Idea for Codezen Hackathon

Project Title: Real-Time AI Security Log Analyzer & Threat Explainer

> “An AI system that watches live logs and instantly detects and explains security threats.”

1. Why This Idea Is Perfect for the Team

This project provides the best balance of Pathway alignment, feasibility within 36 hours, skill compatibility, and strong judge appeal.

Skill Match Overview:

- Python – Required heavily and already known by the team
- React – Used for dashboard and live updates
- LLM (Gemini) – One team member is sufficient
- Streaming concepts – Learnable within a few hours

This project does not require advanced machine learning or model training.

Pathway is designed for streaming data, event-driven AI, and live decision-making, making this project a perfect fit.

2. Project Overview

Problem:

Security teams often analyze logs only after an attack has occurred, which is too late.

Solution:

- Reads live authentication, API, and server logs
- Detects suspicious patterns instantly
- Uses AI to explain what is happening
- Displays alerts on a live dashboard

3. Hackathon-Friendly Feature Set

Core Features (Must Have):

- Live log streaming (simulated)
- Rule-based anomaly detection
- Detection of multiple failed logins
- Detection of a single IP hitting many endpoints
- AI-generated threat explanation
- Live dashboard

Optional Bonus Features:

- Threat severity score (Low / Medium / High)
- Suggested mitigation actions

- Export alerts as JSON

4. System Architecture

- Simulated Log Generator
- Pathway for real-time stream processing
- Threat detection logic in Python
- Gemini LLM for explanation
- React dashboard with live updates

Simulated logs are completely acceptable in hackathons.

5. Required Skills

- Python: stream reading, conditional logic, JSON handling
- Pathway: streaming ingestion and real-time transformations
- Gemini / LLM: prompt design and API usage
- React: dashboard UI and live updates

6. Team Role Breakdown

- Member 1: Pathway and backend setup, log streaming, anomaly detection
- Member 2: Gemini integration and AI explanation logic
- Member 3: React frontend and dashboard UI
- Member 4: Integration, deployment, and demo preparation

7. 36-Hour Execution Plan

- Hours 0–4: Planning, feature finalization, role assignment
- Hours 4–14: Backend development and Pathway setup
- Hours 14–22: AI integration and frontend development
- Hours 22–30: System integration and bug fixing
- Hours 30–36: UI polish and demo preparation

8. Sample Demo Script

> “We are simulating live server logs. Normal traffic is flowing. Now we trigger multiple failed login attempts from a single IP. Pathway instantly detects the anomaly, and our AI explains it as a brute-force attack, along with recommended actions.”

9. Backup Idea

Real-Time AI Customer Support Alert System: monitors live chats, detects frustrated users, and suggests responses. This option is safer but has slightly less technical impact.