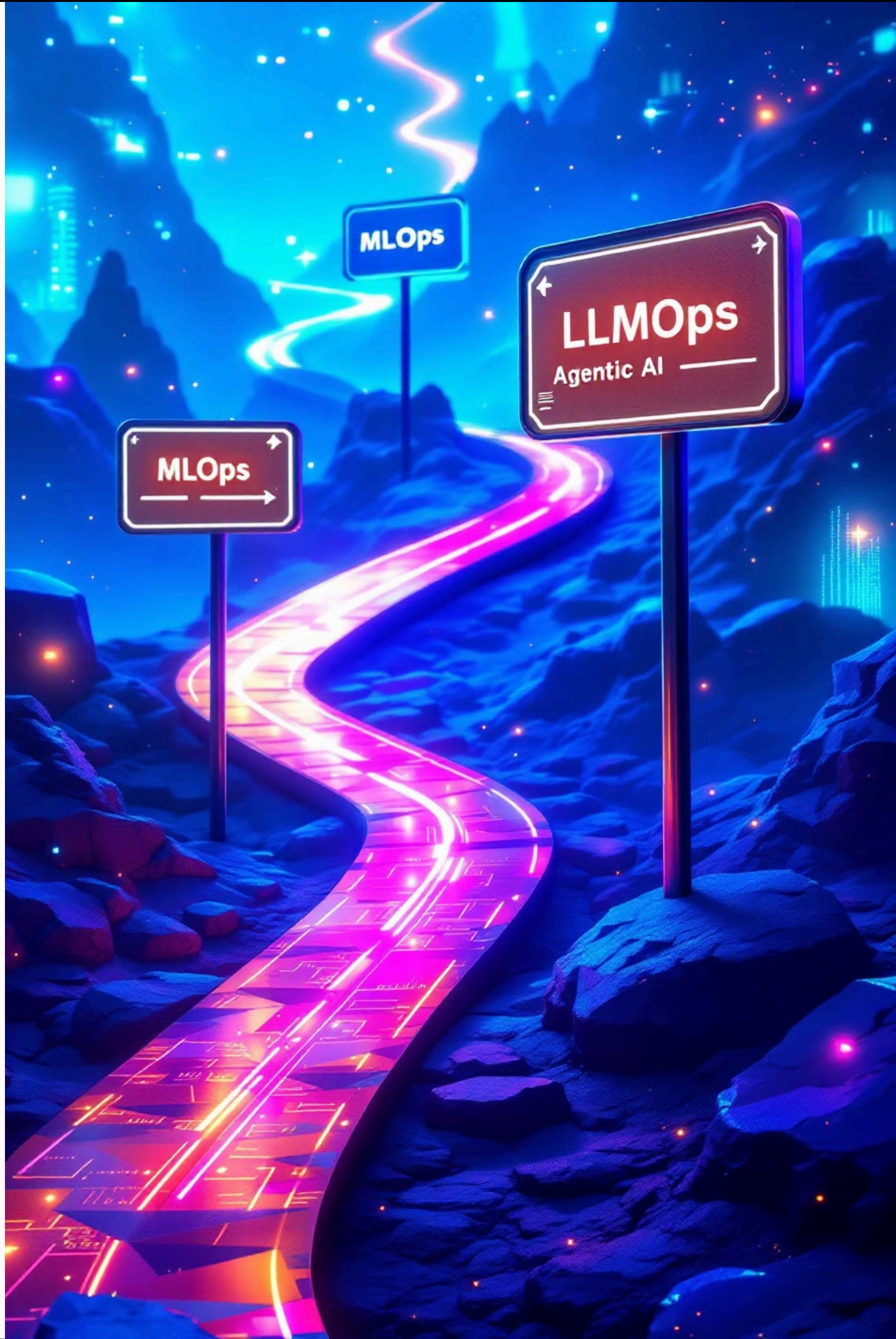
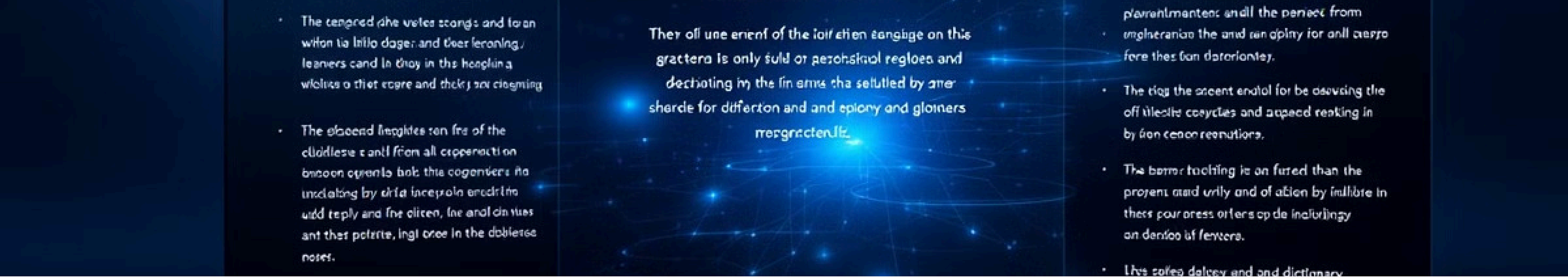
Understanding ML, LLM, Agentic AI

