SentinelX

PROFESSIONAL EDITION v6.5

Complete Technical Blueprint & Operational Manual

Integrated with PRIME_AI Assistant

A Sovereign Infrastructure Intelligence Platform

Generated for: Administrative Command

Table of Contents

1. Project Vision & Mission

SentinelX Professional is designed for organizations that demand total sovereignty over their data and infrastructure. In an era of cloud-dependency, SentinelX stands as a bastion of local intelligence.

Primary Objectives:

- Autonomous Stability: Identifying potential failures before they impact the bottom line.
- Zero-Trust Intelligence: Localized LLMs that never leak sensitive logs to external APIs.
- Verification at Scale: Real-time automated testing of complex network clusters.
- Visual Clarity: Turning raw JSON metrics into actionable 2D/3D topology maps.

Usage Scenarios:

- Finance: Monitoring transaction clusters for anomalous latency spikes.
- Healthcare: Securing patient record servers with local-first AI auditing.
- DevOps: Automating regression testing of infrastructure deployments.
- Security: Visualizing real-time pings on the Global Radar scanner.

2. Technical Architecture (A-Z)

The SentinelX platform utilizes a multi-layered Micro-Monolith architecture for maximum speed and minimal maintenance.

Frontend (The Interface)

Vanilla HTML5/JS/CSS3. We utilize GSAP for hardware-accelerated animations. No heavy frameworks like React are used to ensure sub-100ms load times.

Backend (The Orchestrator)

Node.js v20+ with Express. Handles the high-concurrency WebSocket streams via Socket.IO.

Database (The Memory)

Sequelize ORM abstraction allows for seamless switching between SQLite for edge deployments and PostgreSQL for enterprise clusters.

Neural Core (The Brain)

A dedicated Python 3.10 microservice running Flask. It utilizes PyTorch-based Transformers for log classification.

3. PRIME_AI Neural Core Logic

The heart of SentinelX is the PRIME_AI assistant. Unlike traditional regex-based alert systems, our neural core uses a hybrid approach:

Phase 1: Bayesian Classification - Fast-pass filtering of known attack signatures (0.01ms).
Phase 2: Local Transformer Analysis - If a log is anomalous, it is sent to the local LLM for root-cause context.
Phase 3: Fallback Intelligence - If the Python service is offline, a native Node.js Natural Language processor takes over.

This ensures that even during a partial system failure, PRIME_AI remains "awake" and able to triage critical security threats.

How to Invoke:

Users interact with PRIME_AI via the floating action button (FAB) or dedicated AI Lab. The bot accepts natural language queries like "Analyze last 50 logs" or "What is our current system health?".

4. Advanced Automation Lab

The Automation Lab is where human intervention is eliminated. It provides specialized tools for infrastructure validation.

- API Stress Tester: Simulates 10,000+ RPS to find the breaking point of load balancers.

- Vulnerability Scanner: Actively probes for SQLi, XSS, and open dev ports (e.g., 8080).

- DB Integrity Check: Audits referential integrity and WAL log health.

- UI Performance Audit: Measures Lighthouse metrics (LCP, CLS, FCP) in real-time.

Implementation:

The lab uses a specialized "Directives Repository" where users select a tool from a dropdown. Results are streamed in real-time to an on-screen terminal console with PASS/FAIL benchmarks.

5. Security Pulse & Threat Radar

Visual surveillance of the global threat landscape.

The Security Pulse view utilizes a specialized radar scanner animation. It tracks:

1. Regional Risk Vectors: High-risk pings from undetermined proxies.
2. PPS Rate: Packets Per Second monitoring to detect DDoS precursors.
3. Trust Scores: A dynamic percentage score of the overall ecosystem health.
4. Global Lockdown: A "one-click" Protocol-9 trigger that severs all external API connections in case of a breach.

Practical Application:

Used by security officers to monitor "Signature Anomalies". When a regional risk bar hits >80%, the system automatically flags the incident for PRIME_AI triage.

6. Network Topology

The Topology Map turns raw server lists into a living organism.

- Intelligent Routing: Visual lines connect the "CORE" to all active peripheral nodes.
- State Coloring: Green for nominal, Pulse-Red for critical failure.
- Dynamic Ingest: As new servers are added via the Client Agent, they automatically appear on the map without a refresh.
- Use-Case: Perfect for NOC (Network Operations Center) displays where immediate visual triage is required.

7. Audit Vault & Historical Compliance

Every event in SentinelX is stored in the Audit Vault.

The Vault is an immutable historical record. It is used for:

- Forensic Analysis: Rewinding to the exact second a breach occurred.
- Compliance Auditing: Exporting system state for ISO/SOC2 audits.
- Searchable Archive: Filtering 100k+ records by Node, Category, or Severity.
- Resolution Tracking: Showing exactly who or what (PRIME_AI) resolved the issue.

10. The v7.0 Horizon

The evolution of SentinelX Professional is just beginning.

Phase -> v7.0 Core

WebGL-powered 3D Topology with "Virtual Reality" inspection.

Phase -> Voice Module

"Project Jarvis" integration for voice-controlled server reboots.

Phase -> Distributed Core

Sharding the database across multiple continental clusters.

Phase -> Self-Healing

Autonomous script execution when AI confidence exceeds 98.5%.