



# Agents and MCP: The AI Alliance Projects

**TechXchange** | October 6-7, 2025

Dean Wampler, Dave Nielsen, Jeffrey Borek

IBM and The AI Alliance

[aialliance.org](http://aialliance.org)



# These Slides:

QR code TBD

# Outline



# Outline

- What Is the AI Alliance... and Why?
- Building AI-empowered Applications: Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

# Outline

- What Is the AI Alliance... and Why?
- Building AI-empowered Applications: Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

[aialliance.org](https://aialliance.org)

The AI Alliance brings together organizations, people, and resources to accelerate *open innovation, technology development* and *adoption*.

Launched December 5, 2023



[bsky.app/profile/aialliance.bsky.social](https://bsky.app/profile/aialliance.bsky.social)



[linkedin.com/company/the-aialliance/](https://linkedin.com/company/the-aialliance/)

# Map of Members

Member organizations in the AI Alliance comprise academia, commercial, research and non-profits and span the globe.

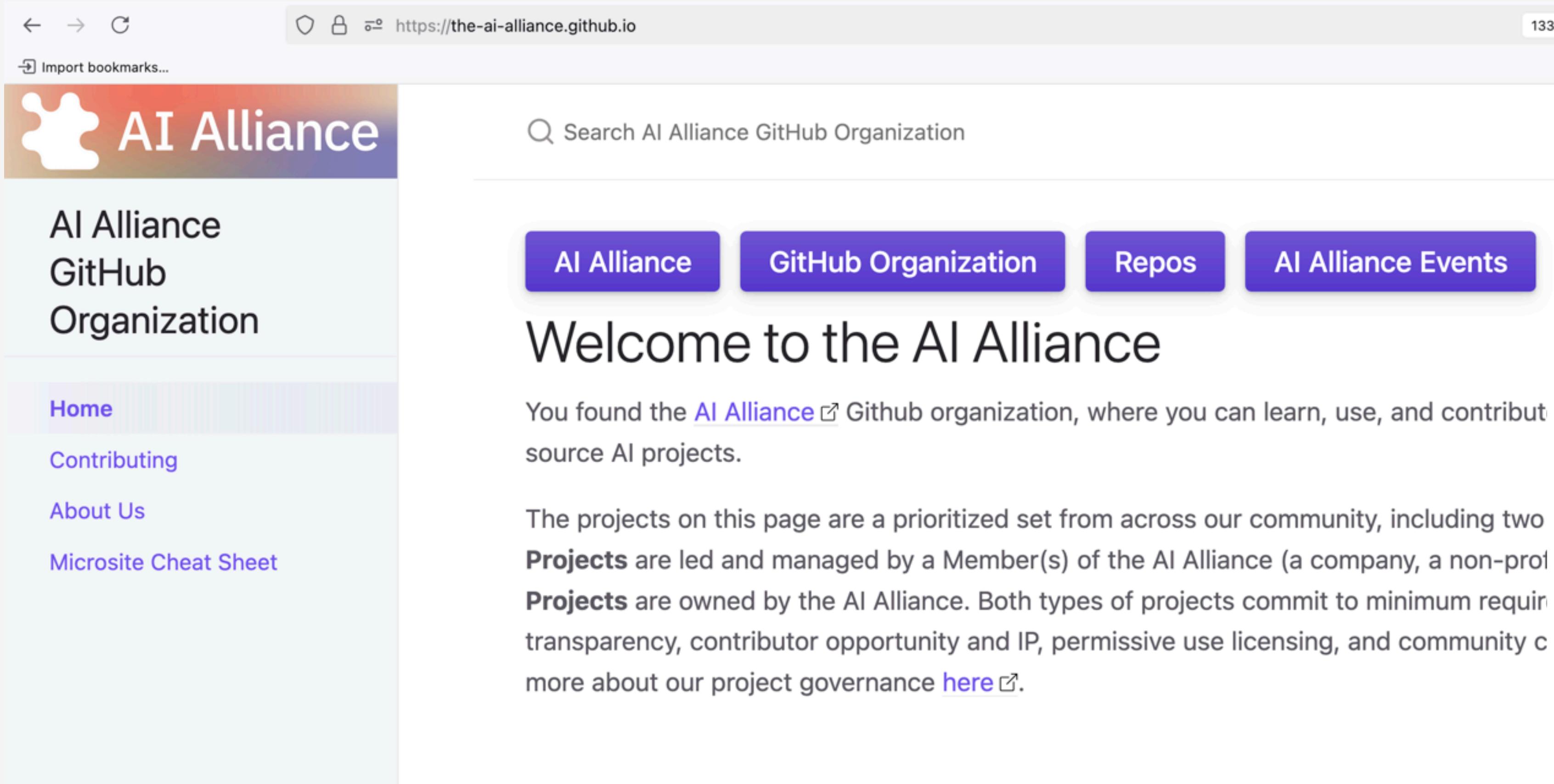
Our core beliefs in AI  
that is open is the tie  
that binds us, despite  
our differences.



