Lateralus Pentester: Product Overview

A professional penetration testing platform built on the Lateralus pipeline model

Lateralus Language

bad-antics · April 2026 · Lateralus / nullsec

ABSTRACT Lateralus Pentester is the commercial product tier of the nullsec platform. It extends the open-source nullsec toolkit with: a graphical engagement management interface, a collaborative pipeline editor for team-based testing, an automated evidence chain for compliance reporting, and integrations with leading ticketing and SIEM systems. This paper is a product overview targeted at security teams evaluating the platform.

1. Product Tiers

Lateralus Pentester is available in three tiers:

```
Community (free):   nullsec toolkit, CLI only, single user
Professional:       GUI + team features, 5 users, $299/mo
Enterprise:         Full platform, unlimited users, SSO, SLA
```

The Community tier is the open-source nullsec toolkit described in companion papers. This overview focuses on the Professional and Enterprise tiers.

2. Engagement Management

The engagement management module provides a dashboard for tracking active penetration testing engagements. Each engagement has: a scope definition, a timeline, assigned team members, and a findings log.

```
// Engagement record (simplified)
record Engagement {
    id:           EngagementId,
    client:       ClientInfo,
    scope:        EngagementScope,
    start_date:   Date,
    end_date:     Date,
    assigned_to:  Vec<TeamMember>,
    status:       EngagementStatus,
    findings:     Vec<Finding>,
}
```

The GUI presents a Kanban-style board for each engagement phase (reconnaissance, scanning, exploitation, reporting). Cards represent individual findings and can be assigned to team members, tagged with severity, and linked to evidence.

3. Collaborative Pipeline Editor

The pipeline editor is a visual IDE for composing nullsec pipelines. Team members can drag-and-drop stages from the tool library onto a canvas, connect them visually, and execute the pipeline from the GUI.

The editor validates pipeline connections in real time: connecting two incompatible stages (schema mismatch) is flagged with a red connector and a tooltip explaining the type error. This brings the Lateralus compile-time type checking to the visual layer.

4. Evidence Chain

Every finding in Lateralus Pentester has an attached evidence chain: a sequence of tool outputs, screenshots, and analyst notes that document how the finding was discovered and confirmed.

The evidence chain is automatically populated from the pipeline output (structured findings from the nullsec tool protocol) and can be extended with manual screenshots and annotations. At report generation, the evidence chain is embedded in the report as a reproducibility artifact.

5. Compliance Report Templates

The Professional and Enterprise tiers ship compliance report templates for common frameworks:

```
Templates included:
  - PCI DSS v4.0 penetration testing report
  - NIST SP 800-115 technical guide report
  - OWASP WSTG web application test report
  - SOC 2 Type II security review report
  - Custom template builder (Enterprise only)
```

Templates are populated automatically from typed finding data. Each template maps finding types to the relevant compliance sections and generates the required evidence format.

6. Integrations

Enterprise tier integrations:

- **SIEM**: Splunk, Elastic Security, Microsoft Sentinel — stream finding events in real time.
- **Ticketing**: Jira, Linear, GitHub Issues — automatically create tickets for each finding with severity, evidence, and remediation guidance.
- **SSO**: SAML 2.0 and OIDC for enterprise identity providers (Okta, Azure AD, Google Workspace).
- **REST API**: full API for custom integrations; all GUI operations are available via the API.

7. Deployment Options

Lateralus Pentester is available as:

- **Cloud SaaS**: hosted by the Lateralus team, data residency in US, EU, or AU regions.
- **Self-hosted Docker**: run on the customer's infrastructure with a Docker Compose file.
- **Air-gapped**: Enterprise tier only; offline deployment with no internet connectivity required.

The air-gapped deployment is intended for government and financial sector customers with strict network isolation requirements. Tool updates are delivered as signed OCI image archives.

8. Security of the Platform Itself

Lateralus Pentester handles sensitive engagement data including credentials, architecture diagrams, and vulnerability details. The platform security model:

- All data at rest encrypted with AES-256-GCM.
- All data in transit over TLS 1.3.
- Ed25519 signing of all exported reports.
- SOC 2 Type II audit report available to Enterprise customers.
- Bug bounty program at HackerOne (scope: *.lateraluspentester.dev).