

Table of Contents

Introduction to AI Agents

- Agenda
- What is an AI Agent?
- Chatbot vs Workflow vs AI Agent
- LLM vs (LLM-based) AI Agent
- The Agent Execution Loop
- AI Agent Core Components
- Three Core Components of Every Agent
 - 1: LLM — Agent's Brain
 - 2: Tools — Agent's Hands
 - 3: Loop (Orchestration) — Agent's Nervous System
- Reasoning Patterns
- Major Reasoning Frameworks
- Chain of Thought (CoT): Thinking Step by Step
- CoT limitations for Agents
- ReAct: Reasoning + Acting in a Loop
- Building your first AI Agent
- Agent Frameworks
- Step 1: Pick AI brain
- Step 2: Define 4 tools
- Python Essentials You'll Need
- Anatomy of an Agent Tool
- Step 2 — build the agent's toolbox
- Step 3: create_agent
- Step 3 — Agent's Secret: a reasoning loop
- Step 4: Ask Questions
 - Question 1: "What is $42 + 58$?"
 - Question: " 15×8 , then $\div 3$ "
 - Question 3: rectangle area + square root
- Safety and Guardrails
- Real-World Agent Attacks: These Already Happened
- AI Agent Threat Model: What Can Go Wrong

Defense in Depth: Layered Guardrails Architecture

What You've Learned

LangChain for AI Agents

Agenda

Introduction to LangChain

What is LangChain?

LangChain Ecosystem

Models – Reasoning Engine

Prompt Template – Steering the Model

Chains — Connecting the Pieces

Build your first Agent using LangChain

What Makes an AI Agent?

Tools — Giving LLMs Superpowers

Anatomy of an Agent Tool

Python Essentials You'll Need

The ReAct Pattern

Build Your First Agent

LangChain Agent under the hood

User runs the Python code

LangChain calls Model API

Model Returns a Tool Call #1

LangChain interprets the response

LangChain maps Tool name to real Python function reference

LangChain executes the Python Function (Multiply)

LangChain sends the Tool#1 result back

Model reasons and requests Tool #2

LangChain (interprets) and executes Python Function #2

LangChain returns Tool #2 result

Model generates final answer

Python prints the result

What LangChain hides from you

Your code

LangChain

What You've Learned

Introduction to MCP

- Agenda
- What is Model Context Protocol?
- What is MCP?
- The Problem MCP Solves
- MCP Architecture
- MCP Core Components
- Core Primitives
- The MCP Connection Lifecycle
- MCP uses JSON-RPC 2.0
- MCP Method #1: tools/list
- MCP Method #2: tools/call
- MCP Transport Mechanisms
- Add MCP Server to your First Agent
- Before MCP: First Agent
- After MCP: Two separate files (Client, Server)
- MCP Server
- Agent (MCP Client) connects to the MCP Server
- Agent (MCP Client) discovers (and call) tools from MCP Server
- After MCP: Agent Architecture
- After MCP: What Changed (Tool Execution)
- What Your Agent App No Longer Needs To Do
- From the LLM's Point of View
- Why MCP makes your Agent better
- When Does MCP Actually Help?
- Real-world MCP Walkthrough
- From Sandbox to Real World MCP
- Different Boundaries – Math vs Oracle Usage MCP server
- OCI Usage MCP Server Details
- What You've Learned

OpenAI Responses API and Agents SDK

- Agenda
- OpenAI Agent Stack
- What is an AI Agent?

The OpenAI Agent Stack

Choosing between Responses API and Agents SDK

OpenAI Responses API

The Responses API

Your First Responses API Call

Conversation Chaining with Responses API

Built-in Tools (Model Callable)

Built-in Tool

OpenAI Agents SDK

The Agents SDK

Your First Agent

INSIDE THE SDK (the agent loop — automatic)

Tools and Function Calling

Tools — Giving Agents Superpowers

Building a Function Tool

YOUR CODE (4 steps)

SDK AGENT LOOP (automatic — runs until done)

OpenAI Agents SDK vs LangChain

Multi Agent Systems with Handoffs

Multi-Agent Systems

Building a Multi-Agent System with Handoffs

Guardrails and Safety

Guardrails — Keeping Agents Safe

Guardrail Code Example

Tracing — See What Your Agent Did

Putting it All Together

Q: where is my order ORD-001?

What You've Learned

Agentic AI for Enterprises

Agenda

Need for Agent Lifecycle and Runtime

The question every beginner hits

The car analogy

Agent Stack

Inside the runtime — things you didn't write

Two paths to production

Key Takeaway

Introduction to OCI Enterprise AI Platform

OCI Enterprise AI Platform

OCI Enterprise AI Models — Chat, Embed, Rerank

OCI Enterprise AI Models — Serving Mode

End-to-end Lifecycle + Runtime, Simplified

OCI Enterprise AI Governance

Introduction to OCI Enterprise AI Agents

OCI Enterprise AI Agents

Two approaches to building with OCI Enterprise AI Agents

OCI Enterprise AI Agents — Lifecycle + Runtime, delivered

OCI Enterprise AI Agents Building Blocks

The OCI Responses API

Agent Tools — Your Agent's Superpowers

Agent Memory — Remembering Context

Agent Lower-Level Building Blocks

Getting started with OCI Enterprise AI Agents

Getting Started

Setting Up Authentication

Your First Agent — Simple Chat

OCI Enterprise AI Agents – Deploy and Scale

Two approaches to OCI Enterprise AI Agents

Deploying Agents — From Local Dev to Production

What You've Learned

Agentic AI for Oracle AI Database

Agenda

Agentic AI for Oracle AI Database

Introduction to Oracle AI Vector Search

The Problem: Why Keywords Aren't Enough

Vectors & Embeddings: Turning Meaning into Math

How Embeddings Are Created

What Is Oracle AI Vector Search?

Oracle AI Vector Search Workflow

Generating Vector Embeddings

Chunking: Splitting Documents for Embedding

The VECTOR Data Type

Distance Functions & Similarity Search

Oracle AI Vector Search Demo

Oracle AI Vector Search Demo – Setup

Oracle AI Vector Search Demo – Data Ingestion

Oracle AI Vector Search Demo – Similarity Search

Oracle AI Vector Search Demo – Top 3 Matches

Oracle AI Vector Search Demo – Vector + Relational Search

Oracle AI Database Private Agent Factory

What Is Oracle AI Database Private Agent Factory?

How Agent Factory Works

Agent Builder

Oracle Select AI Agent Framework

What is Select AI Agent?

Why does this matter?

Architecture: four cooperating layers

Tools: three categories you'll wire up

In practice: a Customer Return Agent

Oracle Autonomous AI Database MCP Server

What Is the Autonomous AI Database MCP Server?

Why a Database-Native MCP Server?

How It Works — Architecture

What You've Learned