Aegis-R — Pilot Readiness Plan

Purpose: align product direction, staffing roles, and pilot timeline with a clear, credible plan.

1) Product Vision (Layman Terms)

- Aegis-R checks whether a security alert is actually possible in your environment, not just “likely.”
- It explains its reasoning in plain language, so people can trust the decision.
- It tracks an attack across time instead of treating alerts as isolated events.
- It highlights missing evidence so teams know exactly what data to collect next.
- Humans stay in control: nothing is blocked automatically, and approvals are auditable.
- The system gets smarter about what to ask for using optional, advisory learning — without changing verdicts.

2) Team Roles (Minimum Viable Team)

Role	Core Responsibilities	Must-have Skills
Platform & SaaS Integration Engineer	Package and deploy Aegis-R (hosted SaaS). Build de[illegible]	Linux, Docker, cloud (AWS/GCP/Azure), Go[illegible]
Product UI Engineer (Security UX)	Build analyst UI (reasoning, queue, audit, governance). [illegible]	React, TypeScript, Tailwind, D3/visx, B2B/SOC [illegible]
Customer Enablement / Solutions Engineer	Onboard pilots, configure ingestion, support tuning, do[illegible]	Technical support + CLI/JSON + SIEM/EDR [illegible]

3) Ownership & Division of Work

- Shakeeb: engine optimization, reasoning quality, performance and testing.
- Raunaq: business, sales, partnerships, pilots, fundraising, and investor communication.

4) Engine Optimization Focus (Near-Term)

- Improve “impossible vs incomplete” edge cases using real pilot data.
- Expand vendor adapters with deeper field mapping for key event types.
- Increase coverage across identity, cloud, and endpoint techniques.
- Keep outputs deterministic and audit-friendly; ML assist stays advisory only.

5) Pilot Readiness Timeline (8 weeks)

Week	Milestones
1–2	Finalize hosted deployment, CI/CD, and baseline onboarding docs.
3–4	Pilot integration: 1–2 data sources (Okta/CloudTrail/EDR).

5–6	Run pilot; collect feedback and tune rules/telemetry.
7–8	Publish pilot report (metrics, false positives reduced, workflow impact).

6) Pilot Success Metrics (Examples)

- Reduce false positives in chosen alert stream by 30–50%.
- Cut Tier■1 triage time by 25–40%.
- Audit-ready explanation generated for every decision.
- Analyst satisfaction: “clearer decisions and less noise.”

7) Immediate Next Steps

- Finalize hosted demo packaging and onboarding checklist.
- Prepare pilot outreach materials and short demo script.
- Identify 1–2 design partners and start data access discussions.

Document prepared for planning and investor/pilot discussions.