

AGENT HARNESS

IN AGENT FRAMEWORK



AgentCamp 2026, Microsoft NERD, Cambridge MA

Jason Haley

AGENDA



- Past 2 years
- Quick Intro to Agent Framework
- What is an Agent Harness?
- Resources

PAST 2 YEARS



HOW HAVE THINGS CHANGED FOR YOU IN THE PAST 2 YEARS?

Just for context this is June 2026 ... so what were you doing in June 2024?

Simple RAG chatbot using Semantic Kernel and GPT-4o

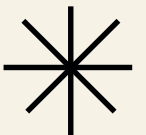


2024

GEN AI BECAME PRACTICAL

PROMPT ENGINEERING

- Multimodal models arrived
- RAG became mainstream
- Function calling matured
- Long context windows expanded
- Coding assistants took off
- Structured outputs started to improve
- Agent concepts started to emerge
- Enterprises launched pilots
- First reasoning model appeared
- MCP introduced

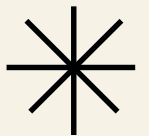


2025

YEAR OF THE AGENTS

CONTEXT ENGINEERING

- Reasoning models matured
- MCP standardized tool integration
- Agent frameworks started to mature
- Agentic architectures started to mature
- Workflows and multistep patterns became more popular
- RAG evolved to Agentic RAG
- Enterprise AI moved from pilots to production
- Coding agents became useful
- Models got **really** good at writing code
- Agent skills introduced

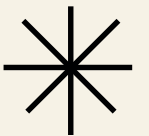


2026

AGENT OPERATIONS

- Open Claw became popular really fast
- Autonomous Agent concerns highlighted
- Coding Agents replaced Coding Assistants
- Agent Skills gained popularity
- Agent Harness concept solidified
- Human orchestration
- Agent security emerging as a major discipline

HARNESS ENGINEERING



AGENT FRAMEWORK



MICROSOFT AGENT FRAMEWORK

Based on two popular frameworks from Microsoft:



Semantic Kernel

Full SDK designed to build AI agents with ease, excellent for single agents and can be extended for multi-agents with integrations to AutoGen



AutoGen

Powerful multi-agent research framework with pre-built conversation orchestration patterns for handling complex agent systems



