Methodology & Tooling

Assessment Methodology

PrimeNexus assessments follow a structured, repeatable methodology designed to identify configuration weaknesses, assess risk impact, and align findings with recognized security frameworks.

1. Scope Definition
Identification of the operating system, configuration baseline, and applicable security frameworks.

2. Automated Baseline Assessment
System configurations are evaluated using industry-standard compliance tooling to identify deviations from recommended security baselines.

3. Control Validation & Analysis
Detected gaps are reviewed to determine severity, exploitability, and operational impact.

4. Framework Mapping
Technical findings are mapped across relevant compliance frameworks to maximize remediation efficiency.

5. Reporting & Review
Findings are summarized for executive stakeholders and detailed for technical teams, with clear remediation guidance.

Tools Used

- OpenSCAP – Industry-standard compliance scanning framework
- SCAP Security Guide (SSG) – Benchmark content for Oracle Linux 8
- Oracle Linux 8 Security Benchmarks – Platform-specific guidance

Framework Alignment

- CIS Oracle Linux 8 Benchmark
- DISA STIG for Oracle Linux 8
- NIST SP 800-53

Automation Disclaimer

Automated tooling is used to identify configuration gaps; however, all findings are reviewed and contextualized by security consultants to ensure accuracy, relevance, and risk-based prioritization.