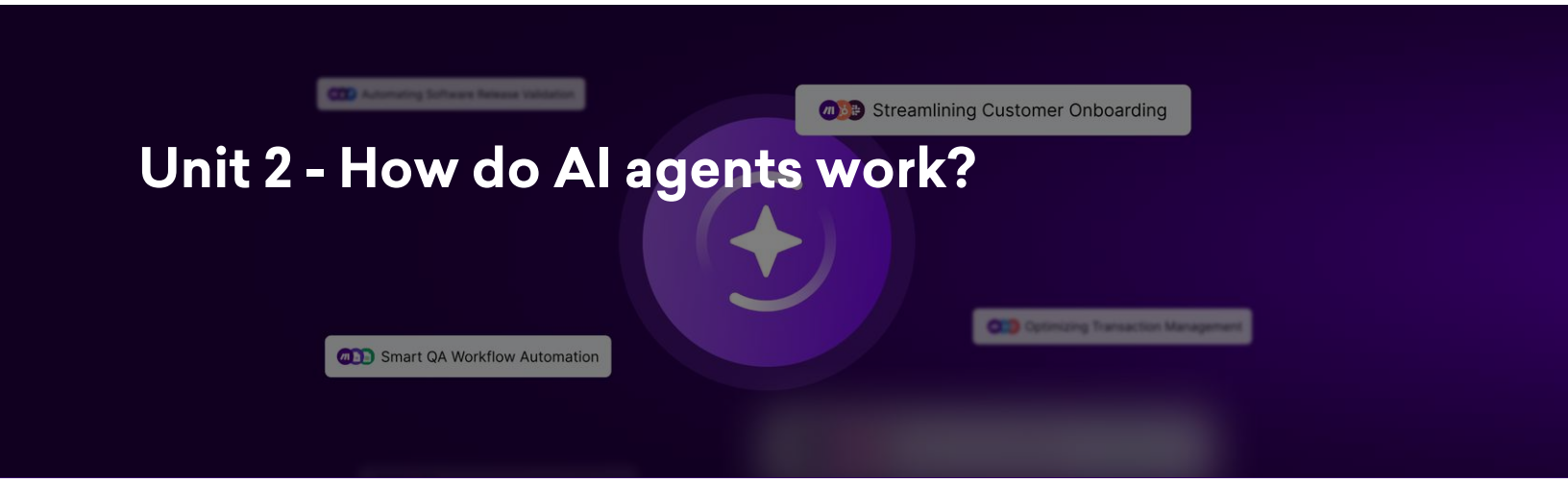



# Unit 2 - How do AI agents work?

UNIT 2: HOW DO AI AGENTS WORK?

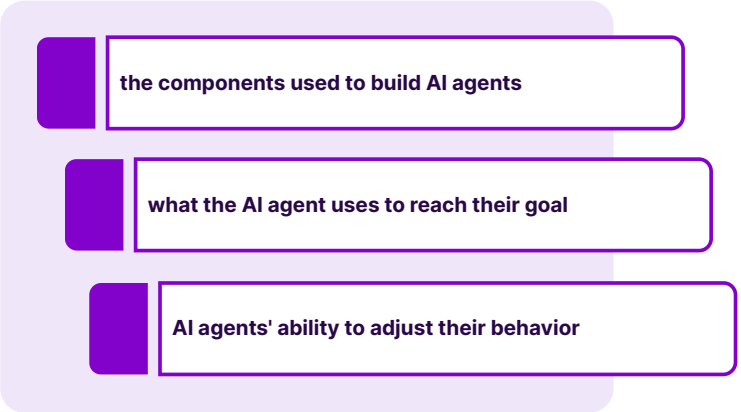
Unit 2
How do AI agents work?

## 2.1 Unit Introduction

# Welcome to the second unit of the course AI agents for beginners!

Now that you know what AI agents are, it's time to explore how they actually work.

**You will focus on :**



## Ready to collect some more clues about AI agents?

Continue to 2.2: Components

## 2.2 Components

In the previous unit, you saw that **AI agents** are software that can act on their own to achieve a specific goal. In this unit, you will learn how AI agents are built and how they work!

