## **AI Platform – Phase 1 / Day 1 Must-Have Capabilities**

1. **Core MLOps Foundation**
   * Model registry, versioning, and experiment tracking
   * CI/CD pipelines for training and deployment (GitOps/ArgoCD/Terraform)
   * Automated packaging, promotion, and rollback
   * Support for both ML and LLM endpoints
2. **Data Management & Feature Store (DataOps Base)**
   * Secure data ingestion and validation
   * Central data catalog and lineage tracking
   * Initial feature store or dataset registry for reusability
   * Schema validation and basic data quality monitoring
3. **Observability & Monitoring Setup**
   * Logging (Loki / Cloud Logging), metrics (Prometheus / Cloud Monitoring), tracing (OpenTelemetry)
   * Model performance dashboards (latency, drift, accuracy)
   * Basic alerting and incident notifications
4. **Security & Access Control**
   * SSO / IAM integration (Okta / Azure AD / Cloud IAM)
   * Encryption at rest and in transit (KMS / CMEK)
   * Role-based access control (RBAC) for data, models, and pipelines
   * Secrets management (Vault / Secret Manager)
5. **Governance & Compliance Foundations**
   * Model and dataset documentation (model cards, metadata)
   * Approval workflow for production model deployment
   * Audit logging and evidence capture for SOC2/PCI readiness
   * PII/PHI handling guidelines and DLP integration
6. **Initial FinOps & Resource Optimization**
   * Budget monitoring and alerts
   * VM/GPU auto-parking or idle resource shutdown
   * Cost dashboards (per model / per project)
   * Tagging and labeling for chargeback and visibility
7. **Developer & Data Scientist Enablement**
   * Secure notebook environments (Vertex AI Workbench / SageMaker Studio / JupyterHub)
   * Standardized SDKs and CLI for experimentation and deployment
   * Internal documentation hub and reusable code templates
8. **LLM Enablement (Controlled Start)**
   * Prompt templates and basic evaluation setup
   * Integration with one provider (e.g., Bedrock or Vertex AI)
   * Guardrails for safety, content filtering, and prompt logging
   * Embedding store and simple RAG prototype
9. **Infrastructure Automation & Deployment Backbone**
   * Terraform for IaC and standardized environments
   * Kubernetes/EKS/GKE setup for scalable workloads
   * Secure networking (VPC, Private Service Connect, Service Mesh if needed)
   * CI/CD integration with Vault-based secrets
10. **Roadmap & Platform Operating Model Definition**

* Define roles: Platform Ops, Data Ops, ML Ops, FinOps, SecOps
* Establish review cadence (Estimation Council / Governance Board)
* Create Phase 2 & 3 backlog (LLMOps maturity, Agentic AI, Multi-tenancy)
* Document KPIs: reuse %, ROI, model SLA compliance