

AI Bootcamp 2025

FLOW:

OpenAi Agents SDK + MCP

X

Vasilii Bologov

Oleg Seifullin







MCP stands for Model Context Protocol. It's an open standard that provides a universal way for AI models, particularly large language models (LLMs).









Standardization

MCP standardizes how AI models access and utilize external resources, making it easier to build and deploy AI applications





Key Components

MCP includes specifications, SDKs, and reference implementations to guide developers in building and integrating with MCP-enabled tools and services.



Benefits

MCP simplifies the development of AI agents, enables secure cross-agent collaboration, and promotes the creation of portable toolsets for AI applications.







Inspiration

MCP takes inspiration from the Language Server Protocol (LSP), which is widely used for code editors and IDEs.

What's the trubble?



MCP is a fairly new and raw technology for building agents and does not provide sufficient stability and diversity (for example, in programming languages)















GitHub

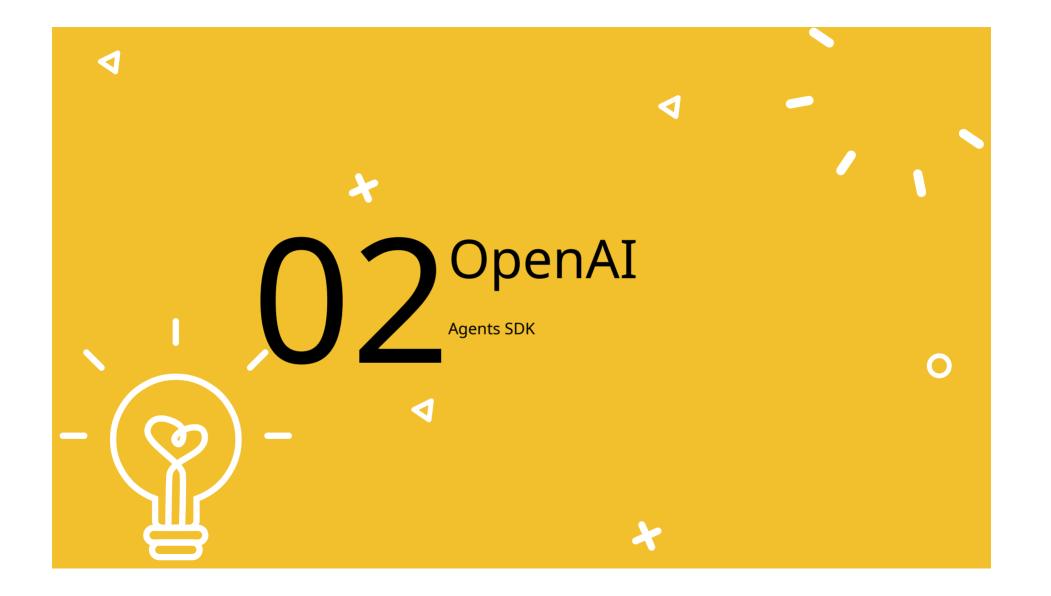


https://www.anthropic.com/news/model-context-protocol

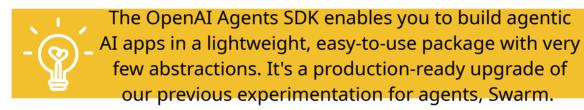


https://github.com/modelcontextprotocol/python-sdk





OpenAI Agents SDK



















Agents, which are LLMs equipped with instructions and tools

Handoffs, which allow agents to delegate to other agents for specific tasks

Guardrails, which enable the inputs to agents to be validated



What's the trubble?



Agents SDK is an even newer and more raw library than even MCP. It only works on pure Python.











