MLOps Engineer Interview Challenge

Background

A healthcare technology company has developed several machine learning models to predict patient outcomes, medication adherence, and readmission risk. These models were developed by data scientists and currently exist as research code with inconsistent approaches to deployment. The company wants to standardize their ML infrastructure to enable reliable deployment, monitoring, governance, and continuous improvement of these models in a heavily regulated healthcare environment.

The challenge is to design and implement a robust MLOps platform that can support the entire ML lifecycle while ensuring compliance with healthcare regulations, model explainability requirements, and the need for consistent model performance across diverse patient populations.

Objective

Design and implement an end-to-end MLOps platform that enables the company to reliably deploy, monitor, and update machine learning models in production. Your solution should emphasize reproducibility, compliance, monitoring, and operational excellence throughout the ML lifecycle.

Dataset Overview

- **Models**: Three Python-based ML models (patient readmission risk, medication adherence, complications prediction)
- **Data Sources**: Simulated patient data schemas (no actual PHI) showing expected input formats
- **Model Artifacts**: Model code, training notebooks, and basic documentation from data scientists
- **Compliance Requirements**: Summary of regulatory requirements (HIPAA, FDA) for model deployment
- **Infrastructure**: Details of current cloud environment (Azure) and on-premises systems

Scope of Work

1. MLOps Infrastructure Design

- Design an architecture for model training, evaluation, deployment, and monitoring
- Implement CI/CD pipelines for ML workflows
- Create infrastructure-as-code for reproducible environments
- Address security and compliance requirements specific to healthcare

2. Model Packaging & Deployment

- Standardize model packaging across different model types

- Implement container-based deployment strategies

- Design versioning and artifact management systems

- Create rollback and canary deployment capabilities

3. Monitoring & Observability

- Implement comprehensive model monitoring (performance, drift, outliers)

- Design alerting systems for model degradation

- Create dashboards for model performance visibility

- Implement audit logging for regulatory compliance

4. Governance & Documentation

- Design model registry with approval workflows

- Implement automated documentation generation

- Create model cards with standardized information

- Design explainability interfaces for clinical users

5. Automation & Operational Excellence

- Implement automated retraining workflows

- Design feature store capabilities for consistent feature engineering

- Create A/B testing infrastructure for model updates

- Implement data and model lineage tracking

Technical Requirements

- Infrastructure-as-code using Terraform, Pulumi, or equivalent

- Containerization with Docker and orchestration with Kubernetes

- CI/CD implementation with appropriate tooling (GitHub Actions, Azure DevOps, etc.)

- Monitoring implementation with appropriate visualization (Prometheus, Grafana, etc.)

- Security and compliance considerations throughout the implementation

Evaluation Criteria

Your solution will be evaluated based on:

- Architecture design and infrastructure implementation

- Security and compliance considerations

- Monitoring and observability implementation

- Automation and operational excellence

- Code quality, documentation, and reproducibility

Discussion Questions

- How would your system ensure model reproducibility across environments?
- What strategies would you implement for detecting and addressing model drift?
- How does your solution handle model explainability requirements for healthcare?
- What are the trade-offs between model performance and operational complexity?
- How would you manage the transition from research code to production systems?

Deliverables

- Complete code repository with infrastructure-as-code and deployment pipelines
- Architecture diagrams and technical documentation
- MLOps platform implementation for the provided models
- Monitoring and governance implementation
- Brief presentation outlining your approach and key decisions

Final Notes

This challenge evaluates your ability to design and implement MLOps systems that address the unique challenges of deploying machine learning models in regulated industries. Focus on creating a solution that not only works technically but also addresses the governance, security, and compliance requirements specific to healthcare applications.