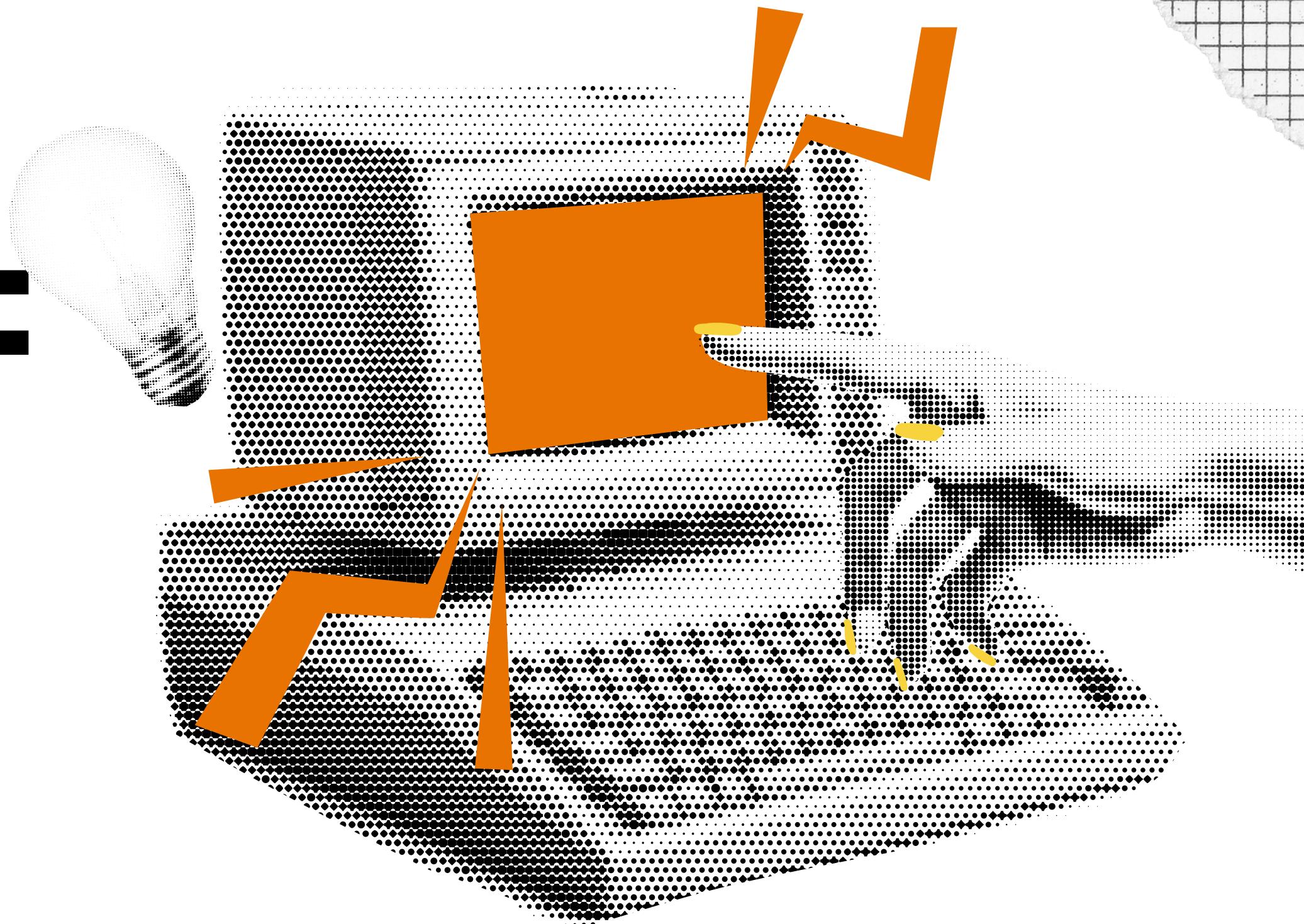


EdgeRun.Ai | GammaXon

# AI-AUGMENTED CYBERSECURITY: LOW-CODE AI

**Training Workshop**

AI-Augmented Cybersecurity: Low-Code AI Edition



**Presented by Bryce Kunz**



# MODULE ZERO



# ABOUT ME



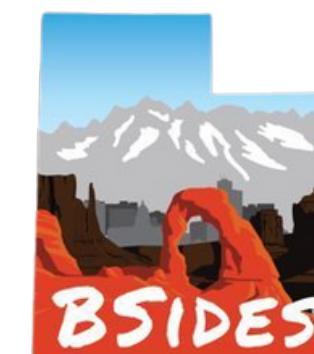
Bryce Kunz // @TweekFawkes



 Adobe  STAGE 2  
SECURITY

 ultraviolet

 black hat®





# SUBSCRIBE FOR MORE!

AI + CyberSecurity

@BryceKunz



**Bryce Kunz**

@brycekunz · 105 subscribers · 16 videos

AI & Cybersecurity, De-mystified ...more

[linkedin.com/in/brycekunz](https://linkedin.com/in/brycekunz) and 6 more links

Customize channel

Manage videos

Home Videos Shorts Playlists Posts

Hacking AI: Bypassing Security Filters to Steal Secrets (Merlin CTF)  
107 views · 2 days ago

ChatGPT GPTs Exposed! How Your Secrets Can Be Stolen (& How to Stop It)  
57 views · 2 weeks ago

Create QR Codes in Seconds! (Easy Tutorial)  
35 views · 2 weeks ago

Hacking an AI: Revealing Secrets on the Gandalf LLM Challenge  