Agents • Orchestration • Memory • State • Cloud-agnostic • Enterprise-ready

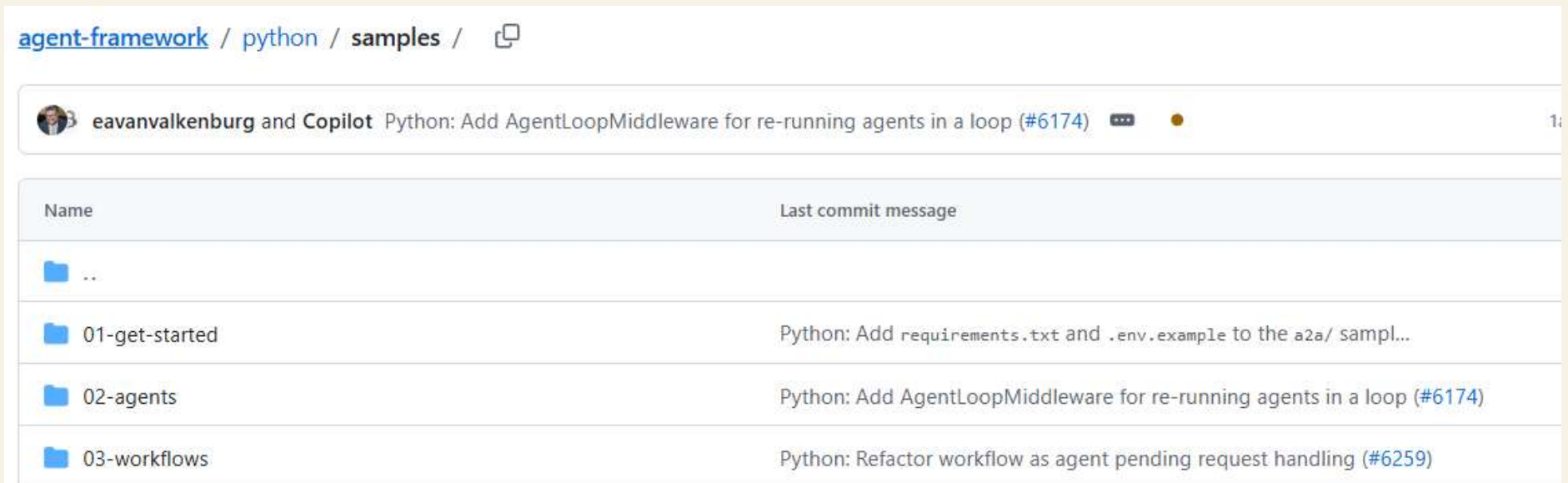
AGENT FRAMEWORK CONCEPTS

- **Chat Clients** – access to LLM providers
- **Agents** – core building block, combines a model, instructions, tools
- **Tools / function calling** – functions agents can invoke to interact with external systems
- **Memory / context providers** – persistent state and context enhancing providers
- **Multi-agent orchestration** – patterns for coordinating agents
- **Workflows** – structured execution of multi-step processes
- **Provider integrations** – multiple options for model providers
- **Data integrations** – connectors to services like Azure AI Search, Cosmos DB, Redis, etc.
- **Observability** – Logging, tracing, monitoring and diagnostics
- **Agent Harness** – execution layer that connects model reasoning to enable actions, workflows and tool usage. *“connects the brain with hands to do things”*

LET'S LOOK AT SOME DEMOS

These are in the source code:

<https://github.com/microsoft/agent-framework/tree/main/python/samples>



The screenshot shows a GitHub repository directory listing for the path `agent-framework / python / samples`. The repository is owned by `eavanvalkenburg` and `Copilot`. The last commit message is `Python: Add AgentLoopMiddleware for re-running agents in a loop (#6174)`. The directory listing shows the following files and folders:

Name	Last commit message
..	
01-get-started	Python: Add <code>requirements.txt</code> and <code>.env.example</code> to the <code>a2a/</code> sampl...
02-agents	Python: Add AgentLoopMiddleware for re-running agents in a loop (#6174)
03-workflows	Python: Refactor workflow as agent pending request handling (#6259)

AGENT HARNESS



CHATBOT WITH TOOLS

User:

Compare these contracts

- Single interaction
- Model is responding to current prompt

Flow:

1. Prompt
2. Retrieve docs
3. LLM Compares
4. Returns answer

AGENT HARNESS

User:

Compare these contracts

- Potentially dozens of tool invocations
- Multiple states
- Long-running workflow
- The harness coordinates everything

Flow

1. Receive contract
2. Create review task
3. Analyze clauses
4. Call retrieve tools
5. Call comparison skill
6. Generate findings
7. Validate findings
8. Request approval
9. Generate report

WHAT IS AN AGENT HARNESS?


Execution environment for agents




- Context management
- Skills and Tools
- Memory and State
- Planning
- Approvals
- Lifecycle hooks
- Observability
- Execution Loop





LET'S LOOK AT A DEMO

This is in the source code:

<https://github.com/microsoft/agent-framework/tree/main/python/samples/02-agents/harness>

agent-framework / python / samples / 02-agents / harness / 

 westey-m and Copilot Python: Integrate shell tool into harness agent (#6451)  

Name	Last commit message
 ..	
 console	Python: Parse MCP CallToolResult.structuredContent field to prevent t...
 README.md	Python: Integrate shell tool into harness agent (#6451)
 harness_research.py	Python: Harness console for python (#6312)

RESOURCES



CODE

Agent Framework Source Code Repo

- <https://github.com/microsoft/agent-framework>

Harness samples

Python:

- <https://github.com/microsoft/agent-framework/tree/main/python/samples/02-agents/harnes>

C#:

- <https://github.com/microsoft/agent-framework/tree/main/dotnet/samples/02-agents/Harness>

CODE

Agentcamp Workshop Agent Framework

Original:

- <https://github.com/GlobalAICommunity/agentcamp-workshop-agent-framework>

Fork:

- <https://github.com/JasonHaley/agentcamp-workshop-agent-framework>

Chainlit Contract Review Agent

- <https://github.com/JasonHaley/chainlit-contract-review-agent>

RESOURCES

Microsoft Build Session "Build26-BRK243-claw-and-agent-harness-in-microsoft-foundry"

- Recording: <https://build.microsoft.com/en-US/sessions/BRK243?source=sessions>
- GitHub: <https://github.com/microsoft/Build26-BRK243-claw-and-agent-harness-in-microsoft-foundry/tree/main>

Article: Agent Harness Explained: Build Production-Ready AI Agents with Microsoft Agent Framework

- <https://dev.to/monuminu/agent-harness-explained-build-production-ready-ai-agents-with-microsoft-agent-framework-666>