The AI Alliance is made up of ~200 organizations in  
24+ countries, and growing



# Numerous Projects:



The screenshot shows the homepage of the AI Alliance GitHub organization. The URL in the address bar is <https://the-ai-alliance.github.io>. The page features a header with the AI Alliance logo and a search bar. Below the header are four navigation buttons: "AI Alliance", "GitHub Organization", "Repos", and "AI Alliance Events". The main content area has a heading "Welcome to the AI Alliance" and a paragraph explaining the organization's purpose and project governance. A sidebar on the left lists links: Home, Contributing, About Us, and Microsite Cheat Sheet. At the bottom right of the page is a call-to-action button with the text "github.com/the-ai-alliance.github.io".



A large QR code is displayed on the right side of the page, which links to the AI Alliance GitHub organization. The QR code has a central graphic element featuring the AI Alliance logo and the text "AI Alliance".

# Outline

- What Is the AI Alliance... and Why?
- Building AI-empowered Applications: Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

# Open Agent Lab

AI ALLIANCE

About Agents Components Use Cases Research Q Log In

## Open Agent Lab

Innovators, researchers, and engineers uniting to craft the next generation of domain-specific AI —powered by open source and tested in real-world enterprises.

All Agents Components Use Cases Research Newest

**AFerretti** @AFerretti · September 17, 2025 Components

**NextGem Catalog**

NextGem is an innovative tool designed to transform the open data landscape by focusing on transparency and usability. Imagine a world where...

[View external link](#)

0 0

**Tim Bonnemann** @tbonnema · September 16, 2025 Components

**DANA**

Domain-Aware Neurosymbolic Agent (Dana), an agent-native programming language

[View external link](#)

0 0

**Tim Bonnemann** @tbonnema · September 16, 2025 Components

**Docling**

Docling simplifies document processing, parsing diverse formats — including advanced PDF understanding — and providing seamless...

[View external link](#)

0 0

**Tim Bonnemann** @tbonnema · September 16, 2025 Components

**Llama Stack**

Composable building blocks to build Llama Apps

[View external link](#)

0 0

**Tim Bonnemann** @tbonnema · September 16, 2025 Components

**SEMIKONG**

First Open-Source Industry-Specific Model for Semiconductors

[View external link](#)

0 0

**Tim Bonnemann** @tbonnema · September 16, 2025 Agents

**Deep Research Agent for Finance**

This app is an example application of a deep research agent designed to collect comprehensive information about publicly-traded companies an...

[View external link](#)

0 0

github.com/the-ai-alliance.github.io



AI Alliance

# MCP Projects

AI Alliance GitHub Organization

Home Home Contributing About Us Microsite Cheat Sheet

AI Alliance

https://the-ai-alliance.github.io 133% Other Bookmarks

## Model Context Protocol (MCP) Ecosystem and Related Projects

The [Model Context Protocol](#) (MCP) from [Anthropic](#) is quickly becoming an industry standard for communications between models, agents, data repositories, and other tools. The AI Alliance seeks to advance this protocol and foster a robust suite of tools around it to enable broad, trusted, and high-value use in production.

Links	Description
<a href="#">repo</a> <a href="#">dashboard</a> <a href="#">issues</a> <a href="#">discussions</a>	MCP has enormous potential to accelerate AI adoption in enterprises. This "live" features chapters written by experts on various aspects of deploying, managing successfully in enterprise settings. It contains the first two chapters with many Contributions are welcome!
<a href="#">repo</a> <a href="#">dashboard</a> <a href="#">issues</a> <a href="#">discussions</a>	The Deep Research Agent for Finance project demonstrates MCP in action for design pattern, <i>Deep Research Agent</i> . This example shows how a financial analysis deep research agent to find, aggregate, and analyze information about a public company (and other potential investment). There are many other applications possible. The accompanying <a href="#">MCP Agent</a> , developed by <a href="#">LastMile AI</a> , discussed next.
<a href="#">repo</a> <a href="#">issues</a>	github.com/the-ai-alliance.github.io

**MCP in the Enterprise: A User Guide**

- [repo](#)
- [dashboard](#)
- [issues](#)
- [discussions](#)

MCP has enormous potential to accelerate AI adoption in enterprises. This "live" features chapters written by experts on various aspects of deploying, managing successfully in enterprise settings. It contains the first two chapters with many Contributions are welcome!