227 views · 3 weeks ago

Python Crash Course: Quick Refresher for AI & LLM Projects  
30 views · 1 month ago

Fool Hackers with AI! Creating a Realistic Honeypot using Gemini & React  
54 views · 1 month ago

Unlock Google Gemini: FREE Access, HUGE Context & Python API Guide  
51 views · 1 month ago

30-Second Security Scan: Are Your Internet Services Exposed? Find Out Now!  
28 views · 1 month ago

Langchain for Beginners: Build Your First AI Automation (Easy Tutorial)  
4:51

Build Your First AI Agent (No Framework Needed!): React Design & Code Explained  
9:53

LLM Function Calling with OpenAI & More!  
13:16

Upload PDF →

ChatGPT AI Markdown



# PREREQUISITES



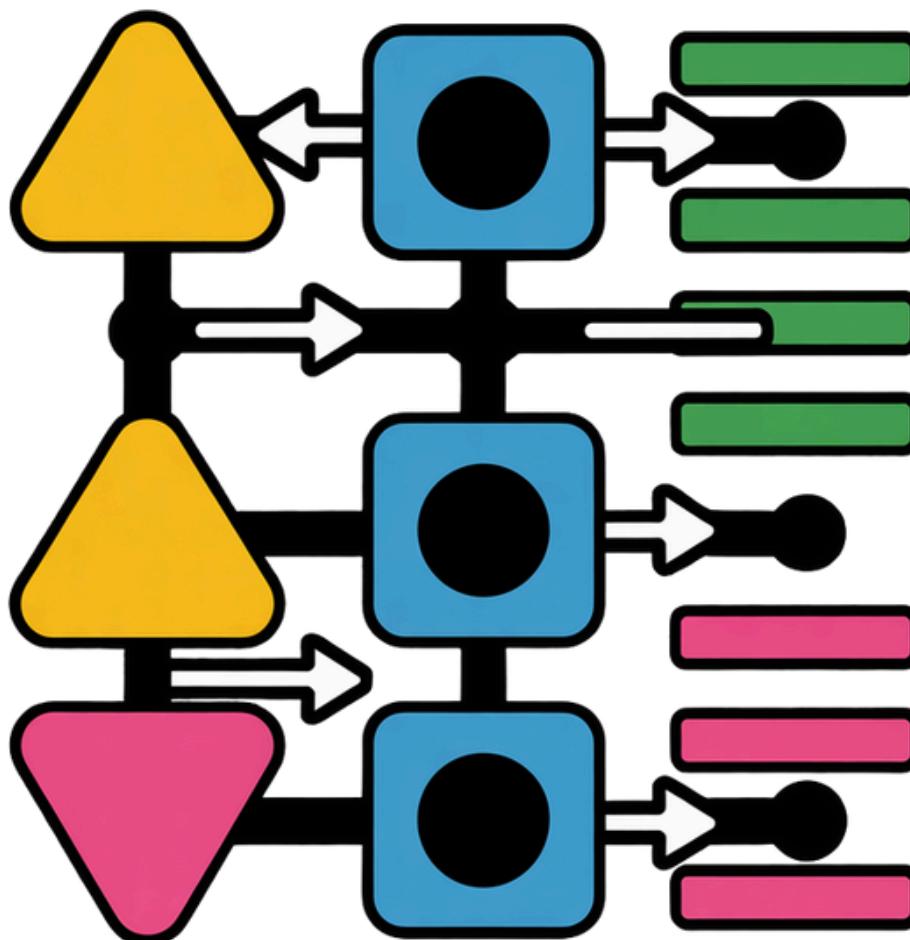
- ★ Some Prompting Experience w/ LLMs is Helpful  
Some Programming Experience (e.g. Python, JavaScript, etc.) is Helpful
- ★ Follow Along:  
[https://github.com/TweekFawkes/AI\\_Augmented\\_Cybersecurity](https://github.com/TweekFawkes/AI_Augmented_Cybersecurity)
- ★ AI Tools:  
<https://Gamma626.org>



