Aegis-AI Team Playbook (Mentoring Round)

Simple explanations • demo flow • USPs • RunAnywhere SDK • common Q&A

1. What Aegis-AI is (in simple language)

Aegis-AI is an offline-first verification tool that detects whether an incoming voice note/video/image is authentic or AI-generated. It is designed for high-stakes environments where internet may be unavailable and decisions must be made in seconds.

- Problem: deepfake commands and misinformation can cause real-world damage.
- Solution: scan media locally, return a verdict + confidence + human-readable explanation.
- Why now: voice cloning and synthetic media are cheap, fast, and widespread.

2. What we have built for the mentoring round

- UI Prototype: a complete product workflow (Audio/Video/Image), dashboards, history, reports, result views.
- Localhost Demo: an upload-to-report experience that generates a forensic-style report in seconds (offline on localhost).
- Both are designed to prove feasibility + product thinking + execution ability in a short time.

3. Core USPs (what makes us hard to reject)

- Offline-first: works without internet (critical for defense/field operations).
- Real-time: target is < 2 seconds per verification.
- Explainable: we show what signals contributed to the decision.
- Privacy-first: media stays on-device; only model updates/telemetry are optional.
- Forensics-ready: chain-of-custody and report generation concept.

4. RunAnywhere SDK (how it fits)

RunAnywhere SDK is planned as the deployment layer to run optimized inference on-device across platforms. It helps with packaging, runtime efficiency, and consistent execution on edge hardware.

- Why we need it: reliable edge inference (Android/iOS/edge devices) with performance constraints.
- How we use it: ship quantized models + inference runtime as part of the app; execute locally.
- Expected impact: lower latency, lower battery usage, predictable performance offline.

5. Mentoring-round questions (and strong answers)

Use these as short, confident answers. Keep answers to 20–40 seconds unless asked deeper.

- Q: How do you prove it works offline? A: We run inference on-device/localhost, no network dependency; we can disable Wi■Fi and still generate the report.
- Q: What about false positives? A: We show confidence + multiple signals. For high-risk decisions, the system recommends secondary verification.

- Q: What data do you store? A: By default, none; optional secure logs for chain-of-custody can store hashes and metadata.
- Q: What is your moat? A: Offline edge-first + forensics workflow + deployment practicality for defense/field.
- Q: Who pays? A: Government/enterprise per-device licensing + subscription for reporting/management.

6. Pitch flow (3 minutes)

- Hook (20s): demonstrate the risk (fake command scenario).
- Solution (40s): Aegis-AI does instant offline verification + report.
- Demo (60s): upload audio2/audio4 (fake) then audio1/audio3 (real).
- USPs (40s): offline, real-time, explainable, privacy-first.
- Business (20s): defense/enterprise licensing + pilots.