**Deep Research Agent for Finance**

- [repo](#)
- [dashboard](#)
- [issues](#)
- [discussions](#)

The Deep Research Agent for Finance project demonstrates MCP in action for design pattern, *Deep Research Agent*. This example shows how a financial analysis deep research agent to find, aggregate, and analyze information about a public company (and other potential investment). There are many other applications possible. The accompanying [MCP Agent](#), developed by [LastMile AI](#), discussed next.

**LastMile AI MCP Agent**

- [repo](#)
- [issues](#)

github.com/the-ai-alliance.github.io

patterns. See the [Deep Research Agent for Finance](#), discussed in the previous row, which is



# User Guide: MCP in the Enterprise

The screenshot shows a web browser displaying the AI Alliance User Guide at <https://the-ai-alliance.github.io/enterprise-MCP/developing-mcp-servers/>. The page title is "MCP in the Enterprise: A User Guide". The main content area features a search bar, three purple buttons for "Join This Project", "GitHub Repo", and "Discuss This Guide", and a large heading "Developing MCP Servers: Tools, Techniques, and Design Patterns". Below the heading is a summary text about the section's purpose. A blue callout box labeled "Demo" is overlaid on the left side of the content area. The sidebar on the left includes links for Home, Developing MCP Servers (which is expanded to show "Building a Deep Research Agent Using MCP-Agent"), Getting to Know MCP and Its Ecosystem, Contributing, and About Us. The bottom left corner features the AI Alliance logo.

## Developing MCP Servers: Tools, Techniques, and Design Patterns

This section contains chapters about how to write effective MCP servers, including experience reports, tools to consider, and other guidance. Here is a summary of these chapters.

### Building a Deep Research Agent Using MCP-Agent

In [Building a Deep Research Agent Using MCP-Agent](#), Sarmad Qadri , Co-founder and CEO at LastMile AI, and creator of [mcp-agent](#)  documents the journey of building a **Deep Research Agent** with mcp-agent, highlighting the evolution from an initial *Orchestrator* design, to an over-engineered *Adaptive Workflow*, and finally to the streamlined [Deep Orchestrator](#)  now supported in mcp-agent. Sarmad emphasizes his view that "MCP is all you need," and shows how connecting LLMs to MCP servers with simple design patterns enables agents to perform complex, multi-step research tasks. Key lessons include the importance of simplicity over complexity, leveraging deterministic, code-based verification alongside LLM reasoning, external memory for efficiency, and structured prompting for clarity. The resulting Deep Orchestrator balances performance, scalability, and adaptability, proving effective across domains like finance research. Future directions include remote execution, intelligent tool and model selection, and treating memory and knowledge as MCP resources. The open-source project, available on [GitHub](#) , offers developers a powerful foundation for creating general-purpose, AI research agents.

# MCP + Agents

AI Alliance GitHub Organization

Home Home Contributing About Us Microsite Cheat Sheet

AI Alliance

https://the-ai-alliance.github.io 133% Other Bookmarks

## Model Context Protocol (MCP) Ecosystem and Related Projects

The [Model Context Protocol](#) (MCP) from [Anthropic](#) is quickly becoming an industry standard for communications between models, agents, data repositories, and other tools. The AI Alliance seeks to advance this protocol and foster a robust suite of tools around it to enable broad, trusted, and high-value use in production.

Links	Description
<a href="#">repo</a> <a href="#">dashboard</a> <a href="#">issues</a> <a href="#">discussions</a>	MCP has enormous potential to accelerate AI adoption in enterprises. This "live" features chapters written by experts on various aspects of deploying, managing successfully in enterprise settings. It contains the first two chapters with many <a href="#">Contributions are welcome!</a> .
<a href="#">repo</a> <a href="#">dashboard</a> <a href="#">issues</a> <a href="#">discussions</a>	The <a href="#">Deep Research Agent for Finance</a> project demonstrates MCP in action for design pattern, <i>Deep Research Agent</i> . This example shows how a financial analysis deep research agent to find, aggregate, and analyze information about a public company (and other potential investment). There are many other applications possible. The agent is implemented using the <a href="#">MCP Agent</a> , developed by <a href="#">LastMile AI</a> , discussed next.
<a href="#">repo</a> <a href="#">issues</a>	Build effective agents using Model Context Protocol and simple to sophisticated patterns. See the <a href="#">Deep Research Agent for Finance</a> , discussed in the previous row, which is

**Deep Research Agent for Finance**

**LastMile AI MCP Agent**



# MCP + Agents: Deep Research App

The screenshot shows a GitHub repository page for 'The-AI-Alliance/deep-research-agent-for-finance'. The repository is public and has 19 stars. It was generated from 'The-AI-Alliance/microsite-template'. A large blue button labeled 'Demo' is overlaid on the repository's commit history. The commit history lists several recent changes, including a merge pull request, updates to '.github' and 'docs' files, and various commits related to deep finance research and orchestrator integration.