# MODULE ONE

# MAKE.COM

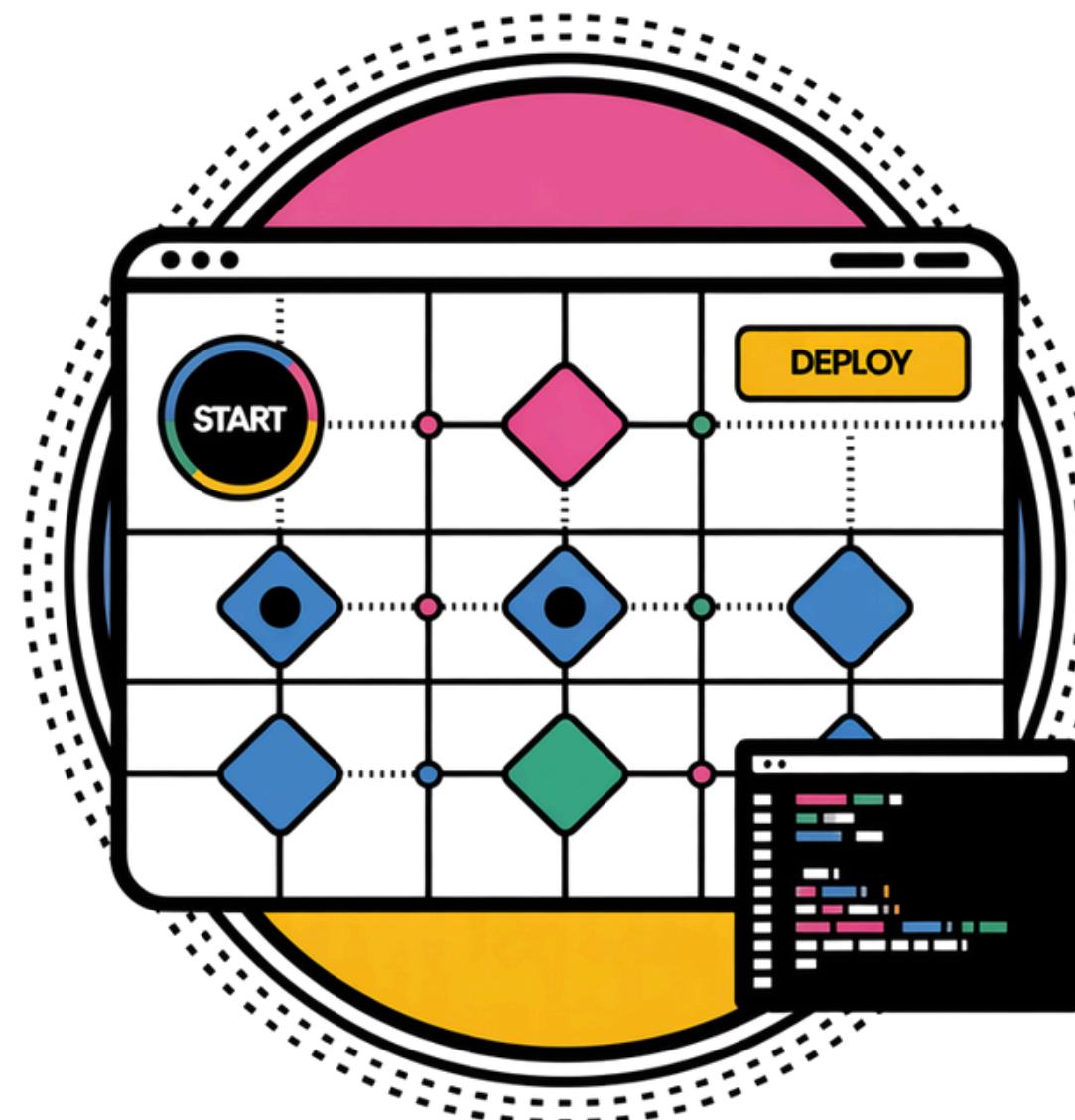
# AUTOMATION BUILDING BLOCKS



- ★ Triggers initiate workflows when specific events occur—form submissions, alerts, or system changes
- ★ Actions execute tasks automatically through API calls, database updates, or tool integrations
- ★ Logic applies decision-making rules to determine next steps based on conditions and context



# LOW-CODE/NO-CODE (LCNC)



Drag-and-drop features eliminate need for heavy coding while maintaining customization



Low-code platforms reduce development costs and require fewer resources than traditional methods



Visual editors make automation accessible to security teams without engineering expertise



