Insider Threat Detection Dashboard - Project Documentation

1. Project Overview

The Insider Threat Detection Dashboard is a full-stack application designed to monitor and visualize potentially risky user behaviors within an organization. It serves as a security-focused monitoring tool, providing real-time detection and visualization of abnormal activities such as large file downloads or deletions.

2. Why This Project Is Important

Insider threats, whether intentional or accidental, are a growing concern for cybersecurity. Traditional tools often lack contextual behavioral data and real-time alerts. This dashboard brings modern technologies like FastAPI, D3.js, and real-time simulation to provide dynamic insights into user activity and detect threats more efficiently.

3. What Makes This Project Unique

- Real-time behavior log simulation with Kafka-style producer
- Live threat scoring using D3.js visualizations
- Risk alert component for suspicious behaviors
- Modern responsive UI using Tailwind CSS
- Full stack integration from frontend to backend to database

4. System Architecture & Workflow

1. Kafka simulator sends user logs to the FastAPI backend.
2. FastAPI stores logs in PostgreSQL.
3. React frontend fetches logs from backend.
4. Logs are displayed in a table with risk alerts.
5. D3.js visualizes user risk scores in a bar chart.

5. Technologies Used

- Frontend: React.js, Tailwind CSS, D3.js

- Backend: FastAPI (Python), SQLAlchemy ORM
- Database: PostgreSQL
- Log Simulation: Python script
- Tools: VS Code, Postman, Browser Dev Tools

6. How It Was Developed

1. Backend with FastAPI and SQLAlchemy for API and database interaction.
2. PostgreSQL for structured log storage.
3. Kafka-style Python simulator to generate logs.
4. React frontend using Tailwind CSS and D3.js for charts.
5. Real-time alerts implemented via polling in useEffect.

7. Key Features

- Admin Login system
- Live behavior log display
- Risk alerts for suspicious activity
- Interactive D3.js risk chart
- Clean, modular component structure

8. Final Notes

This project demonstrates how full-stack technologies can create intelligent security monitoring dashboards. It combines frontend interactivity with backend intelligence and real-time simulation.