An AI agent is made up of the following components:

1. **LLMs**
2. **Prompts**
3. **Tools**
4. **Context files**
5. **Memory**

Each component plays a specific role, and together they enable the AI agent to understand the task and take action to reach its goal.

These components also define the **environment** in which the AI agent works and operates. The AI agent isn't free to do whatever it wants. Its actions depend on how you set it up and the components you give to it when building it.

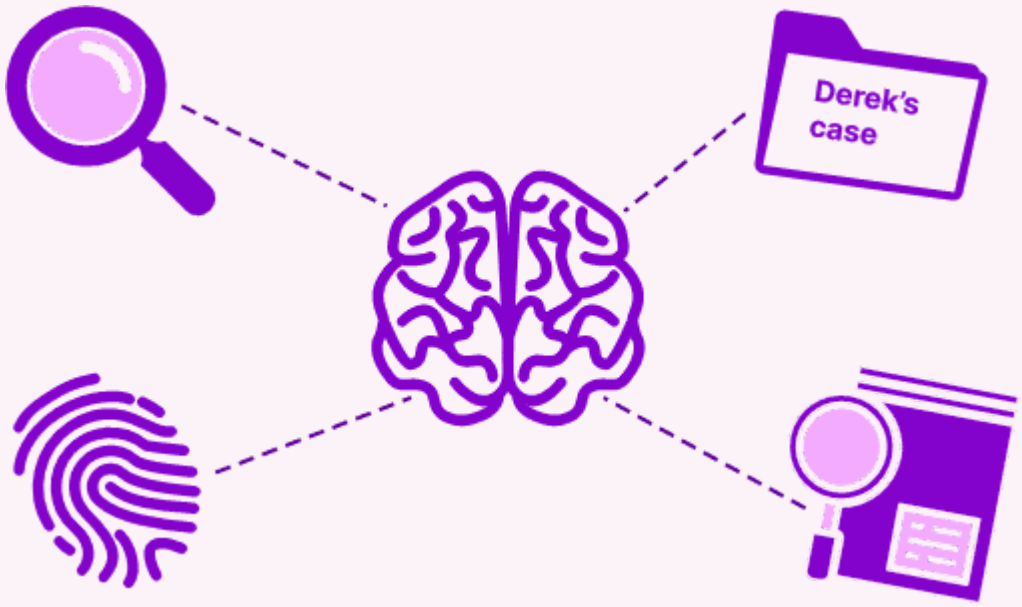
***On his first day on the job, Barbara the Boss gives Derek the Detective everything he needs to work: his job description, a detective toolkit, and access to the police database. This is what he can use at the crime scene, along with his brain, of course.***

Let's explore each of the components.

Continue to 2.2.1: LLMs

## 2.2.1 LLMs

**AI agents are built on top of LLMs, which work as their thinking brain.**




**Large Language Models (LLMs)** are a type of AI that can **understand and generate human language**, as explained in the [AI Fundamentals] course. AI agents use this ability to think, plan, and communicate.

In an AI agent, the LLM acts like the brain. It plays a central role in helping the AI agent complete tasks.

What can the AI agent do with LLMs?

***Click each tab to learn more.***

**Understand instructions** _

Read and interpret the prompt (the instructions or request you give it) to understand what it needs to achieve.

**Think through the problem** _

Reason about what it should do to reach the goal.

**Plan the steps** _

Develop a plan for the actions it needs to take to reach the goal.

**Choose tools** _

Decide which tools (apps, services, or resources) to use and how to use them

from the list of tools available.

**Communicate results**

Write the result.

The LLM is involved in every step AI agents take to achieve their goals.

***Derek the detective has a sharp mind that helps him solve each case. When he gets a new case, he reads the file carefully, thinks through the clues, and creates a smart plan to solve it. He figures out which tools to use and writes up his findings to report back to Barbara.***

Continue to 2.2.2: Prompt

## 2.2.2 Prompt

**The prompt is the instruction you give to the AI agent. It tells the AI agent who it is and what it should do.**

There are two different types of prompts that guide the AI agent:

- **System prompt**, you set it up when creating the AI agent.
- **User prompt**, you give it to the AI agent when asking it to do a specific task.