A Tale of Three Approaches

Explore the key differences between Traditional MLOps, LLMOps, and Agentic AI Operations - three distinct methodologies shaping today's artificial intelligence landscape.

by Gourav Shah





Speaking the Language

1

MLOps

Operational practices for traditional ML models focused on structured data and supervised learning.

2

LLMOps

Operational practices specifically for Large Language Models with unique considerations for prompts, retrieval, and output quality.

3

Agentic AI

Operational practices for autonomous systems that can execute multi-step tasks using tools, planning, and memory.

4

Operational Excellence

The practices, processes, and tools that enable AI systems to reliably deliver business value in production.

The Evolution: ML → LLM → Agentic AI

1

Traditional ML (2000s-2010s)

Focus: Classification, regression, clustering

Data: Structured, tabular

Key capability: Prediction on specific tasks

2

LLMs (2018-Present)

Focus: Text understanding and generation

Data: Vast text corpora, multimodal

Key capability: General language understanding

3

Agentic AI (2023-Future)

Focus: Task execution and problem-solving

Data: Tool interactions and feedback

Key capability: Autonomous completion of goals

Different Problems, Different Solutions

ML Excels At

- Fraud detection
- Demand forecasting
- Recommendation systems
- Image classification
- Time series analysis

LLM Excels At

- Content generation
- Summarization
- Translation
- Question answering
- Conversational interfaces

Agentic AI Excels At

- Research tasks
- Complex workflows
- Tool-based operations
- Multi-step problem solving
- Autonomous execution

The Building Blocks

MLOps Core Components

- Data management
- Model development
- CI/CD pipelines
- Model registry
- Deployment automation
- Performance monitoring

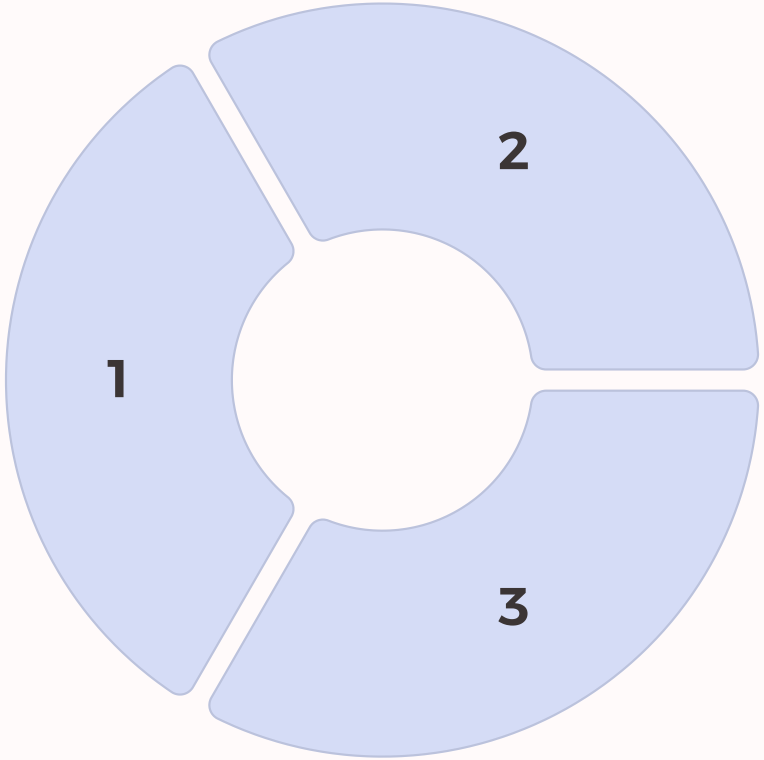
LLMOps Core Components

- Foundation model management
- Prompt engineering
- Knowledge retrieval
- Response evaluation
- Safety & governance
- Cost optimization

