MiniSentinel — Mini SIEM System Software Requirements Specification (SRS)

1. Introduction

1.1 Purpose

MiniSentinel is a log aggregation and threat detection platform that collects logs, detects suspicious activity using predefined rules, and alerts administrators. This document specifies the system requirements.

1.2 Scope

The system will collect logs from multiple sources, store and index them, apply detection rules, generate alerts, and provide a security dashboard for visualization and investigation.

2. Overall Description

MiniSentinel consists of a log ingestion API, storage layer, rule engine, alerting system, and a web dashboard. It is designed to simulate core SIEM functionalities in a simplified form.

3. Functional Requirements

3.1 Log Ingestion

FR-1: The system shall expose an endpoint POST /api/logs/ingest.
FR-2: The endpoint shall accept timestamp, source, level, ip, and message fields.

3.2 Log Storage and Indexing

FR-3: The system shall persist all logs.
FR-4: The system shall index logs by time and source for efficient search.

3.3 Detection Engine

FR-5: The system shall run a rule engine periodically.
FR-6: The system shall support rules for brute force detection, DDoS detection, and suspicious endpoint access.

3.4 Alert System

FR-7: The system shall create an alert when a rule condition is met.
FR-8: Each alert shall include type, severity, related logs, created_at, and status.

3.5 Dashboard and Search

FR-9: The user shall see logs timeline, active alerts, and top IPs.
FR-10: The user shall be able to filter and search logs by time, source, level, and IP.

4. Initial Detection Rules

Brute Force Rule: More than 5 failed logins from the same IP in 60 seconds.
DDoS Rule: More than 100 requests from the same IP in 10 seconds.
Suspicious Access Rule: Access to forbidden endpoints triggers an alert.

5. Non-Functional Requirements

NFR-1: The system shall ingest at least 10,000 logs per minute.
NFR-2: Search results shall be returned in under 1 second.
NFR-3: The system shall not lose logs on crash and shall ensure durability.

6. Data Models

Log(id, timestamp, source, level, ip, message)
Alert(id, type, severity, created_at, status)
Rule(id, name, condition)

7. System Architecture

The system consists of log producers sending data to an ingestion API, which stores data, feeds a rule engine, generates alerts, and serves a dashboard for visualization and investigation.