Let's start by looking at the system prompt. You will learn about the user prompt later.


The **system prompt** defines the AI agent's **role**. It tells the AI agent **who it should act as**, and you define it when you build the AI agent.

This influences the way the AI agent writes its response and decides what to do. It determines:

- **Tone of the response:** it shapes how the AI agent replies to the user. It can sound friendly, formal, serious, or playful, depending on the type of conversation.
- **Language choice**: it influences the vocabulary and phrasing depending on its audience.
- **Decision-making:** it defines how the AI agent chooses between options, such as when to simplify vs. elaborate, or when to focus on speed vs. completeness.

**How does the system prompt look like for the inventory management AI agent?**

"You are an inventory management specialist focused on analyzing inventory levels, customer behavior, and product popularity".

***Click each card to see the impact of this system prompt.***

| | |
|---|---|
| **Tone of the response** | Professional and clear |

| | |
|---|---|
| **Language choice** | Terms related to inventory and sales |
| **Decision-making** | Priority to data-driven decisions |

*It's Derek the Detective's first day on his job. Barbara gives him his job description. He's a police detective that investigates robberies. This tells Derek that he has to speak seriously and professionally when interviewing witnesses, using investigation-related terms like suspect, evidence, and alibi. He also knows that he chooses to double-check evidence before jumping to conclusions, because accuracy matters more than speed when solving crimes. And avoid sending to jail an innocent person.*

Continue to 2.2.3: Tools

## 2.2.3 Tools

**AI agents act using tools.**

AI agents need LLMs to understand instructions, plan, and make decisions. But **LLMs can’t do things on their own**: they can't access the

internet, update a file, or send an email. LLMs can only handle text, but cannot act. However, AI agents need to perform actions to reach a goal.

**That's where tools come in.**

**Tools** are **external resources** AI agents use to actually do things. Think of it like this: if the LLM is the brain, then tools are the hands, they perform actions the brain decides to do.

Here are some examples of the types of tools AI agents can use.

***Click each tab to learn more.***

**Web search tools**

Allow the AI agent to search the web to find real-time information, such as the latest news, prices, or product details.

**File handling tools**

Allow the AI agent to open and interact with documents, spreadsheets, or databases to retrieve information or update records.

**Messaging tools**

Allow the AI agent to communicate with users by sending emails, chat messages, or notifications.

**Other software or applications**

Allow the AI agent to use external software or applications to perform specific actions, like for example managing bookings, processing payments, updating calendars, or checking the weather.

**What kind of tools can you give to the inventory management AI agent?**

- **Database search tool** to look up inventory levels, product info, and past sales data.
- **Email or messaging tool** to notify suppliers or update the sales team when stock is low.
- **Spreadsheet or report generator** to create summaries, charts, or reports about product trends and customer behavior.

When you build the AI agent, you give it **a list of tools it can use**. The AI agent will **use the tools to perform actions** that will bring it closer to its goal. For each tool, you provide its **name** and a short **description** of what it does. The LLM reads this information, understands what each tool does, and figures out which tool is right for each task.

***On his first day on the job, Derek receives his detective toolkit. It contains a magnifying glass, a fingerprint kit, and a notepad. He will use each tool depending on the situation: the magnifying glass to examine tiny clues, the fingerprint kit to identify who touched an object, and the notepad to record observations. He doesn't need step-by-step instructions, he understands what***

*each tool does and decides which one to use to get closer to solving the case.*

Continue to 2.2.4: Context

## 2.2.4 Context

**Context files are documents and data that give an AI agent the information it needs to achieve its goal.**


Context files are needed because they give the AI agent important **background information** it can refer to while working. This can include things like how a task should be done, rules to follow, examples that worked well before, or any other information that help the AI agent understand the situation better.

Without context files, the AI agent might miss key information or choose solutions that are not optimal. They make the AI agent **more accurate, efficient, and help it reach its goals**.

Context files are **different from the files the AI agent accesses using tools**. Context files store **fixed information** that helps the AI agent understand the task or remember past interactions. In contrast, files accessed through tools can **change over time and can be updated or edited by the AI agent** as part of its work. Context files **stay the same** once stored, and the AI agent doesn't modify them.

