**Seraphim Feature & Build Request for Nikita Clark**

**Objective**

This document outlines a staged feature request and deliverables roadmap to guide the pricing, estimation, and timeline for the Seraphim Proof of Concept (POC), MVP 1, MVP 2, and future build-out.

The scope below is drawn from the standardized Vanguard architecture and cross-sector use cases discussed in our prior documentation.

Initial beta deployments will focus on the energy and oil & gas sectors, so compliance features should align with relevant industry standards and operational needs.

**Immediate Priority:** We need one more high-quality demo video using the current POC visuals. This will be used for investor presentations to secure final funding. Please prioritize this delivery before we expand into MVP stages.

**⚙️ STAGED BUILD PLAN**

**PHASE 1: POC Build**

**Goal:** Demonstrate functional logic and visual governance of agent workflows using the Vanguard framework.

**Features:**

* Low-fidelity UI (as currently shown)
* Agent Launch Panel (initiate goal/task)
* Agent Activity Log (step-by-step task chain)
* Basic Governance Panel with Vanguard overlays:
  + Security Vanguard (flag/block unsafe actions)
  + Integrity Vanguard (input validation alert)
  + Accuracy Vanguard (traceable output logging)
* 1–2 Mock Integrations (e.g., file ingestion + API call)
* Visual flags for human-in-the-loop (approve/deny)

**Deliverables:**

* Figma + Frontend dev files
* Basic working dashboard (Streamlit or Retool OK)
* Mock backend logic for agent flow simulation

**PHASE 2: MVP 1**

**Goal:** Implement interactive, semi-functional agent orchestration with live integration hooks.

**Features:**

* Medium-fidelity UI w/ animations, gradients, and smooth transitions
* Secure agent runtime container (Dockerized logic)
* Configurable Vanguard rule sets (on UI)
* Policy Engine UI (toggle rule types, thresholds)
* Logging Layer (simple OpenTelemetry or LangSmith integration)
* API connector module (drag & drop or JSON configuration)
* Dashboard Filtering (by Vanguard trigger, task type, time)

**Deliverables:**

* Modular UI code (React/Next.js preferred)
* Functional frontend-to-mock-agent backend (FastAPI or Node.js)
* Log viewer + download/export logs (JSON, CSV)

**PHASE 3: MVP 2**

**Goal:** Launch full-featured design and system interoperability.

**Features:**

* High-fidelity production UI (mobile responsive, animated state flow)
* Admin panel: define agent roles, policies, and sandbox permissions
* Full Vanguard AI Governance:
  + Security Vanguard w/ API Gateway logic
  + Integrity Vanguard w/ document validation
  + Accuracy Vanguard with RAG or fallback options
* Live integration w/ 2–3 APIs (OpenAPI spec)
* Data ingestion + output validation modules
* Full-agent traceability map (step-wise + source links)

**Deliverables:**

* React + containerized backend ready for enterprise deployment
* Admin dashboard panel + security config JSON schema
* All mock integrations replaced with real APIs (or firm spec stubs)

**FUTURE PHASE: Seraphim Platform (Full Stack AI Governance)**

**Goal:** Develop enterprise-grade Seraphim Platform w/ studio builder, marketplace, and zero-trust runtime.

**Long-Term Features:**

* Drag-and-drop agent builder studio (Streamlit or custom UI)
* Enterprise role-based access management (RBAC)
* Plugin store / Marketplace for templates and tools
* Air-gapped agent execution
* Full audit trail export module (JSON, PDF, SIEM integration)
* Configurable compliance schema focused initially on energy and oil & gas sector requirements (e.g., NERC CIP, ISO 27019)

**Next Steps**

1. Review this document and confirm phases are scoping-aligned.
2. Provide feedback on prioritization or feasibility.
3. Return with proposed:
   * Cost estimate per phase (or hourly)
   * Any technical constraints or assumptions