Insider Threat Detection Dashboard - Project Documentation

Project Overview

Goal: Build a real-time dashboard to monitor and visualize risky user behaviors (e.g., unauthorized deletions or large file downloads) that may indicate insider threats.

This system simulates logs, identifies risky actions based on rules, displays alerts, and visualizes user risk scores.

Idea & Objectives

Primary Objectives:

- Simulate user behavior logs using a Kafka-style Python script.
- Build a backend API using FastAPI to receive and store logs.
- Use PostgreSQL as the database to store all behavioral logs.
- Create a React-based dashboard:
  - Display real-time logs.
  - Highlight risky behaviors (delete actions or file size > 750KB).
  - Visualize risk scores using D3.js bar charts.
  - Provide admin login functionality.

Tech Stack

Frontend: React + Tailwind CSS + D3.js

Backend: FastAPI

Database: PostgreSQL

Log Simulator: Python

Deployment: Localhost

Insider Threat Detection Dashboard - Project Documentation

Functional Modules

1. Kafka Simulator (producer.py)

- Sends a log every 3 seconds with delete action and large file size.

2. Backend API (main.py)

- FastAPI-based API to receive and store logs.

- SQLAlchemy models define the DB schema.

- CORS support for frontend access.

3. Frontend Dashboard (App.js)

- Admin login interface (admin / admin123).

- Displays logs, risk alerts, and D3.js charts.

4. RiskAlert Component (RiskAlert.js)

- Displays visual alerts for risky user behaviors.

5. RiskChart (RiskChart.js)

- Displays risk scores with color-coded bars based on score.

How to Run the Project

1. Start PostgreSQL and ensure 'insider_db' exists.

2. Start backend: uvicorn backend.main:app --reload

3. Start frontend: cd frontend && npm start

4. Run Kafka simulator: python kafka-simulator/producer.py

Login: admin / admin123

Insider Threat Detection Dashboard - Project Documentation

Risk Scoring Logic

+1 for normal actions

+3 for delete action

D3 visual color:

- Green: Safe (<5)

- Yellow: Medium Risk (5-9)

- Red: High Risk (10+)

Future Enhancements

- Real user authentication

- ML-based anomaly detection

- Alert notifications (email/SMS)

- Docker/Kubernetes deployment

- Admin panel with RBAC