# UNDERSTANDING WORKFLOW TRIGGERS



- ★ Triggers are events that automatically initiate workflows and start processes
- ★ Common triggers include new emails, scheduled times, or system changes
- ★ Event-driven architecture enables real-time responses to security threats
- ★ Time-based triggers enable scheduled security scans and compliance checks



# EXAMPLE SCENARIO - TRIGGER





# ACTIONS DRIVE RESULTS



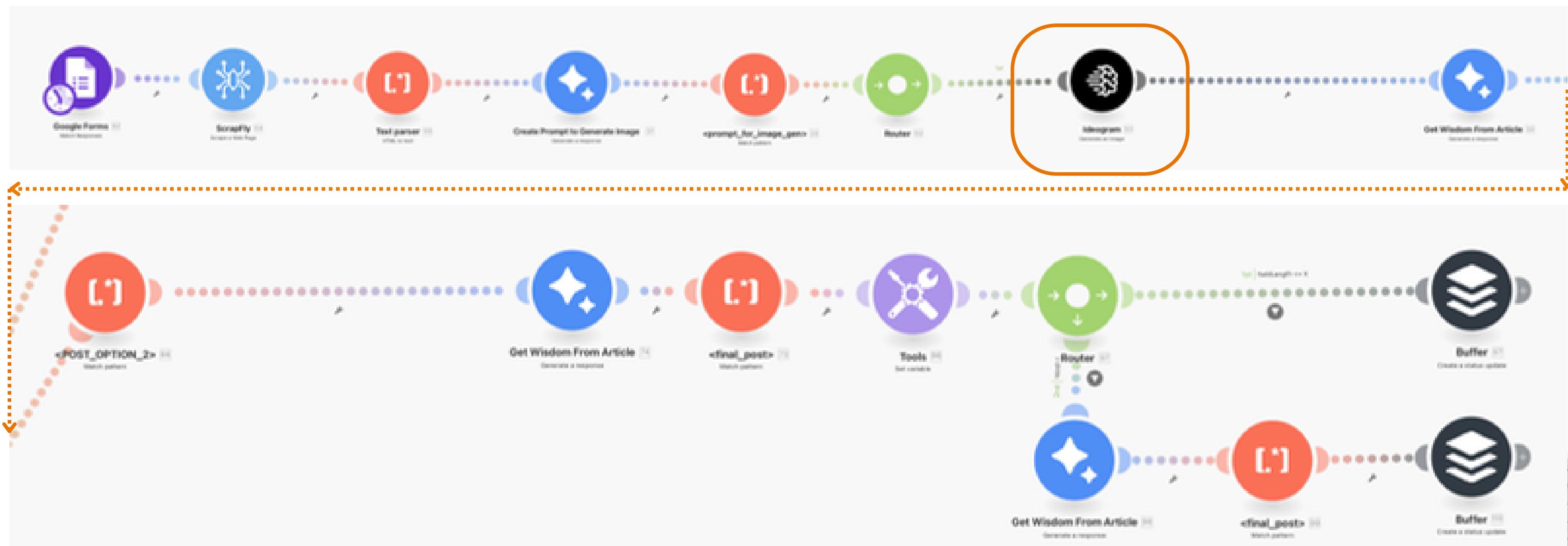
- ★ Actions are automated tasks performed in response to triggers
- ★ Machine-speed execution reduces Mean Time To Respond significantly
- ★ Drag-and-drop interfaces make AI automation accessible to all analysts
- ★ Multiple actions can execute simultaneously for faster response times



