Agents Unleashed Resource Guide – August 15th, 2025

Agents

- [Agents](#)

- [2025 in LLMs so far, illustrated by Pelicans on Bicycles — Simon Willison](#)
- [How We Build Effective Agents: Barry Zhang, Anthropic](#)
- [Andrej Karpathy: Software Is Changing (Again)](#)
- [microsoft/generative-ai-for-beginners: 21 Lessons, Get Started Building with Generative AI](#) 🔗 https://microsoft.github.io/generative-ai-for-beginners/
- [microsoft/ai-agents-for-beginners: 11 Lessons to Get Started Building AI Agents](#)

- [Building effective agents \ Anthropic](#)

- [AI Agents from First Principles](#)

- [My Startup's AI Agent Playbook for 5-10x Engineering Speed (with Claude Code, MCP's, etc) - YouTube](#)

- [Tips for building AI agents](#)
- [[Session] MCP vs ACP vs A2A: Comparing Agent Protocols with Laurie Voss from LlamaIndex](#)
- [Four AI Agent Strategies That Improve GPT-4 and GPT-3.5 Performance](#)
- [VS Code: Open-Source AI Editor](#) (**GitHub Copilot Chat open source)**
- [[2505.22954] Darwin Godel Machine: Open-Ended Evolution of Self-Improving Agents](#)
- [How I program with Agents | crawshaw - 2025-06-08](#)
- [Choosing the right AI model for your task - GitHub Docs](#)
- [How to deploy AI safely | Microsoft Security Blog](#)
- [AI Strategy: A Practical Framework Using Jobs-to-be-Done (JTBD) | by Mike Boysen | Apr, 2025 | Medium](#)
- [Design Patterns for Securing LLM Agents against Prompt Injections](#)
- [Red-teaming a RAG app with the Azure AI Evaluation SDK | Microsoft Community Hub](#)
- [A Survey of Context Engineering for Large Language Models](#)
- [GitHub - Meirtz/Awesome-Context-Engineering: 💧 Comprehensive survey on Context Engineering: from prompt engineering to production-grade AI systems. hundreds of papers, frameworks, and implementation guides for LLMs and AI agents.](#)

[John Alexander](#) - https://github.com/JRAlexander/kcdc-2025

Agents Unleashed Resource Guide – August 15th, 2025

MultiAgents

- Lessons from Toyota for building durable multi-agent copilots
- Conceptual Guide: Multi Agent Architectures
- A2A Protocol - Agent-to-Agent Communication
- [1706.02275] Multi-Agent Actor-Critic for Mixed Cooperative-Competitive Environments

Prompting

- GPT-5 prompting guide
- GPT-5 Prompt Migration and Improvement Using the New Optimizer
- State-Of-The-Art Prompting For AI Agents
- The Prompt Engineering Playbook for Programmers
- Enhance your prompts with meta prompting
- AI-assisted coding for teams that can't get away with vibes - nilenso blog
- AI-assisted coding (simon willison)
- GPT-4.1 Prompting Guide
- The rise of "context engineering"
- Claude 4 System Card
- A Systematic Survey of Prompt Engineering in Large Language Models:
- Techniques and Applications
- Best Practice Guidelines for Prompt Markdown Instructions (.md Files) · GitHub
- GPT-5: Will it RAG?

Tool Calling

- Introducing the Model Context Protocol \ Anthropic
- Introduction - Model Context Protocol
- MCP Dev Days: Day 1 - DevTools
- MCP Dev Days: Day 2 - Builders
- microsoft/mcp-for-beginners: This open-source curriculum is designed to teach the concepts and fundamentals of the Model Context Protocol (MCP), with practical examples in .NET, Java, TypeScript, JavaScript and Python.
- My Lethal Trifecta talk at the Bay Area AI Security Meetup - Simon Willson
- To MCP or not to MCP?
- MCP Gets OAuth: Understanding the New Authorization Specification

John Alexander - https://github.com/JRAlexander/kcdc-2025

Agents Unleashed Resource Guide – August 15th, 2025

- [How to call functions with chat models](#)
- [Authorization - Model Context Protocol](#)
- [The New MCP Authorization Specification · Den Delimarsky](#)
- [Please Don't Write Your Own MCP Authorization Code · Den Delimarsky](#)
- [Announcing Model Context Protocol Support (preview) in Azure AI Foundry Agent Service | Azure AI Foundry Blog](#)
- [Build Agents using Model Context Protocol on Azure | Microsoft Learn](#)
- [Open Protocols for Agent Interoperability Part 1: Inter-Agent Communication on MCP | AWS Open Source Blog](#)
- [Open Protocols for Agent Interoperability Part 2: Authentication on MCP | AWS Open Source Blog](#)
- [Building Agents with Model Context Protocol - Full Workshop with Mahesh Murag of Anthropic](#)
- [How to call functions with chat models](#)
- [Build AI agent tools using remote MCP with Azure Functions | Microsoft Community Hub](#)
- [modelcontextprotocol/inspector: Visual testing tool for MCP servers](#)
- [NLWeb Pioneer Profiles: Customer Success Stories & Use Cases](#)
- [Agentic Coding Recommendations | Armin Ronacher's Thoughts and Writings](#)
- [GitHub - github/awesome-copilot: Community-contributed instructions, prompts, and configurations to help you make the most of GitHub Copilot.](#)

Reports and Industry Studies

- [KPMG AI Quarterly Pulse Survey](#)
- [State of AI Agents | Langbase Research](#)
- [AI agents and autonomous AI | Deloitte Insights](#)
- [Trends_Artificial_Intelligence.pdf](#)
- [16 Changes to AI in the Enterprise: 2025 Edition | Andreessen Horowitz](#)

Examples

- [Shubhamsaboo/awesome-llm-apps: Collection of awesome LLM apps with AI Agents and RAG using OpenAI, Anthropic, Gemini and opensource models.](#)
- [microsoft/multi-agent-reference-architecture: Guide for designing adaptive, scalable, and secure enterprise multi-agent systems](#)
- [hugobowne/AI-for-SWEs: AI for Software Engineers](#)

[John Alexander](#) - https://github.com/JRAlexander/kcdc-2025