SenSIEM: Security Event and Intrusion Monitoring System

Project Overview

SenSIEM (Security Event and Intrusion Monitoring System) is a comprehensive log analysis and intrusion detection platform built using FastAPI (backend) and React (frontend). It allows security analysts to monitor, detect, and respond to suspicious events in real time.

The project supports universal log ingestion, log parsing, full-text search, rule-based alert generation, dynamic dashboards, and integration with alerting systems like email, Slack, and Telegram.

Core Features

1. **Log Ingestion and Parsing**:
   - Ingest logs from multiple sources (files, forwarded logs).
   - Automatically detect log type using pattern-based parsing.

2. **Log Search and Filtering**:
   - Splunk-like search with support for filters like log level, source, time range, and text content.
   - Alias keys mapped for flexible queries.

3. **Alerting System**:
   - Rule-based detection engine using brute-force, suspicious IPs, and threshold-based rules.
   - Alerts are stored in the database and displayed with metadata like severity, IP, source.

4. **Dashboards**:
   - Real-time dashboards for log-level counts, alerts, top IPs, error trends, and geo-location-based visualizations.

5. **Settings and Notification Management**:

- UI to manage log paths, enable/disable notifications.
- Backend configuration testing (API test).

6. **Detection Rules Engine**:
   - Rules stored in the database with interval settings.
   - Rules are auto-executed in background with buffer logic to avoid missing logs.
   - Detection rule types include brute-force, threshold, anomalies etc.

Architecture

- **Frontend**: React + TailwindCSS, Recharts, Lucide icons, stateful UI, toast messages.
- **Backend**: FastAPI with SQLite (or PostgreSQL) using raw SQL and DB connection pooling.
- **Alerting**: Notifications via Email, Slack, Telegram with enable/disable feature.
- **Detection Engine**: Runs active rules on an interval (default: 5 mins) with buffer logic.
- **Storage**: All logs and alerts are persisted and queryable via the dashboard.

Technologies Used

- **Frontend**: React, Tailwind CSS, ShadCN UI, Recharts
- **Backend**: FastAPI, SQLite3, SQLModel/Raw SQL, APScheduler
- **Other**: GitHub, JSON, Regex, Git, GitHub Actions (optional), PDF report via Python FPDF

Future Enhancements

- Add real-time alert streaming via WebSockets.
- Integration with machine learning for anomaly detection.

SenSIEM: Security Event and Intrusion Monitoring System

- Correlation engine between logs.
- Advanced threat intel enrichment (VirusTotal, AbuseIPDB).