Here are some examples of context files:

- **Instructions or guidelines**: step-by-step guides on how the AI agent should perform a specific task.
- **Company style guide**: rules for tone and formatting in written communication that the AI agent can follow when replying to users.
- **Frequently Asked Questions (FAQ)**: common user questions and approved answers the AI agent can refer to when responding.
- **Manuals**: written guides that explain how a software or product works, which the AI agent may need to consult.
- **Glossaries or terminology lists**: predefined vocabulary the AI agent should use or recognize for consistency and clarity.

**What are some context files that you can give to your inventory management agent?**

**Product catalog**: a file with details about all available products, including product IDs, descriptions, categories, and pricing.

**Inventory policies**: rules on how to handle stock levels, restocking amounts, and preferred suppliers.

**Sales report template**: a predefined format the AI agent should follow when generating and presenting sales or inventory reports.

***Derek the Detective uses a manual from the police station that explains how to handle gem robbery cases. It tells him how to log evidence, interview witnesses, and write reports. This manual doesn't change with each case, it's a fixed reference that helps Derek follow the station's rules and stay consistent every time. And make Barbara the Boss happy.***

Continue to 2.2.5: Memory

## 2.2.5 Memory

**Memory is the ability of AI agents to save and remember past information.**

When you build an AI agent, you don't just use it once, you **give it different tasks over time**.

You can have a **conversation** with the AI agent, where you ask questions or make requests, receive answers or actions based on those requests. You can also provide extra details or clarifications to help the agent

understand better, give instructions on how to handle tasks, and offer feedback or corrections to improve its responses. When you're done, you can **start again with a new request**.

The AI agent needs to **remember past interactions and details** to handle these tasks well. That's why memory is important: it helps the AI agent keep track of what happened before, understand ongoing situations, and make better decisions based on everything it has learned.

AI agents have two types of memory. ***Click each tab to learn more.***

**SHORT-TERM MEMORY** | **LONG-TERM MEMORY**

Short term memory in AI agents holds information from the current conversation. It helps the AI agent keep track of recent details, so it can respond appropriately without forgetting what just happened.

**SHORT-TERM MEMORY** | **LONG-TERM MEMORY**

Long-term memory stores information from past conversations. This allows the AI agent to remember facts, preferences, or patterns that help improve future responses and make decisions

based on what it learned before.

Let's look at some examples.

***Click each element to learn more***.

**Short-term memory**

- Recent questions and answers
- Instructions or details from the current conversation
- Current tasks or actions being performed
- Temporary data needed to complete ongoing tasks
- Recent user feedback or corrections

***For the inventory management agent***

- Stock quantities currently being checked or updated
- Details of orders being processed right now

- Recent questions or requests from users about inventory

**Long-term memory**

- User preferences and habits
- Common procedures or workflows
- Product or service knowledge
- Historical data and trends
- Rules and guidelines for tasks

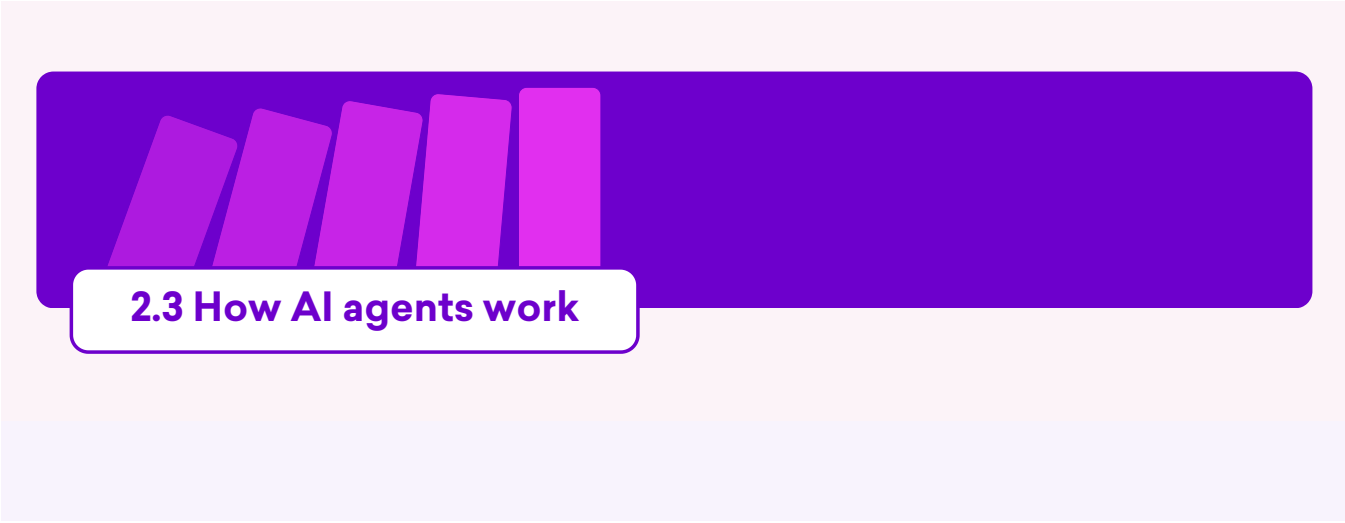
***For the inventory management agent***