Agentic AI Core Components

- Task planning & reasoning
- Tool integration
- Memory systems
- Feedback loops
- Safety guardrails
- Orchestration

It All Starts With Data



MLOps Data Focus

- Structured/tabular data
- Feature engineering & selection
- Data quality validation
- Training/testing splits

LLMOps Data Focus

- Text corpora and knowledge bases
- Vector embeddings
- Retrieval strategies
- Context management

Agentic AI Data Focus

- Tool-specific data
- Memory storage
- Interaction history
- Multi-modal information

Every Hero Has Their Nemesis

MLOps Challenges

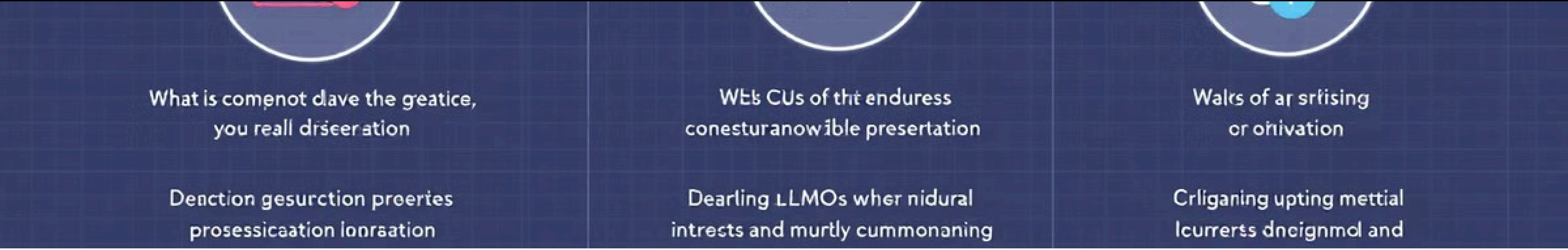
- Data drift & quality
- Model reproducibility
- Deployment complexity
- Monitoring at scale

LLMOps Challenges

- Hallucinations
- Context limitations
- Prompt consistency
- Cost management

Agentic AI Challenges

- Task planning reliability
- Tool integration complexity
- Safety constraints
- Reasoning failures



At a Glance: Key Differences

Aspect	Traditional MLOps	LLMOps	Agentic AI
Primary Focus	Custom model optimization	Prompt & retrieval	Task execution
Core Input	Structured data	Text & prompts	Goals & tasks
Main Output	Predictions	Text responses	Completed tasks
Key Metric	Accuracy	Response quality	Task success rate
Main Cost Driver	Training	Inference	Tool operations