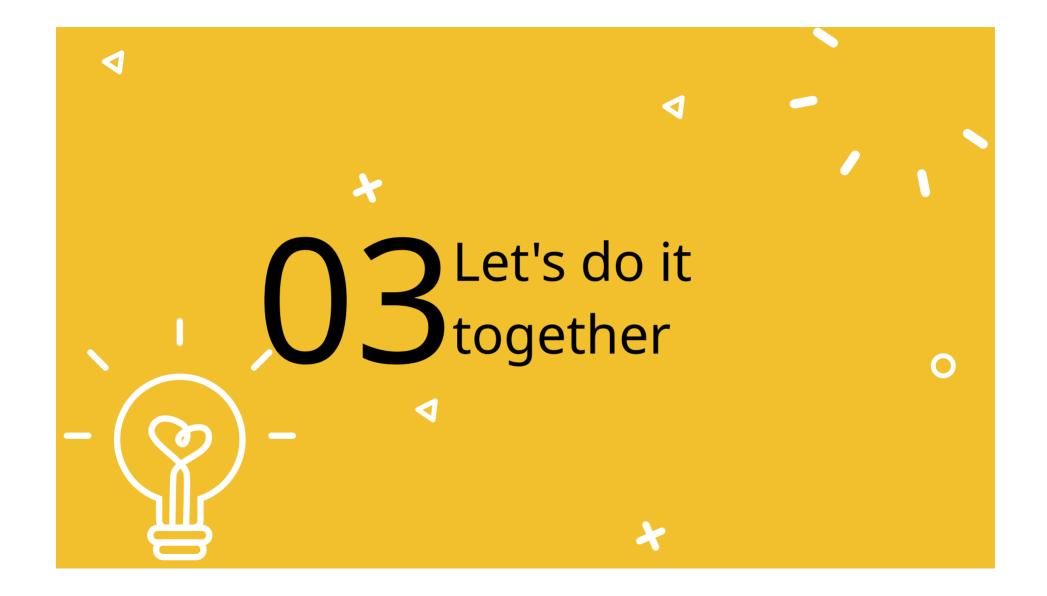
OpenAI Agents SDK



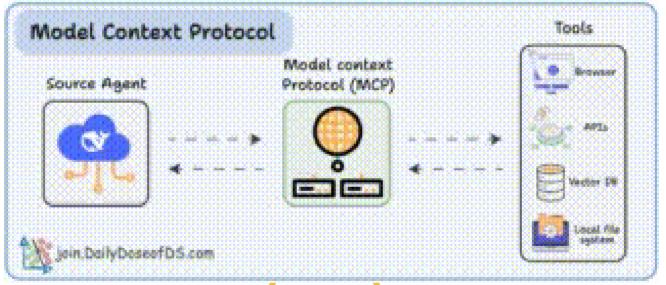
https://openai.github.io/openai-agents-python/







How does this work

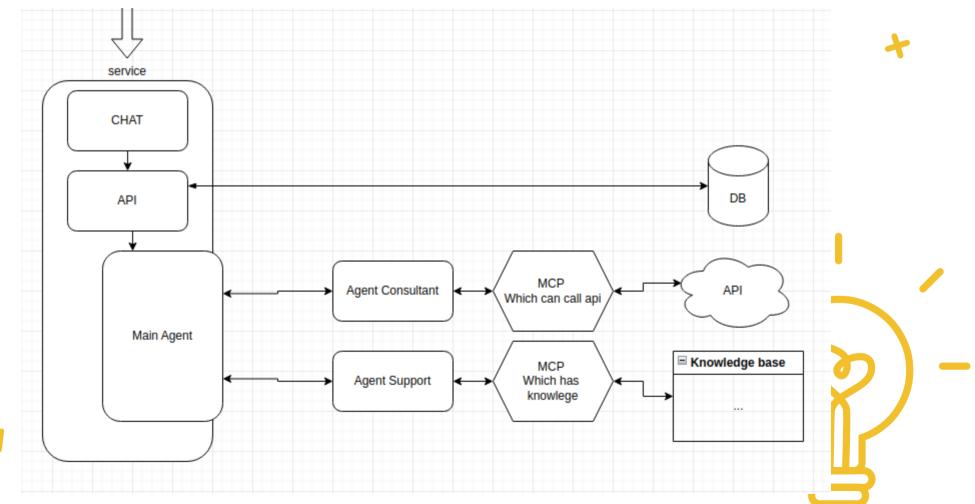














Prototype





https://ai-chat-service.azurewebsites.net/