- Usual reorder levels for products based on past demand
- Supplier reliability and delivery times remembered from past orders
- Patterns of product popularity over months or seasons

***Derek the Detective doesn't miss a beat. He keeps track of key details during each case, like names, clues, and leads, so he doesn't forget any important information of the case he's working on. But that's not all, he also remembers how he solved past cases, which strategies worked, and what to avoid next time. These help***

*him work smarter and solve new cases more effectively. Who wouldn't want Derek on their case?*

Continue to 2.3: How AI agents work




## AI agents follow this cycle to complete their tasks.


In the previous unit you've seen the cycle that the AI agent follows when working to reach a goal. When you want your AI agent to do something, you give it a prompt, that's what starts the cycle. This prompt is different from the system prompt you saw earlier, and it's called **user prompt**.

## The user prompt sets the AI agent's **goal**, it tells the AI agent what it needs to achieve.

***Barbara the Boss tells Derek that there's been a theft of a very precious gem and he needs to identify the criminal. Derek immediately jumps on the case. Beware thief, Derek will find you!***

When you interact with an AI agent, everything starts with the **user prompt**, the AI agent's goal. This is where you **ask a question**, **give a request**, or **explain what you want the AI agent to do**. The AI agent then replies, takes action, or asks for more details if needed. You can have a full conversation with the AI agent, going back and forth to clarify things, give more instructions, or ask for changes. And when you're done with one task, you can move on to something completely different, and have a conversation about that as well.

Think about the inventory management AI agent working for the *I can't help falling in love with clues* store.

**Task A - Step 1**

You ask the AI agent to check the current stock of trench coats. The AI agent replies with the stock count.

**Task A - Step 2**

You ask the AI agent to place an order and update the inventory. The AI agent orders more trench coats and updates the stock count.

**Task B - Step 1**

> You ask the AI agent to generate a weekly inventory report that includes low stock alerts. The AI agent generates the report.

And so on. The stock is the limit here.

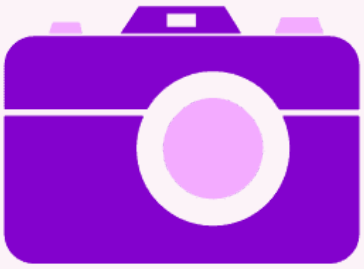
Now that you know how the cycle starts, let's look at each step and see how each component helps the AI agent do its job.

Continue to 2.3.1: Perceive

## 2.3.1 Perceive

The **perceive** step allows the AI agent to **gather all the information it needs to achieve its goal**.

The AI agent can collect different types of information, such as:



**Images or videos**

**Audio transcripts**

**Text**

How are the components used in this step? ***Click each card to learn more.***

## Prompt

Tells the AI agent what the user wants and what information it needs to gather.

## LLM

Starts processing the prompt and figuring out what information is needed. Then decides which tools to use to gather that information.

## Tools

Help the AI agent collect live or external data needed for the task.