The repository page includes standard GitHub navigation links for Code, Issues (4), Pull requests, Discussions, Actions, Projects (1), Wiki, and Security. On the right side, there is an 'About' section with a description of the repository as an example app for building AI applications, along with links to Readme, Contributing, Activity, Custom properties, and statistics like 19 stars and 0 watching.

**Code** | **Issues 4** | **Pull requests** | **Discussions** | **Actions** | **Projects 1** | **Wiki** | **Security**

**deep-research-agent-for-finance** Public Edit Pins Watch Fork Star 19

generated from [The-AI-Alliance/microsite-template](#)

**Demo**

Commit	Message	Time
andrew-lastmile Merge pull request #16 from andrew-la...	Forgot to add the "use case" label.	last week
.github	merge	3 months ago
docs	Added a title.	2 weeks ago
	deep finance research	3 months ago
	Delete src/finance_deep_search/fina...	last week
.gitignore	integrating deep orchestrator	2 months ago
GITHUB_PAGES.md	Typo!	3 weeks ago

**About**

An example app that explores the challenges of building production-quality AI applications.

- Readme
- Apache-2.0 and 2 other licenses found
- Contributing
- Activity
- Custom properties
- 19 stars
- 0 watching

# Outline

- What Is the AI Alliance... and Why?
- Building AI-empowered Applications: Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts



Problem: I want  
a full stack with  
consistent APIs

# Solution: Llama Stack

← → ⌂ https://the-ai-alliance.github.io 133% ⭐

Import bookmarks... Other Bookmarks

## Llama Stack and Llama Stack Agents

The [Llama Stack](#) project standardizes the core building blocks that simplify AI application development. It codifies best practices across the Llama ecosystem, integrates with other open-source tools and managed services, and provides APIs for inference, evaluation, agents, [MCP](#), and deployment requirements like observability. It is designed to support both on-premise and cloud deployments. The ecosystem provides many example applications to help developers build and deploy AI applications quickly and effectively.

AI Alliance members are [contributing directly](#) to Llama Stack development, as well as applications that illustrate its use in various enterprise scenarios. The [llama-stack-examples](#) initial example applications, described in the table below. The first app is a simple getting started app that shows you the basics of creating an app with Llama Stack and how to run it. The second app (Deep Research) is a deep research application, a popular class of AI applications, which we've chosen to cover other common application patterns seen in several industries. [Please join our community](#) to contribute to the Llama Stack ecosystem.

Links	Description
<a href="#">AI Alliance Llama Stack Example Apps</a>	A growing suite of example applications for <a href="#">Llama Stack</a> that demonstrate features and common application patterns: <ul style="list-style-type: none"><li><a href="#">repo</a></li><li><a href="#">issues</a></li><li><a href="#">discussions</a></li></ul> 1 A getting-started chatbot app, which shows how to build and deploy Llama Stack applications. It includes two different UI options and inference with an <a href="#">LLM</a> or <a href="#">Llama 3</a> model.

