PurpleKit App Summary

What it is

PurpleKit is a lightweight purple team operations platform for planning, executing, and tracking security testing engagements.

Who it is for

Purple team operators and red/blue team leads coordinating joint security exercises.

What it does

- Engagement management with scope, objectives, and timelines.
- MITRE ATT&CK technique mapping with tactic categorization.
- Detection outcome tracking (Logged, Alerted, Prevented, Not Logged).
- Kanban workflow for technique status and progress.
- Guided planning wizard with templates and technique picker.
- Security control attribution for detections (EDR, SIEM, NDR, etc.).
- Export engagement data to JSON, CSV, and ATT&CK Navigator.

How it works

- React frontend (port 3000) provides the UI, served by Node.js in production.
- Node.js + Express backend exposes API endpoints used by the frontend.
- PostgreSQL stores engagements, techniques, comments, and related data.
- MITRE ATT&CK data is sourced via TAXII 2.1 with caching.

How to run

- Prereq: Docker and Docker Compose.
- Copy env template: cp .env.example .env
- Start services: docker-compose up --build
- Open http://localhost:3000 in your browser.