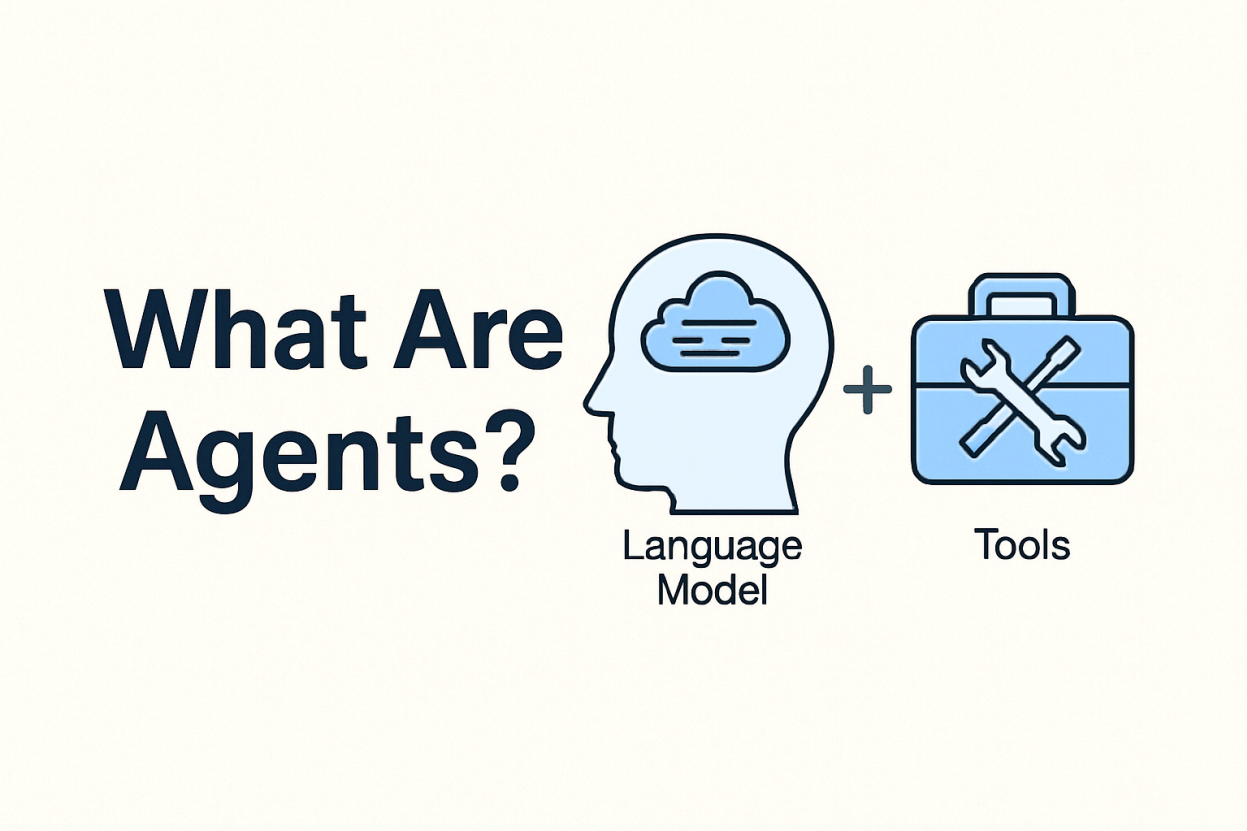
Lesson 1: What Are Agents?

Type	@datasciencebrain

Lesson 1: What Are Agents?

Today, we're going to break down a simple but powerful concept in modern AI: **agents**. This is the foundation for everything we'll be learning going forward.



1. What is an Agent?

An **agent** is not just a language model answering questions. Instead, it's a system that uses a language model to **decide which external tools to use** to accomplish a task.

For example, if you ask a chatbot, *“What’s the weather in Kochi?”*, a regular LLM will try to guess based on training data. But an **agent** knows it doesn’t know the answer. So it **chooses the right tool**—like a web search—and fetches real-time data.

So the key difference is this:

> An agent doesn’t just answer. It reasons and acts.

---

2. Why Do We Need Agents?

Language models are powerful, but they have limitations:

- They **can’t access live information** (like today's weather or news).
- They **can’t run code**, access APIs, or retrieve data from your systems.

Agents solve this by combining a language model with a set of external tools.

Think of it like this:

- The **LLM is the brain**—it understands your request and figures out what needs to be done.
- The **tools are the hands**—they go out and do the actual work (like searching, computing, or calling APIs).

Agents bridge the gap between **language** and **action**.

---

3. How Does an Agent Work?

The simplest way to describe it:

> Agent = Language Model + Tools

Let’s say the user asks:

"Generate a graph of sin(x) from -10 to 10 and describe it."

Here’s what happens inside an agent:

1. The language model decides: “I need to run code for this.”

2. It selects the **PythonTool**.
3. It writes the code and runs it.
4. It returns the graph and a description.

This is far beyond simple prompt and response. The agent is making **decisions**, taking **actions**, and **combining results** to complete the task.

---

4. What Tools Can Be Used?

Tools can be anything the model knows how to call. Some common ones:

- **SearchTool** – queries the internet
- **PythonTool** – runs Python code
- **ImageTool** – generates or processes images

Each tool has:

- A **description** – so the model knows what it does
- A **defined interface** – so it knows how to use it

You can also create your own custom tools for specific business logic or systems.

---

5. Why Agents Matter

Agents unlock entirely new possibilities with language models:

- They can **get real-time answers**, not just guesses.
- They can **perform multiple steps** to complete a task.
- They can **interact with real systems**, not just text.

This is essential for building practical AI applications—like assistants that automate workflows, summarize reports, fetch live data, or interact with software.

Summary

Let's recap the key ideas:

- An **agent** is a language model + a set of tools.

- It decides which tools to use based on the task.
- This allows it to go beyond language and actually **act** in the real world.

Agents turn a passive model into an active system that can solve real problems by using the right tools at the right time.

This is just the beginning. In the upcoming lessons, we'll see how to actually build and use these agents in code, starting from simple tools and moving toward full multi-step systems.