github.com/the-ai-alliance.github.io



AI Alliance



Problem: I need  
open, trusted  
datasets

# Solution: Open Trusted Data Initiative

AI Alliance GitHub Organization

Home Contributing About Us Microsite Cheat Sheet

AI Alliance

https://the-ai-alliance.github.io 133% Import bookmarks... Other Bookmarks

## Open Trusted Data and Tooling

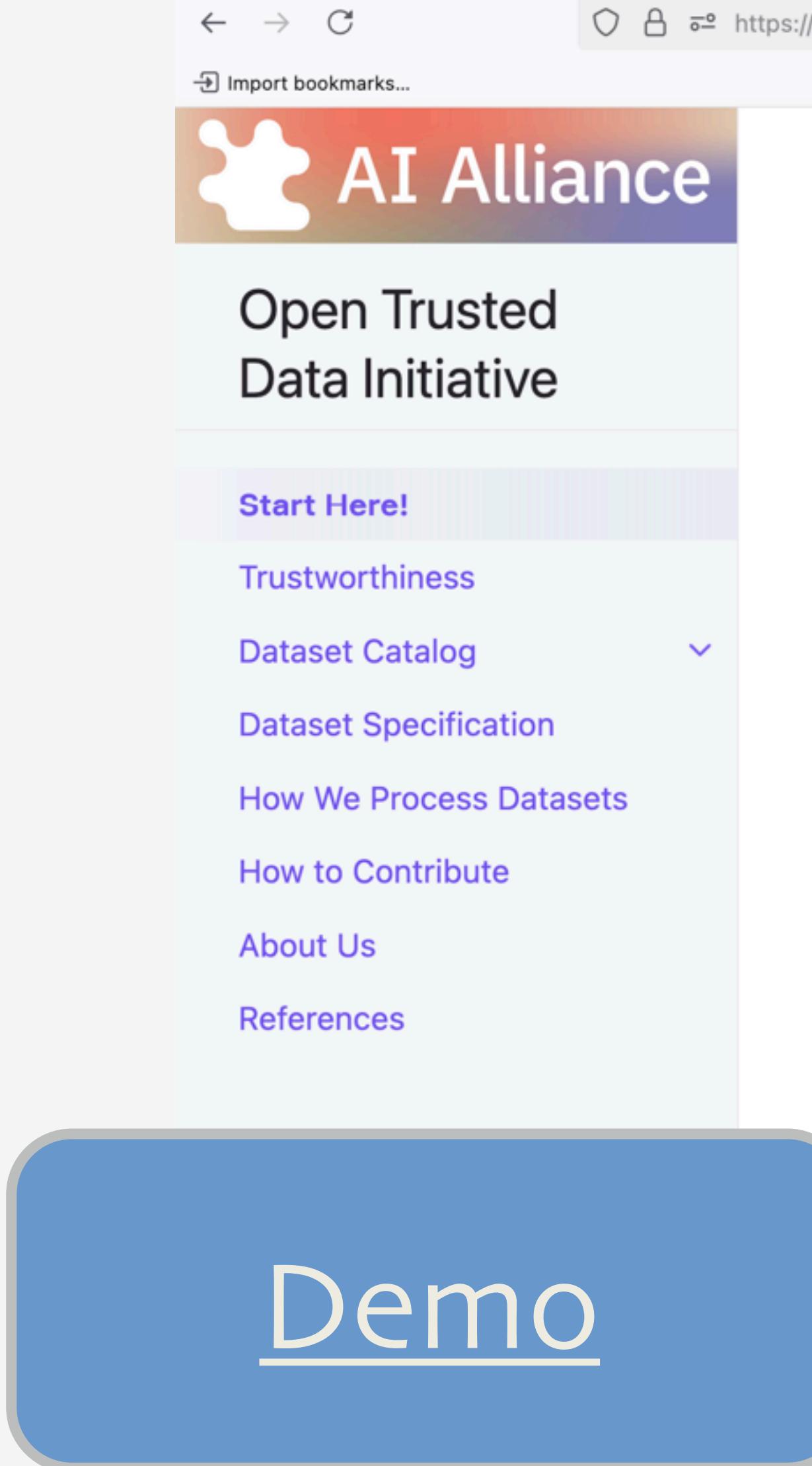
Good datasets are essential for building good models and applications. The AI Alliance is cataloging datasets, and in some cases building them, that have clear licenses for open use, backed by unambiguous provenance and governance constraints.

Links	Description
<a href="#">The Open, Trusted Data Initiative</a>	<p>Open data has clear license for use, across a wide range of topic areas, with clear provenance and governance. OTDI seeks to clarify the criteria for openness and catalog the datasets that meet the criteria. Our projects:</p> <ul style="list-style-type: none"><li>repo ↗</li><li>dashboard ↗</li><li>issues ↗</li><li>discussions ↗</li><li>Open Dataset Catalog: <a href="#">details ↗</a>, <a href="#">current work ↗</a></li><li>Define Openness Criteria: <a href="#">details ↗</a>, <a href="#">current work ↗</a></li><li>Find Diverse Datasets: <a href="#">details ↗</a>, <a href="#">current work ↗</a></li><li>Data Pipelines to Validate Datasets: <a href="#">details ↗</a>, <a href="#">current work ↗</a></li></ul>
<a href="#">Docling</a>	<p>Docling simplifies document processing, parsing diverse formats — including understanding — and providing seamless integrations with the gen AI ecosystem tool for the project <i>Parsing PDFs to Build AI Datasets for Science</i>, discussed at developer: <a href="#">IBM Research ↗</a></p>

github.com/the-ai-alliance.github.io



# Solution: Open Trusted Data Initiative



The screenshot shows the homepage of the Open Trusted Data Initiative (OTDI) from the AI Alliance. The URL is https://the-ai-alliance.github.io/open-trusted-data-initiative/. The page features a top navigation bar with a search bar and three purple buttons: "Join Our Initiative", "Browse the Datasets", and "Contribute a New Dataset". Below this is a large section titled "Open Trusted Data Initiative (OTDI)" with a yellow background containing text about building the world's largest dataset catalog. To the left is a sidebar with links like "Start Here!", "Trustworthiness", "Dataset Catalog", "Dataset Specification", "How We Process Datasets", "How to Contribute", "About Us", and "References". A large blue button labeled "Demo" is prominently displayed in the bottom left corner.