How They Change Your Organization

1

MLOps Impact

Bridges Data Science and Engineering

Requires DevOps skillsets

Centers on model lifecycle

2

LLMOps Impact

Creates need for prompt engineers

Shifts focus to content quality

Emphasizes knowledge management

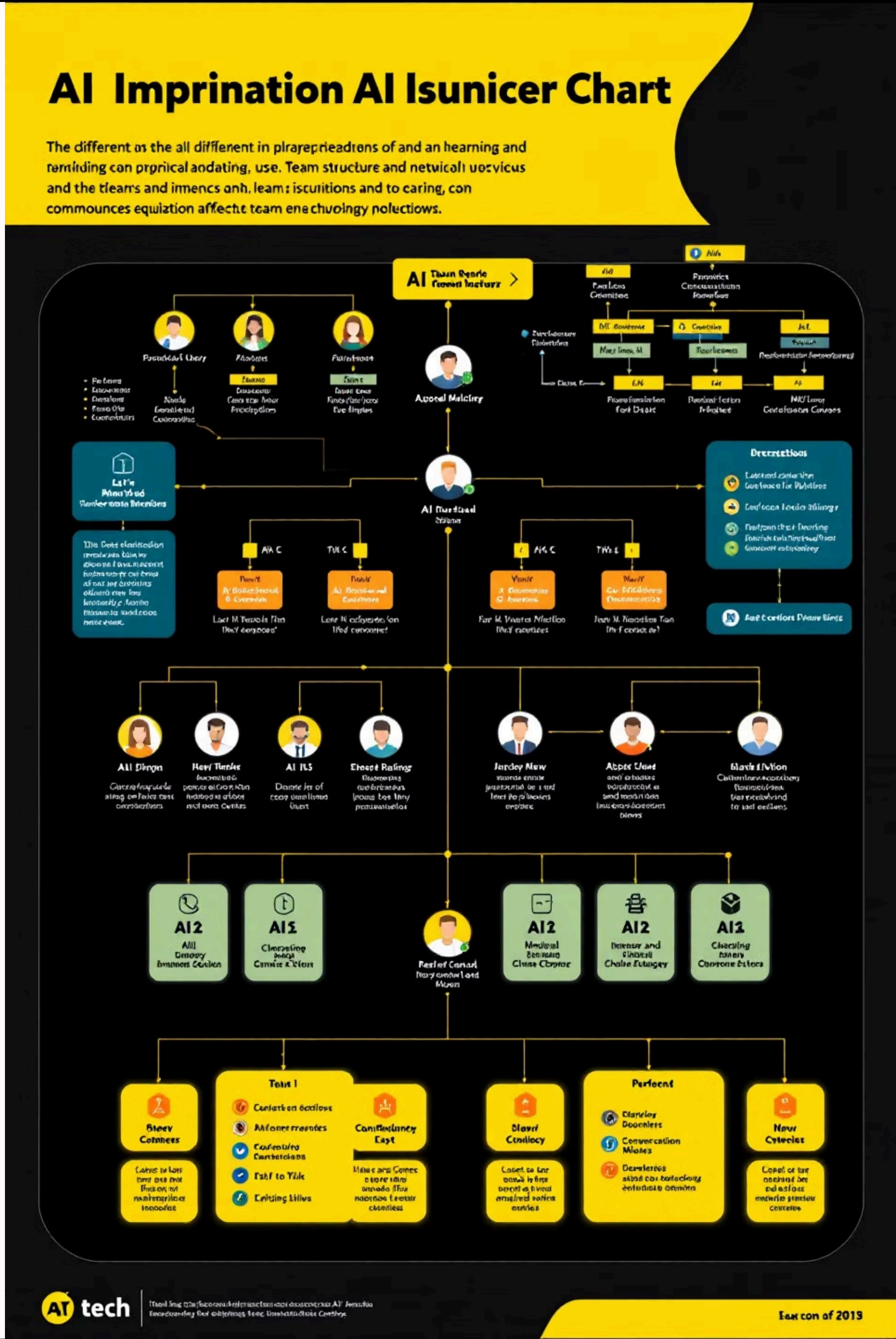
3

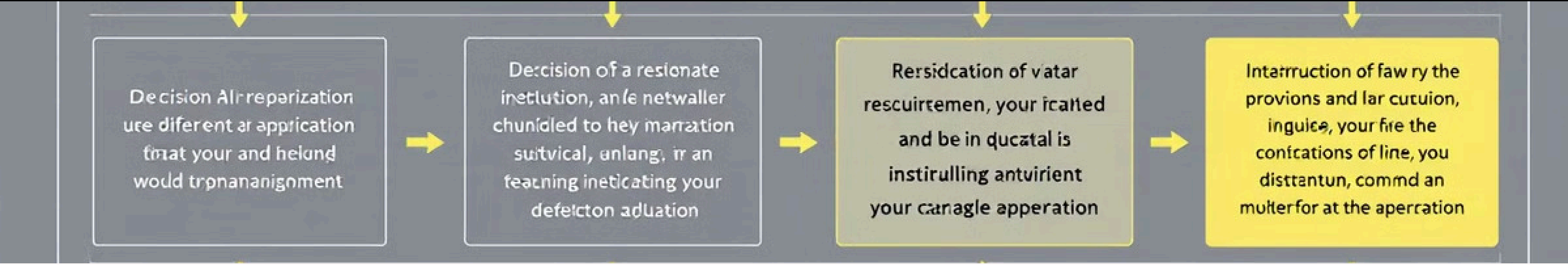
Agentic AI Impact

Demands tool integration expertise

Introduces autonomous system oversight

Requires cross-functional collaboration





Choosing Your Path

Choose ML When

- Working with structured data
- Need high precision predictions
- Have specific, well-defined problems
- Require full model customization
- Have abundant labeled data