## Context files

Provide fixed background info like rules, policies, or task guidelines that help the AI agent understand the task and decide what information to gather and how.

## Memory

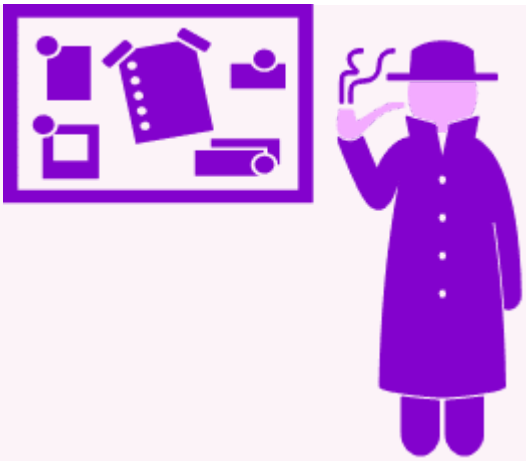
Helps the AI agent recall recent details from the conversation, so it understands the user prompt better and gathers the right information.

When the inventory management AI agent receives the prompt to place an order and update trench coat inventory, it begins by understanding what's being asked. It uses the LLM to interpret the prompt, tools to gather live data like current stock and supplier availability, context files to follow company rules, and memory to recall recent conversations or past preferences. It collects the right information before the next steps.

*Derek the Detective gets a new case and starts figuring out what he needs to solve it. He reads the case file and checks past notes from similar cases to understand which clues he needs to collect. He spots a security camera on the corner and checks the footage. He finds a suspicious list of names and addresses, and uses his magnifying glass to look for fingerprints around the safe. The thief's hours are ticking.*

Continue to 2.3.2: Interpret

## 2.3.2 Interpret



In the **interpret** step, the AI agent **processes and understands the data it collected**.

How are the components used in this step? ***Click each card to learn more.***

## LLM

Analyzes the gathered information to understand what it all means and identify key information.

| | |
|---|---|
| **Context files** | Offer definitions, rules, or examples that help the AI agent interpret the information correctly and follow specific guidelines. |
| **Memory** | Brings in relevant past facts or recent conversation details that help make better sense of the new data. |

The LLM analyzes the data to uncover key ideas, insights, and predictions that will guide its next actions. Here's what it can do:

- **Identify what matters**: focuses on key facts, numbers, or patterns that are useful.
- **Filter out irrelevant information**: removes anything that doesn't help achieve the goal.
- **Make predictions**: based on the current situation, it can estimate what's likely to happen next or which actions have a higher chance of success.

The AI agent analyzes the stock data, sales trends, and supplier availability. It notices that trench coats are selling fast and the current inventory is low. It also sees that the supplier has limited stock.

***Derek lays out all the evidence on a board and starts making connections and crossing off suspects. He studies the security footage, checks the fingerprints, and compares them to his list. He***

*notices that Tyler the Thief was near the scene when the gem disappeared. Based on what he found, Derek identifies Tyler as a suspect. Beware Tyler, Derek is coming for you!*

Continue to 2.3.3: Plan

## 2.3.3 Plan


In the **plan** step, the AI agent **figures out how to reach the goal by deciding what to do and creating a step-by-step plan**.

How are the components used in this step? ***Click each card to learn more.***

## LLM

Creates a step-by-step plan based on the interpreted data and user goal.

## Context files

May include procedures, SOPs, or task-specific guidelines that help shape the plan and ensure it follows company rules.

## Memory

Remembers successful strategies or preferred approaches from past tasks to guide current planning.

The AI agent uses the LLM to decide:

- What to do
- What steps to take
- What order to follow
- Which tools to use in each step

The inventory management agent decides to restock detective trench coats. It plans the steps carefully:

1. First, determine how many trench coats are needed, based on the information from the sales report.
2. Then, pick the best supplier based on delivery time, cost, and stock availability.
3. Next, place the order directly through the supplier’s system.
4. Finally, update the inventory with the new amount.

***Derek has identified that Tyler is the main suspect, so he makes a plan to interrogate him. First, prepare the questions, then look for Tyler's address in the police station records. Next, go to Tyler's house and finally interrogate him. Flawless plan!***

Continue to 2.3.4: Act

## 2.3.4 Act

In the **act** step, the AI agent follows the plan and **performs the actions needed to reach the goal**.