AI Alliance

Open Trusted Data Initiative

Import bookmarks... 133% Other Bookmarks

Search Open Trusted Data Initiative

The AI Alliance

Join Our Initiative Browse the Datasets Contribute a New Dataset

## Open Trusted Data Initiative (OTDI)

*We are building the world's largest, most diverse [catalog](#) of open and transparently sourced datasets for AI. [Join us!](#)*

### Datasets for Languages

Datasets with different human languages.

#### Subcategories

African Languages Languages in the Americas Asian Languages

European Languages Languages in the Middle East

Languages of the Pacific Islands and Nations

### Datasets for Domains

Domains like chemistry, healthcare, etc.



Problem: I can't  
test AI-enabled  
apps!

# Solution: Evaluation and Safety

AI Alliance GitHub Organization

Home Contributing About Us Microsite Cheat Sheet

AI Alliance

<https://the-ai-alliance.github.io>

## Governance, Evaluation, and Safety

Safety, accuracy, red-teaming, security, compliance, and more are required for successful AI applications. How do we know that AI applications are *trustworthy*, that they are *safe*, meaning free of harmful outputs, that they correctly implement the required behaviors? The following projects address these concerns.

Links	Description
<a href="#">The AI Trust and Safety User Guide</a>	An introduction to trust and safety concepts from diverse experts, followed by for how to meet your application's needs. Start here if you are new to trust and leverage the projects discussed next to implement what you need.
<a href="#">Achieving Confidence in Enterprise AI Applications</a>	Are you an enterprise developer? How should you test AI applications? You know deterministic tests for your "pre-AI" applications. What should you do when you AI models, which aren't deterministic? This project adapts existing evaluation "last mile" of AI evaluation; verifying that an AI application correctly implements and use cases, going beyond the general concerns of evaluation for safety, see building nontrivial, reusable examples and instructional materials, so you can learn techniques effectively in combination with the traditional tools you already know. companion <a href="#">Evaluation Reference Stack</a> and <a href="#">Evaluation Is for Everyone</a> projects is part of the <a href="#">Trust and Safety Evaluation Initiative</a> (TSEI).

Evaluation Is for [github.com/the-ai-alliance.github.io](https://github.com/the-ai-alliance.github.io)



# Solution: Evaluation and Safety

The screenshot shows a web browser displaying the AI Alliance website at <https://the-ai-alliance.github.io/ai-application-testing/>. The page title is "Achieving Confidence in Enterprise AI Applications". A large blue button labeled "Demo" is prominent on the left. The main content area features a search bar, two purple buttons ("Join This Project" and "GitHub Repo"), and a large heading. A sidebar on the left lists navigation links.

**AI Alliance**

Achieving Confidence in Enterprise AI Applications

Home  
Testing Problems  
Architecture and Design for Testing  
Testing Strategies and Techniques  
A Working Example  
Glossary of Terms

**Demo**

Search Achieving Confidence in Enterprise AI Applications

Join This Project GitHub Repo

## Achieving Confidence in Enterprise AI Applications

(Previous Title: *AI Application Testing for Developers*)

**I am an Enterprise Developer: How Do I Test My AI Applications??**

I know how to test my traditional software, which is **deterministic** (more or less...), but I don't know how to test my AI applications, which are uniquely **nondeterministic**.

Welcome to the **The AI Alliance** project to advance the state of the art for **Enterprise Testing of Generative AI Applications**. We are building the knowledge and tools you need to achieve the same testing confidence for your AI applications that you have for your traditional applications.

**Tips:**

- 1 Use the search box at the top of this page to find specific content.
- 2 [Capitalized Terms](#) link to glossary definitions.
- 3 Most chapters have a **Highlights** section at the top that summarizes the key takeaways from that chapter.

# Outline

- What Is the AI Alliance... and Why?
- Building AI-empowered Applications: Agents, MCP, ... and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

# Final Thoughts



ContextForge - Meets  
many requirements for  
enterprise deployments  
of MCP.



The AI Alliance - Strives  
to make all users able to  
safely and successfully  
use AI.



ContextForge - Meets  
many requiremen  
enterprise deploy  
of MCP.



Fill out our Trust and  
Safety survey! What are  
you doing? What  
concerns do you have?



The AI Alliance - Strives  
make all users able to  
' and successfully  
l.