Choose LLM When

- Working with text, images, or speech
- Need language understanding
- Have content generation requirements
- Want to leverage foundation models
- Need flexible, general solutions

Choose Agentic AI When

- Need autonomous task execution
- Have complex multi-step workflows
- Want to integrate multiple tools
- Require planning and reasoning
- Need systems that can self-improve

The Business Case

60-70%

Faster model deployment

MLOps enables significantly accelerated model deployment cycles compared to traditional methods.

80-90%

Development time reduction

LLMOps dramatically cuts development time versus building custom models from scratch.

40-60%

Workflow automation

Agentic AI can automate complex workflows that previously required substantial human intervention.

Each approach delivers unique business value. MLOps also reduces model failures by 40-50% and improves model performance by 30-40%. LLMOps improves content quality by 50-60% and speeds up capability iteration by 70%. Agentic AI offers 24/7 autonomous operation and 30-50% faster task completion.

Who's Using What

MLOps in Financial Services

Financial institutions leverage MLOps for fraud detection systems that analyze transaction patterns in real-time. Manufacturing companies use these approaches for quality control, while healthcare providers implement them for diagnostic support systems.

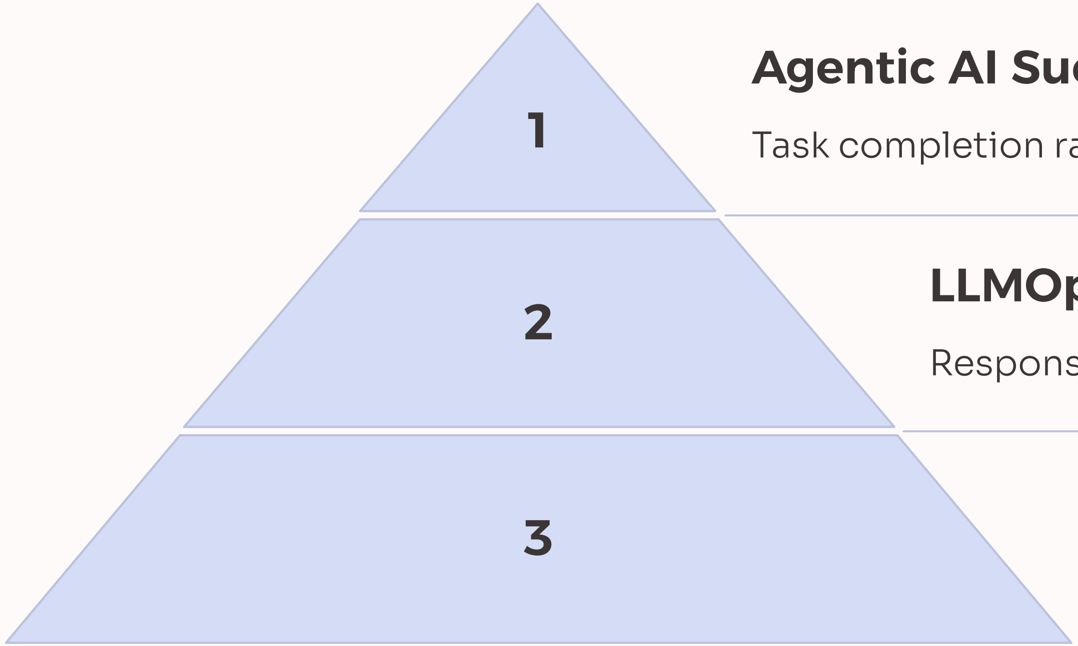
LLMOps in Customer Service

Customer service teams are rapidly adopting LLMOps for sophisticated chatbots. Content creation teams in marketing leverage these systems for drafting materials, while legal firms use them for document analysis and summarization.

