RIMARI SENTINEL Technical Documentation

Version: 2.1.0 (Enterprise Edition)

Date of Issue: 3rd January, 2026

Document ID: KTS-Docs-2026-V2.1.0

1. Overview: The Sentinel Platform

RIMARI Sentinel is a sophisticated, high-performance security auditing platform engineered for modern cloud-native architecture. Built upon the globally distributed foundation of Cloudflare Edge technology, Sentinel offers unparalleled speed and accuracy. Its primary function is to perform comprehensive, non-destructive security audits specifically aligned with the OWASP Top 10:2021 standards.

1.1 Core Philosophy The platform is designed with a "security-by-default" and "non-destructive" philosophy. All probing techniques are passive and meticulously calibrated to avoid adverse impacts on the targeted application's performance or stability, making it safe for production environment scanning.

2. Core Engine Architecture: The Sentinel Scan Matrix

The power of RIMARI Sentinel lies in its unique, parallelized scanning engine, which dramatically reduces time-to-result while increasing the depth of the audit.

2.1 Parallel Probing and Hyperspeed Execution To achieve near real-time audit capabilities, the engine executes critical pre-scan reconnaissance and vulnerability checks concurrently:

- Header Analysis: Immediate inspection and correlation of HTTP headers to identify misconfigurations and outdated security policies (e.g., CSP, HSTS, X-Frame-Options).
- DNS Reconnaissance: Parallelized lookup via Cloudflare DNS-over-HTTPS (DoH) to map network infrastructure and host records.
- Path Traversal Checks: Concurrent testing of common directory and file access vectors to detect server-side vulnerabilities without sequential execution overhead.

2.2 Advanced Content Validation: Eliminating False Positives A major challenge for conventional scanners is the high incidence of false positives triggered by custom error pages or catch-all redirects. Sentinel overcomes this through intelligent content validation:

- Response Body Inspection: The scanner does not solely rely on HTTP status codes. It inspects the response body using an extensive library of RegEx signatures.
- Contextual Signature Matching: This process correlates expected vulnerability payloads (e.g., Git config markers like `[core]` or PHP info strings) with the actual response content to decisively confirm or eliminate findings.

2.3 Infrastructure Intelligence and Fingerprinting The platform integrates advanced fingerprinting logic to understand the target's underlying technology stack:

- **Technology Stack Identification: Accurately identifies platforms such as WordPress, Next.js, Cloudflare, and VTEX Commerce via advanced header and file inspection.**
- **Adaptive Profiling: Identifying the underlying technology allows the engine to highlight technology-specific risks, significantly increasing the relevance of the security audit.**

3. Interpreting Scan Results and Prioritization

Results are presented in an actionable, prioritized, and visually intuitive manner to guide security and development teams efficiently.

3.1 The Weighted Risk Score Every finding contributes to a calculated Risk Score, a numerical rating from 0 (Minimal Risk) to 10 (Critical Risk).

- **Calculation Basis: The score is a dynamic, weighted calculation based on severity (Critical vs. Low) and category alignment with the OWASP Top 10 standard.**

3.2 Visualizing the Attack Surface: The Radar Chart The Radar Chart provides a high-level visualization of the security posture across five primary domains:

- **Access Control: Risks related to broken authorization and exposed sensitive files.**
- **Injection: Coverage for potential Cross-Site Scripting (XSS) and injection risks.**
- **Authentication: Security of session management and authentication protocols.**
- **Security Configuration: Identifying missing security headers and misconfigured server responses.**
- **Monitoring & Logging: Assessing information disclosure and logging failures.**

3.3 Remediation Protocol and Actionable Intelligence Sentinel transforms findings into concrete, solvable tasks:

- **Specific Fixes: Each reported vulnerability includes a technically precise description of the necessary fix, such as implementing specific HSTS or CSP directives.**
- **Authoritative Documentation: Every finding provides a direct link to professional security documentation (e.g., OWASP Cheat Sheets) relevant to the specific vulnerability.**