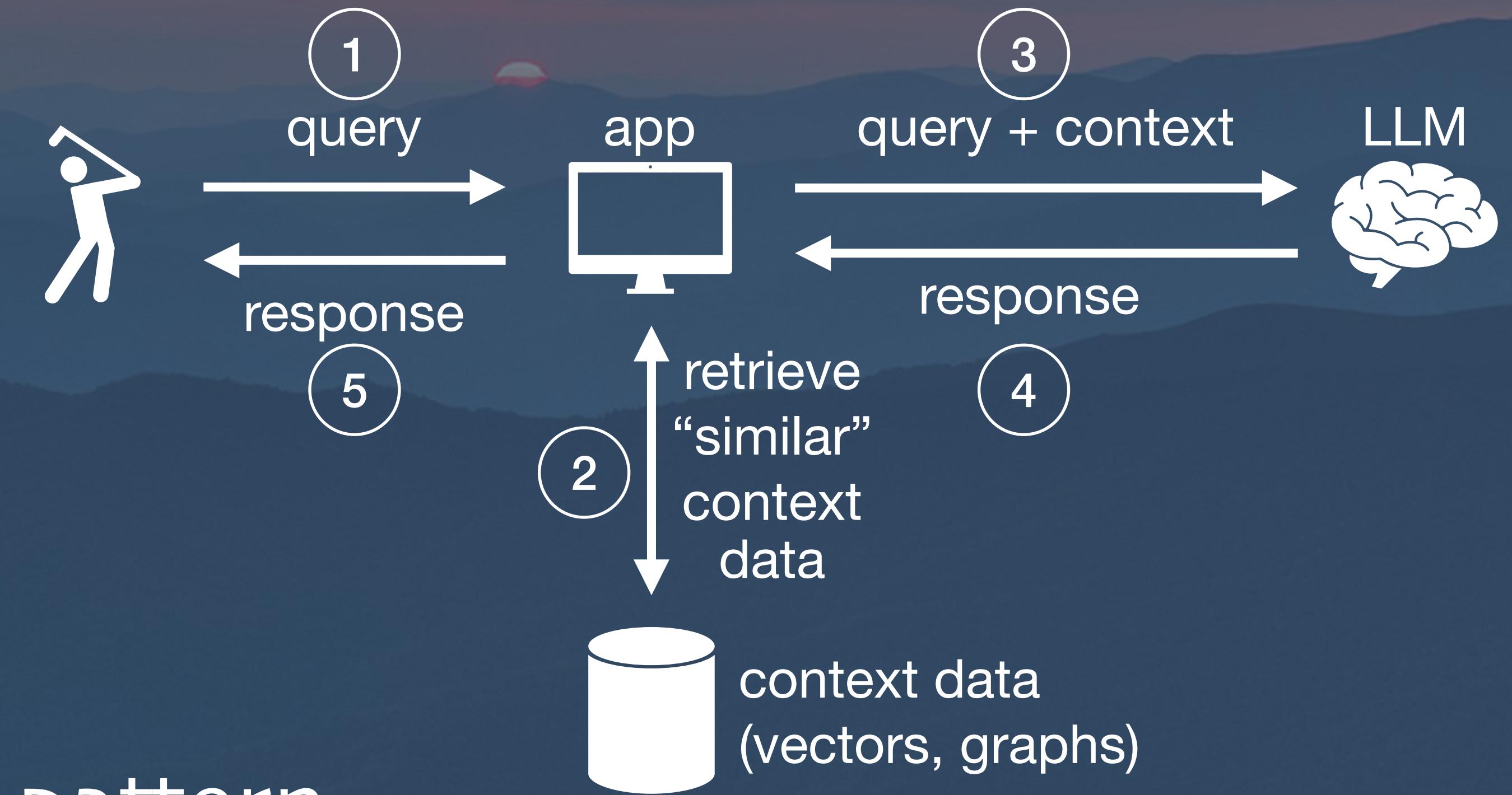
# Extra Slides



# Extra Slides

Retrieval-augmented  
Generation (RAG)

# Retrieval-Augmented Generation (RAG)



The first GenAI application pattern.

- Improves alignment.
- Incorporates new knowledge after training was done.
- Incorporates proprietary domain or use-case knowledge.

# AllyCat

README Apache-2.0 license



license Apache-2.0 issues 16 open Stars 56

## AllyCat

AllyCat is full stack, open source chatbot that uses GenAI LLMs to answer questions about your website. It is simple by design and will run on your laptop or server.

### Why?

AllyCat is purposefully simple so it can be used by developers to learn how RAG-based GenAI works. Yet it is powerful enough to use with your website. You may also extend it for your own purposes.

