

Triage Built in. Not a Spreadsheet.

Pentesterra does not produce a list of 300 items and leave prioritization to you.

The triage system evaluates every finding against three dimensions:

- **Attack chain position** - if this finding is the entry point of a confirmed chain, it is flagged first. **Fix the entry point and the entire chain collapses**.
- **Business impact score** - findings are scored against your actual application workflows. A checkout bypass scores as a financial fraud risk, not a generic “medium severity” item.
- **Compliance mapping** - each finding is automatically mapped to the controls it affects: SOC 2, ISO 27001, PCI DSS, GDPR, NIST. Ready for your next audit without manual work.

Analysts can mark findings as false positive, accepted risk, or mitigated. Each override requires approval and carries an optional expiry. The platform tracks the full disposition history.

Attack Chain Analysis. Three Sources, One Graph.

Pentesterra correlates findings from three data sources into a single deterministic attack graph. The graph contains 145 typed edges between vulnerability classes. A chain is a path through this graph where every node corresponds to a confirmed finding in your environment. No inference: if the nodes exist and the edges match, the chain is real.

Web Pentest Results

35+ active test modules including authenticated scanning of business workflows — payments, admin

Network Scan Results

Services, open ports, exposed admin interfaces, CVEs with active exploits — across internal subnets and cloud

DevGuard Code Signals

Secrets in source code and history, vulnerable dependencies, misconfigured containers, AI toolchain risks

One chain. One entry point to patch. One blast radius score. Compliance gaps mapped automatically.

Business Logic Detection. What Scanners Miss.

Standard automated scanners test HTTP requests. They do not understand what your application actually does.

Pentesterra performs authenticated scanning: it logs into your application with credentials you provide, walks real user flows, and maps where payments happen, where admin operations live, where user data is processed. Combined with code structure signals from DevGuard, it builds a map of your business processes.

Every vulnerability is then scored in context:

- IDOR on `/API/ORDERS/{ID}` - financial fraud risk inside your payment flow, PCI DSS scope
- Auth bypass on `/ADMIN/USERS` - privileged operations exposed, SOC 2 gap
- Checkout step skip - not a medium finding. A financial risk and an attack chain entry point.

This is the class of finding that skilled manual pentesters catch and automated scanners miss.

CVE Hunt. Advisory to Exposure Status in 15 minutes.

A critical CVE is published. In 15 minutes you know exactly which hosts in your environment are affected, including internal nodes that cloud tools cannot reach. Not at next week's scheduled scan.

334,538 CVEs indexed. Detection dispatched across your full asset scope automatically.

DevGuard. Security Before the Code Ships.

DevGuard is a lightweight IDE plugin for VS Code, Cursor, and Windsurf. It runs before every push and catches:

- Secrets and credentials in code and in full commit history (including SVN history, unique on the market)
- Vulnerable dependencies with CVE mapping
- Container and environment misconfigurations
- AI toolchain risks: MCP server configs, IDE plugin vulnerabilities, Copilot and Cursor rules that expose sensitive context

Findings from DevGuard feed directly into the attack chain engine. A leaked developer key in source code becomes a node in the attack graph alongside network and web findings.

Attack Brain Engine. Adaptive, not Scripted.

For complex findings, Pentesterra runs an AI-driven verification loop that behaves like an expert pentester: it reasons about what was found, decides the next action, executes it through a scanner node, observes the result, and adapts.

Unlike scripted verification pipelines where each step runs in isolation, the Brain Engine passes artifacts between steps. A session token extracted in step one is used in step two. A discovered admin panel changes the strategy for subsequent checks.

The full reasoning trace is visible in the UI as a real-time stream. No black box.

Safe to Run on Production. By Design.

Read-only and low-impact checks run automatically. Checks with any potential for disruption require explicit approval before execution. Destructive exploit classes are not in the toolset, not a configuration option.

You can run Pentesterra against live production systems without risk of downtime.

In Production

Two active government pilots across two countries. 12 months of operational use in regulated environments. Available commercially since March 2026.

Who uses it: Head of AppSec, DevSecOps Lead, CISO, CTO at B2B SaaS, Fintech, Healthtech, and Govtech companies with 50 to 500 employees.

Plans & Pricing

No additional licenses. No integration stack to buy.

Everything needed for verification, validation, and PoC generation is included. CI/CD triggers for GitLab, GitHub, and Jenkins are included. Webhooks for Jira, Linear, and Slack are included. Compliance exports for SOC 2, ISO 27001, PCI DSS, GDPR, and NIST are included. REST API for SIEM integration is included.

Small Team

€299/mo

- Web pentest — 35+ modules
- 10 network hosts
- 12 DevGuard projects
- Compliance exports
- CI/CD + webhooks

Team

€1,299/mo

- Web pentest — 35+ modules
- 100 network hosts
- Unlimited DevGuard projects
- Compliance exports
- CI/CD + webhooks

Enterprise

Custom

- Web pentest — 35+ modules
- Unlimited network hosts
- Unlimited DevGuard projects
- Compliance exports
- CI/CD + webhooks
- Unlimited scanner nodes Gray/whitebox scanning
- On-prem or single-tenant

Annual billing saves up to **24%**.

See it on Your Environment

The fastest way to evaluate Pentesterra is a live demo on your environment or a representative target. Exploit, chain, business impact. **Not a slide deck**.

📋 300-item pentest report?

No clear starting point — we show you exactly where to begin.

🚨 Critical CVE just dropped?

Know if you're exposed in 15 minutes, including internal nodes.

🔍 Customer due diligence?

Compliance exports ready. Attack chains documented. Evidence in hand.

🛡️ Three scanners, still unsure?

One graph. One entry point. One blast radius score. Real risk, finally visible.

Book a 45-minute demo on your environment

HTTPS://CALENDLY.COM/PENTESTERRA

OS@PENTESTERRA.COM | PENTESTERRA.COM

Book a Demo

Contact Sales

PENTESTERRA