PENTESTERRA

ENTERPRISE

Offensive Security at Enterprise Scale

Large hybrid infrastructures need more than a single scanner. Pentesterra distributes scanner nodes across your environment, correlates findings into cross-domain attack chains, and integrates with the SIEM, ticketing, and SSO systems you already run.

ENTERPRISE CAPABILITIES

Distributed Scanner Fleet

Deploy scanner nodes across data centers, cloud regions, and remote sites.

- → Nodes as Docker containers or VMs
- → Cloud + on-prem hybrid topologies
- → Per-node scope policies and RBAC

Multi-Domain Attack Chain Analysis

Combines findings from web pentests, network scans, AD enumeration, and DevGuard code scans.

- → Up to 20 attack paths per cycle
- → MITRE ATT&CK phase mapping
- → Cross-domain: code → app → network

Enterprise Integrations

Connects to the tooling enterprises already use - no new portals to manage.

- → SIEM export (CEF/JSON)
- → Jira and ServiceNow auto-ticketing
- → SSO via SAML 2.0 / OIDC
- → REST API for custom workflows

Compliance & Audit Evidence

Per-cycle evidence packages for SOC 2, ISO 27001, PCI-DSS, and NIST CSF.

- → Auditor-ready PDF + JSON exports
- → Continuous retesting after patches
- → Remediation tracking built-in

PENTESTERRA

ENTERPRISE

WHY ENTERPRISE SECURITY TEAMS CHOOSE PENTESTERRA

One risk view across every domain

Web, API, network, Active Directory, and source-code findings land in a single correlated model.

→ Instead of five disconnected tools and five report formats

Every finding is proven, not guessed

Pentesterra runs a real, non-destructive exploit against each finding before it reaches your team.

→ The backlog you triage is exploitable risk - not a CVSS list

It fits the estate you already run

Distributed scanner nodes cover data centers, cloud regions, and isolated segments.

→ Results flow into your SIEM, Jira or ServiceNow, and SSO - no new portal to learn

WHAT EVERY CYCLE DELIVERS

- ✓ Correlated findings with a stable machine status per issue - unconfirmed, verified, exploited - that never silently downgrades
- ✓ A per-finding proof-of-concept and reproduction steps for every verified vulnerability
- ✓ Delta report against the previous cycle: what is new, what was fixed, what regressed
- ✓ Cross-domain attack-chain graphs mapped to MITRE ATT&CK
- ✓ Auditor-ready evidence package (PDF + JSON) for SOC 2, ISO 27001, PCI-DSS, and NIST CSF
- ✓ Automatic re-test and ticket updates after remediation - no full rescan required

FAQ

Can Pentesterra run fully on-premise or in an air-gapped network?

Yes. The whole platform - console, API, workers, and scanner nodes - can run inside your environment with no outbound connectivity.

How does it integrate with our existing security stack?

Findings export to SIEM as CEF or JSON, open and update tickets in Jira and ServiceNow automatically, and the full REST API lets you drive scans and pull results from your own pipelines. Access is via SAML 2.0 or OIDC SSO.

Is automated exploit verification safe to run against production?

Verification is non-destructive by default: no data deletion, no denial-of-service payloads, and nothing that reads or exfiltrates confidential data. A human-in-the-loop mode can require analyst approval before any active exploitation step.

How often do cycles run, and how much does a large estate slow it down?

Cycles run on a schedule or an API trigger - weekly, nightly, or on every infrastructure change. Scanner nodes work in parallel, so coverage scales with the number of nodes you deploy.

Who runs it day to day?

Most enterprise teams run it self-service after onboarding. Pentesterra's team is available for scoping, escalations, and complex business-logic review, and MSSP partners can operate it on your behalf.

See it run across your estate

Distributed scanning, cross-domain attack chains, your existing tooling.

Request Enterprise Demo

info@pentesterra.com · pentesterra.com/solutions/enterprise