★ Found this tool helpful? Give it a star on GitHub to support the project and help others discover it!

🗞 [Allycat news](#) - releases and new features!

### How does it work?

AllyCat uses your choice of LLM and vector database to implement a chatbot written in Python using [RAG](#) architecture. AllyCat also includes web scraping tools that extract data from your website (or any website).

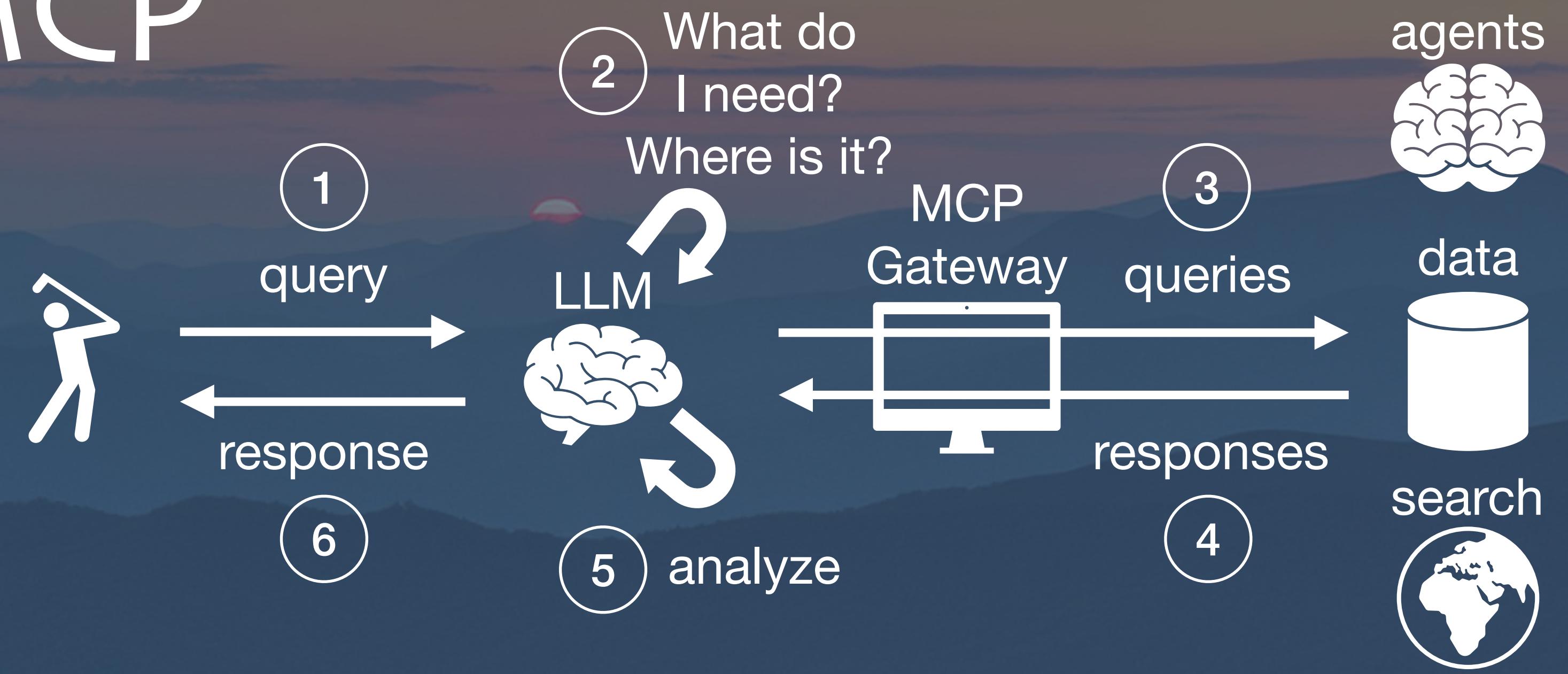
[github.com/The-AI-Alliance/AllyCat/](https://github.com/The-AI-Alliance/AllyCat/)

# Extra Slides

A wide-angle photograph of a mountainous landscape at sunset. The sky is a vibrant orange and yellow, transitioning into darker blues and purples. In the foreground, a winding road or path leads through a grassy, hilly area. The middle ground shows several layers of mountains, their peaks silhouetted against the bright sky. The sun is visible as a small red dot on the horizon. The overall atmosphere is peaceful and inspiring.

Agents and Model  
Context Protocol (MCP)

# Agents and MCP



Repeat 2-5 as needed!

The second+ GenAI application pattern(s).

- LLMs do what they do best. Other tools do what they do best, orchestrated together.
- Flexible for very diverse use cases.