How are the components used in this step? ***Click each card to learn more.***

| | |
|---|---|
| Tools | Perform the tasks identified in the planning step. |
| LLM | Generate instructions or commands for the tools based on the plan. |

In the act step, the inventory management agent follows the plan using its tools to place the order and update the inventory, ensuring the store meets demand.

***Derek follows his precisely crafted plan and discovers that Tyler is the thief. He quickly handcuffs him and brings him to the police station. Tyler fought the law, but the law won.***

Continue to 2.3.5: Communicate

## 2.3.5 Communicate


In the **communicate** step, the AI agent **shares the results of its actions with the user**.

How are the components used in this step? ***Click each card to learn more.***

LLM

Creates the message or response based on the task results.

## Prompt

Guides what the AI agent should say to the user in terms of content and tone.

## Tools

If you use a tool to communicate with the AI agent, like for example a messaging system.

After placing the order, the AI agent informs the user: **"*The trench coats have been reordered. The supplier confirms delivery in 5 days. Inventory levels will be updated once the shipment arrives.*"** It clearly shares the outcome of its actions so the user stays informed.

***Derek tells Barbara that Tyler stole the gem and will be breakin' rocks in the hot sun in no time.***

Continue to 2.3.6: Learn

## 2.3.6 Learn


In the **learning** step, the AI agent reviews the results of its actions and feedback to improve its future performance.

**Feedback** is information the AI agent receives about how well it performed a task. It helps the AI agent understand if its actions were correct, useful, or need improvement.

In practice, **feedback** can come from:

- The **user**, like saying **“that’s not what I meant”** or **“Perfect, thank you!”**

- The **environment**, like a task failing or succeeding (e.g. an order not going through, or stock being updated correctly).

- **Internal checks**, like detecting inconsistencies or errors in its own output, e.g. a mismatch between the demand data and its own order suggestion.

In the learning step, the AI agent **saves the feedback in the memory**. Then, when it faces a similar task, it will adjust its behavior based on what it learned. This helps improve the AI agent's accuracy over time. It becomes more precise, avoids repeating mistakes, and makes better decisions each time.

How are the components used in this step? ***Click each card to learn more.***

LLM

Analyzes the feedback or results to spot mistakes or ways to improve.

| | |
|---|---|
| **Memory** | Stores useful feedback, outcomes, or patterns so they can guide future behavior. |
| **Prompt (optional)** | If the AI agent receives feedback from the user as a prompt, the AI agent uses it to understand what needs to change or what worked. |

The AI agent receives feedback that the last trench coat order arrived too late and caused stock issues. It stores this feedback in long-term memory. Next time it needs to reorder, it avoids that supplier and chooses one with faster delivery, improving its performance.

***Barbara tells Derek that he should have checked the security footage first, instead of starting with the fingerprints. He would have seen Tyler taking the gem and laughing evilly. Derek better remember this for next time!***

Continue to the wrap up for this unit

## 2.4 Wrap up

1

AI agents are built from five components that work together to help them achieve their goals: **LLM, system prompt, tools, context files, and memory**. The AI agent's actions are not completely free; they depend on how you configure it and the components you provide, which shape what the AI agent can understand and do.

2

The **user prompt** sets the AI agent's **goal** and tells it what you want it to do. It's what starts the AI agent's cycle. You can give the AI agent multiple prompts in a row to have a conversation about a task, or switch to unrelated prompts for different tasks.

3

**Feedback** tells the AI agent how well it completed a task. It can come from **the user, the environment, or internal checks**. The AI agent stores this in memory and uses it to **improve future actions**, becoming more accurate and effective over time.

# Unit complete!

**Good job! You have gathered more clues on AI agent.**

By now you should have an understanding of:

- **the components used to build AI agents**
- **what the AI agent uses to reach their goal**
- **AI agents' ability to adjust their behavior**

In the next course you will learn in more detail how AI agents work.

Time to keep investigating!

make | academy

Mark this task complete to continue to the next unit.