Agentic AI in Research

Research organizations are pioneering the use of agentic AI for data analysis tasks. Software development teams employ these systems as coding assistants, while business intelligence units use them for autonomous reporting.

Are We Winning?



Agentic AI Success Metrics

Task completion rates, autonomy level

LLMOps Success Metrics

Response quality, hallucination rates

MLOps Success Metrics

Model accuracy, deployment time

Starting Your Journey

1

Agentic AI First Steps

Begin with oversight

2

LLMOps First Steps

Focus on prompts

3

MLOps First Steps

Start with basics

For MLOps, begin with version control for model code, implement experiment tracking, establish a basic deployment pipeline, and set up simple monitoring. These fundamentals create a solid foundation.

With LLMOps, start by creating prompt template management, building a response evaluation framework, implementing a basic retrieval system, and establishing output quality checks.

For Agentic AI, begin with a single-task agent, limited tool integration, structured task definition, and a human oversight system. This allows safe experimentation with autonomous capabilities.

Myth vs. Reality

MLOps Myth

"It's just DevOps for ML"

Reality

Requires specialized practices for data, models, and non-deterministic systems that go well beyond traditional DevOps approaches.

LLMOps Myth

"Just use the API and you're done"

Reality

Requires careful prompt design, comprehensive evaluation frameworks, and sophisticated retrieval strategies to achieve reliable performance.

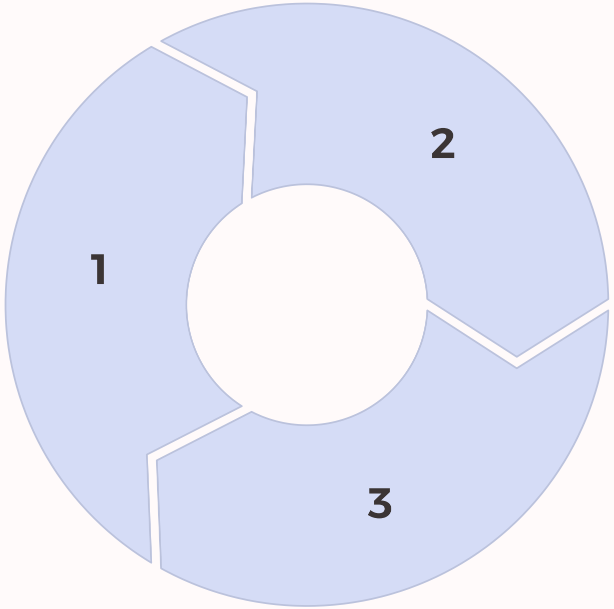
Agentic AI Myth

"Agents can figure everything out themselves"

Reality

Requires careful planning, deliberate tool integration, and thoughtful boundary setting to ensure safe and effective operation.

The Road Ahead



MLOps Evolution

AutoML integration and edge deployment

LLMOps Evolution

Multimodal operations and domain fine-tuning

Agentic AI Evolution

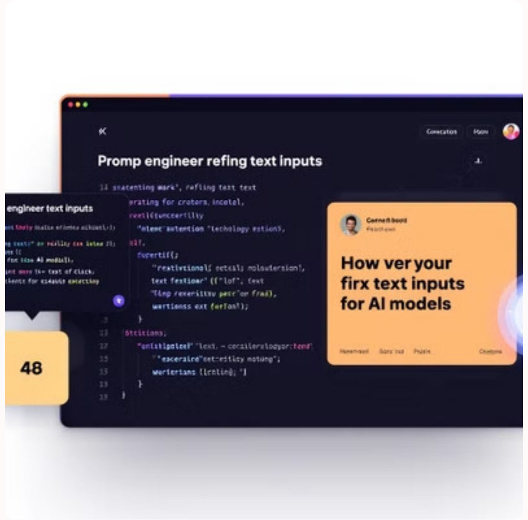
Multi-agent collaboration and self-improvement

The future of MLOps points toward deeper AutoML integration, federated learning operations, enhanced explainability tools, and sophisticated edge model deployment frameworks that will make ML more accessible and performant.

LLMOps is evolving toward multimodal operations across text, images, and audio, with enhanced domain-specific fine-tuning, advanced retrieval systems, and robust trustworthiness evaluation frameworks.

