Securing AI-Driven Financial Operations : RAG & Agentic Systems at Scale

Conf

By: **Swamy Biru**

The Security Imperative

The Challenge

Our Approach

Three-Layer Security Architecture

RAG Knowledge Retrieval

Agentic Orchestration

LLM Processing Pipeline

RAG Security: Multi-Layered Protection

01

Identity Verification

02

Query Sanitization

03

Access Control

04

Audit Logging

05

Secure Transmission

Agent Orchestration: Consensus & Zero-Trust

Specialized Agents

- Trade validation
- Compliance checking
- Risk assessment
- Client communication
- Exception handling
- Operational monitoring

Each agent operates within a strictly defined scope, following the principle of least privilege.

Consensus Mechanism: High-stakes decisions require agreement across multiple specialized agents. A trade execution agent might propose an action, but compliance, risk, and operations agents must independently verify before execution proceeds.

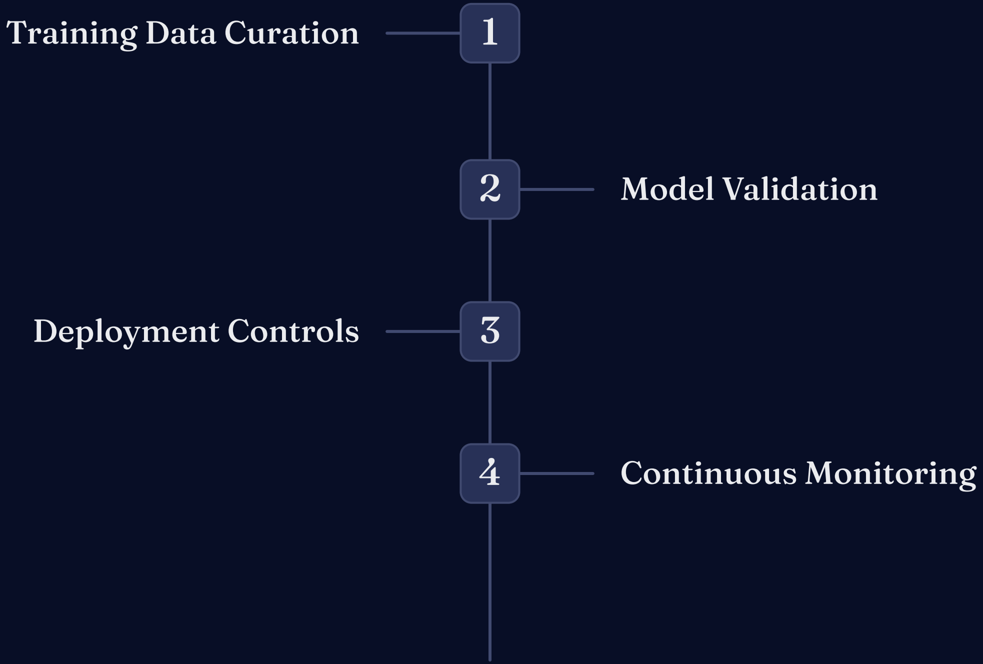
DevSecOps: Integrating Security Seamlessly

Proactive Automated Security Testing

Secure Infrastructure as Code (IaC)

Embracing "Shift-Left" Security

AI Model Security: From Training to Deployment



1 Training Data Curation

2 Model Validation

3 Deployment Controls

4 Continuous Monitoring

Real-Time Threat Detection

AI Securing AI at Millisecond Speed

1M+

Security Events Daily

Processed with sub-millisecond response times

99.8%

Detection Accuracy

High-fidelity alerts with minimal false positives

<1ms

Response Time

Sub-millisecond detection latency for most threats

Multi-Model Detection Approach

Statistical Models

Deep Learning

Graph Neural Networks

Reinforcement Learning

Tiered Alert System

Low Severity

Medium Severity

High Severity

Compliance & Governance Framework

Regulatory Landscape

Explainability Strategy

Performance at Scale

Security Without Sacrifice

System Availability

RAG Query Time

Daily Transactions

Transaction Latency

Key Lessons Learned

Security From Inception

Human Oversight Remains Critical

Cultural Transformation

Adaptive Defense

Future Directions

Emerging Technologies

Federated Learning:

Homomorphic Encryption:

Quantum Computing:

Industry Standards:

Regulatory Evolution

Building the Future of Secure AI

Start with Security

Continuous Process

Invest in Culture

Responsible Innovation

Thank You