Faysal Aziz

Mastering Prompts & Agents

Design and deploy powerful AI workflows: prompt engineering, tool integration (MCP), and the age of autonomous agents - 2 days

FA-0317 · 2 days

Agentic & Generative AI

Introduction

AI that just spits out text? That's yesterday's news. Today's AI thinks, plans, and executes—connecting systems, making decisions, and handling complex workflows without human intervention.

Over two intensive days, you'll master the art of getting AI to do exactly what you want. We'll push ChatGPT, Gemini, Perplexity, and Claude to their limits, figure out when free tools beat premium ones, and build intelligent agents that actually solve real problems using MCP frameworks.

This isn't a classroom exercise. Drawing from three decades of solving actual business challenges, every technique you'll learn has been battle-tested in production environments. You'll walk away with skills that work—not just concepts that sound impressive.

Ready to build AI that gets things done? Let's make it happen.

Learning outcomes

By the end, participants will be able to:

- Understand AI types and their evolution through ML, DL, LLMs, and agents
- Craft effective prompts and compare their efficacy across tools and pricing tiers
- Integrate models with external services via MCP
- Design, deploy, and troubleshoot agentic AI workflows using Manus, ChatGPT Deep Research, and Operator
- Evaluate trade-offs between autonomy, cost, security, and compliance

---

Prerequisites

- Basic understanding of AI/ML and neural networks
- Comfort with prompt-based interactions
- Laptop with internet access and ability to install plugins or APIs

---

Training outline

1. 1. Foundations of AI & Learning Engines

- **Types of AI**: Reactive systems, limited-memory, theory-of-mind, self-aware; narrow vs general AI
- **Machine Learning**: Supervised, unsupervised, reinforcement learning
- **Deep Learning Basics**: Neural networks, architectures (CNN, RNN, Transformers), backpropagation
- **From ML to LLMs and Agents**: How DL powers language models and forms the basis for agentic behavior

2. 2. Introduction to LLMs & Prompt Engineering

- **Core Concepts**: Transformer architecture, token prediction, context windows
- **Prompt Design Variants**: Zero-shot, few-shot, chain-of-thought, structured prompting

  Live Demos & Tool Comparisons

  - Tools: ChatGPT, Gemini, Perplexity, Clause
  - Metrics: response quality, latency, context handling
  - Free vs Paid tiers: comparing Plus/Pro features (e.g., token limits, model versions, compute time)

3. 3. Model Context Protocol (MCP) Deep Dive

- **Overview**: Standard JSON-RPC interface for tool integration
- **Technical Architecture**: Clients, servers, SDKs (Python, TypeScript, Java)
- **Use Cases**: IDE integration, database access, business tools (Slack, GitHub, Postgres, Puppeteer)
- **Security & Risks**: Prompt injection, RCE, unauthorized data access (CVE-2025-49596)

4. 4. Agentic AI: Concepts, Frameworks, & Ethics

- **Definition**: Autonomous systems using ML/DL/RL to act without human intervention
- **Core Traits**: Planning, tool orchestration, monitoring, auditing
- **Ethical Landscape**: Responsibility, governance, misuse, alignment

5. 5. Comparative Agentic AI Platforms

Manus

- Launched March 6, 2025; uses Claude (Anthropic) + Qwen, sandboxed cloud environment
- Multi-agent architecture: planning, execution, validation; real-time audit trail
- Strengths: autonomous execution across tasks; Weaknesses: stability, data privacy, access cost

ChatGPT Deep Research

- Released Feb 3, 2025; autonomous multi-step browsing, citation-aware reporting
- Strengths: depth, citations, PDF/spreadsheet parsing; Limitations: hallucinations, TL computing cost, rate limits

OpenAI Operator

- Research preview browser-based agent; interacts with real web UIs
- Strengths: form-filling, navigation; Weaknesses: shallow outputs, task fragility

6. 6. Hands-On Labs & Comparisons

- **Workshop**: Prompt engineering with ChatGPT, Gemini, Perplexity, Clause; compare outputs, context sensitivity, cost tiers
- **Integrate MCP**: Connect ChatGPT or Gemini with external tools (e.g., KB, spreadsheets) using MCP server

  Agent Design & Execution:

  - Task 1: Manus – automation across research and deployment
  - Task 2: Deep Research flow – autonomous data collection and summary
  - Task 3: Operator – guided browsing and booking via live UI
- **Performance Analysis**: Compare success rates, autonomy level, cost, speed across agents

7. 7. Ethics, Governance & Risk Mitigation

- **MCP Vulnerabilities**: Secure design, hardened SDKs, least privilege model
- **Operational Guardrails**: Human-in-the-loop checkpoints, audit logs, traceability
- **Responsible Agent Use**: Privacy compliance, bias monitoring, transparency

8. 8. Capstone Group Challenge

Design a mini end-to-end agentic workflow

© 2026 Faysal Aziz · Kuala Lumpur