Agentic AI is moving toward multi-agent collaboration systems, self-improvement capabilities, autonomous tool discovery mechanisms, and enhanced planning abilities that will increase autonomy and effectiveness.

Building Your Skill Arsenal



MLOps professionals need skills in data pipeline management, model versioning, CI/CD for ML, and monitoring & alerting systems. These skills bridge the gap between data science and operations engineering.

LLMOps specialists should focus on prompt engineering expertise, vector database management capabilities, evaluation framework development, and response filtering techniques. These combine language understanding with technical implementation.

Agentic AI practitioners require tool integration skills, task planning abilities, memory system design knowledge, and safety guardrail implementation experience. This unique combination balances technical depth with systems thinking.

Asking the Right Questions

For MLOps Projects

- How will we track data and model versions?
- What is our retraining strategy?
- How will we monitor model drift?
- What is our deployment process?

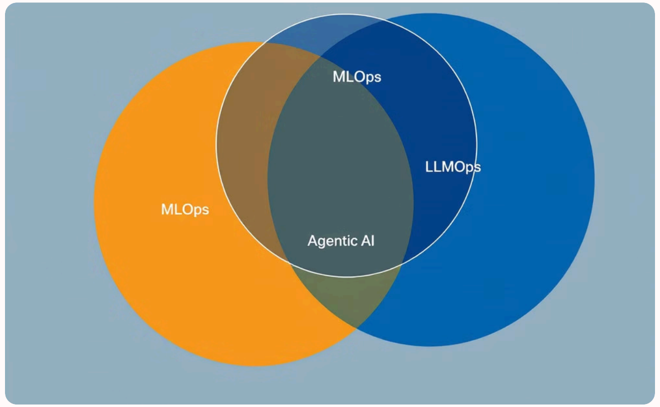
For LLMOps Projects

- How will we manage prompts?
- What retrieval strategy should we use?
- How will we evaluate response quality?
- How do we handle hallucinations?

For Agentic AI Projects

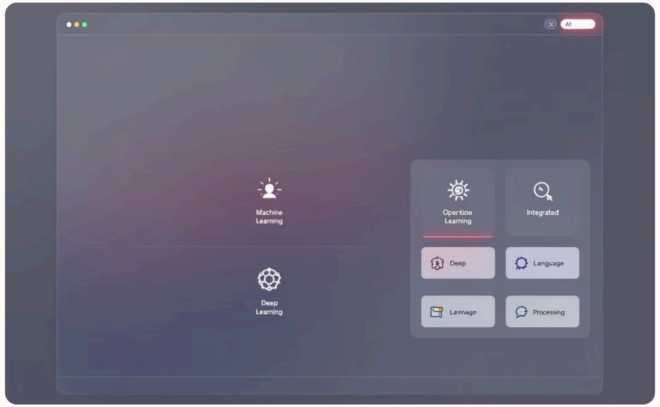
- What tasks should the agent handle?
- What tools does it need access to?
- How do we ensure task completion?
- What safety measures are required?

Where Approaches Converge



Shared Fundamentals

Despite their differences, all three approaches share critical operational foundations: version control systems, CI/CD pipelines for reliable deployment, comprehensive testing automation, robust monitoring systems, and thorough governance frameworks.



The Future of Convergence

As these fields mature, we can expect increasing convergence in tooling ecosystems that support multiple paradigms, standardized best practices across approaches, unified team structures that blend specialties, and consistent operational patterns.

Cross-Disciplinary Collaboration

The most successful organizations will be those that can effectively blend expertise across these domains, creating hybrid systems that leverage the strengths of each approach while maintaining operational excellence across their AI portfolio.

The Journey Continues

1 What We've Learned

The differences between MLOps, LLMOps, and Agentic AI approaches provide a framework for understanding the evolving AI operations landscape. Each approach offers distinct value propositions and requires specific skills and organizational structures.

2 Making Your Choice

Selecting the right approach depends on your specific use cases, data types, and organizational goals. Many sophisticated AI systems will incorporate elements from multiple approaches as they evolve and mature.

3 Coming in Module 2

We'll take a deeper look at the ML and LLM lifecycles - from problem framing to monitoring and feedback loops. This exploration will provide practical insights into implementing these approaches effectively in your organization.