# EXAMPLE SCENARIO - WEBSITE DATA

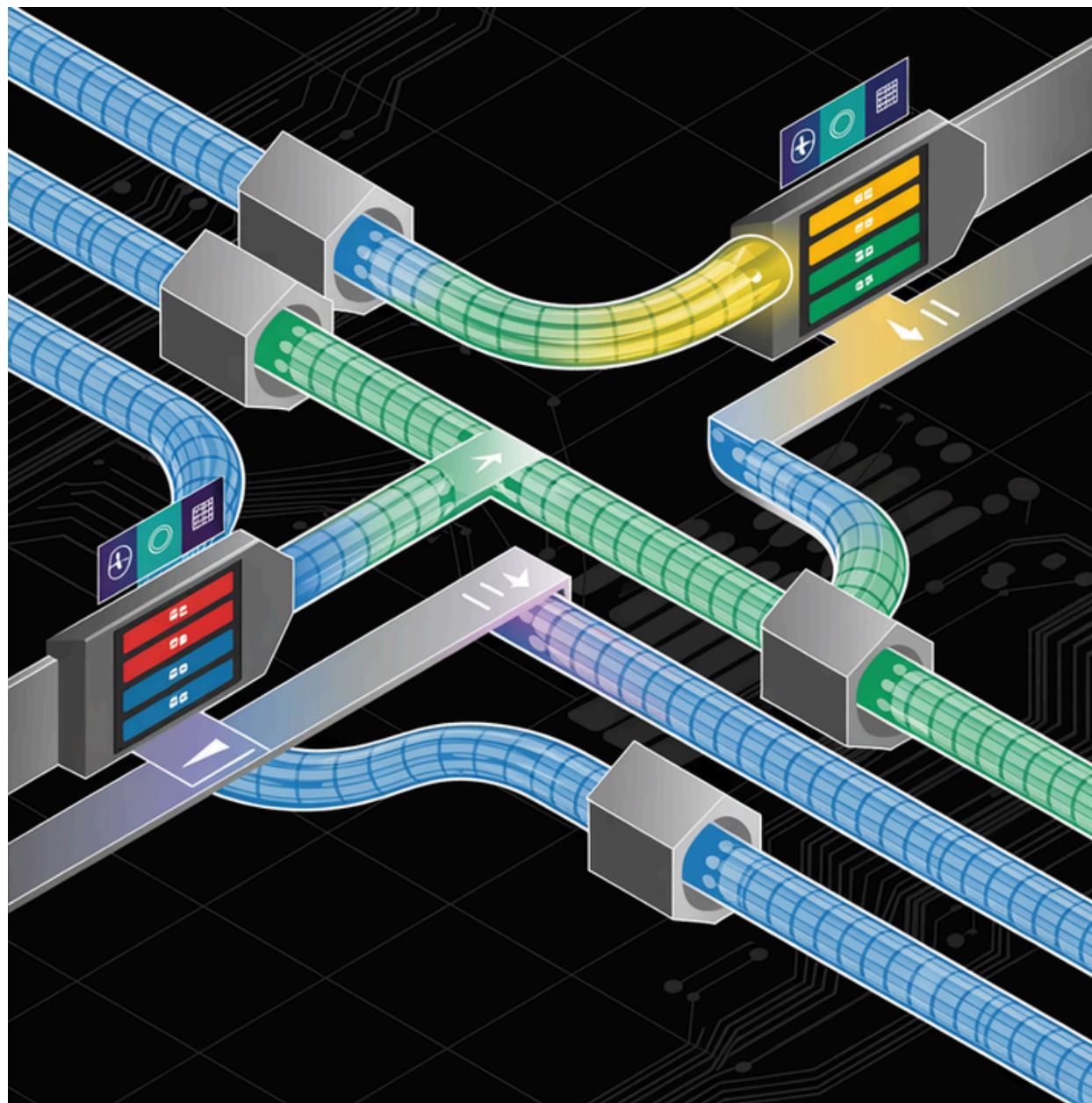


# EXAMPLE SCENARIO - GENERATE IMAGE





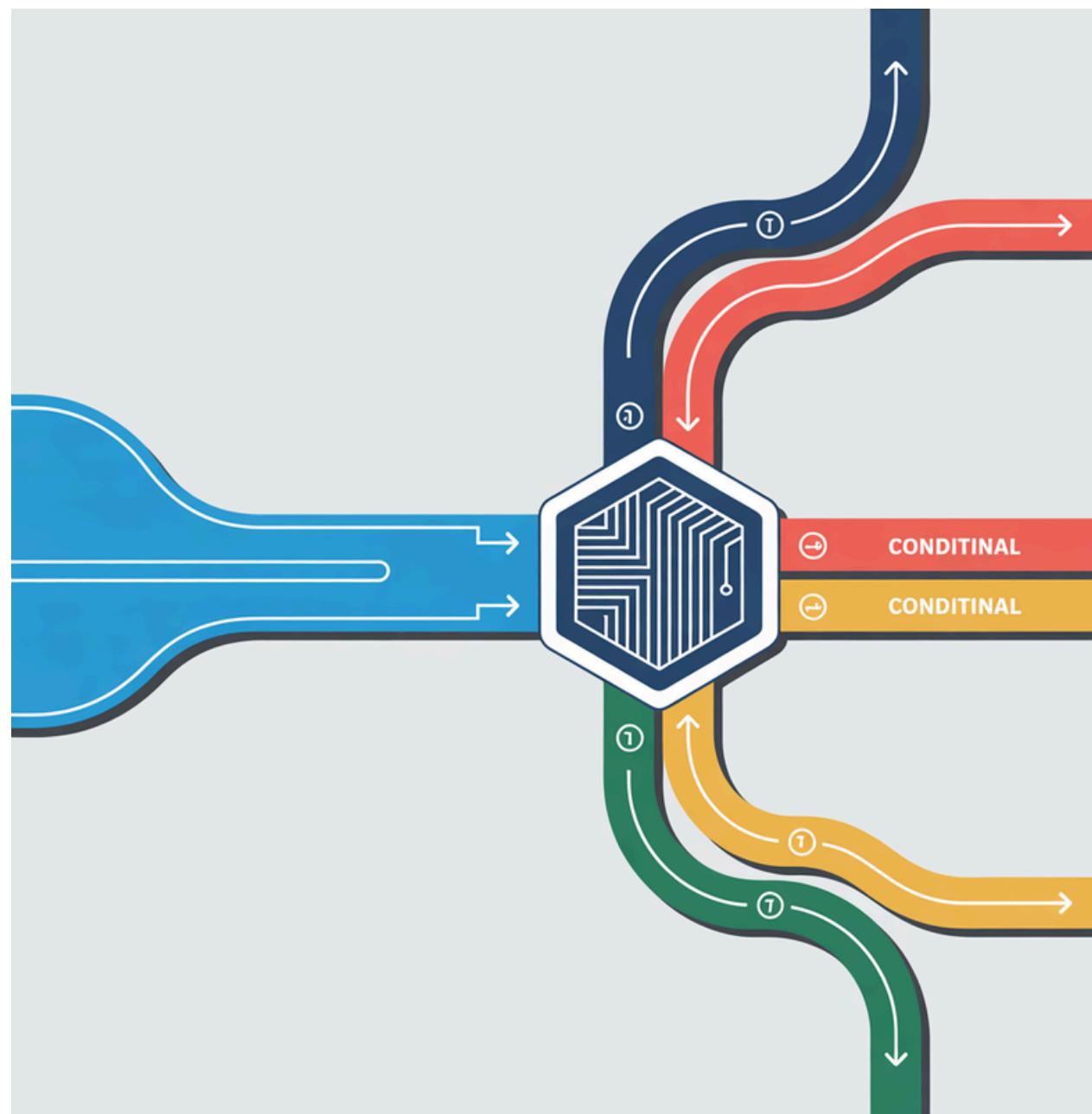
# LOGIC AND CONDITIONS



- ★ Conditions determine whether specific actions should execute or not
- ★ Create complex logic flows that adapt to different security scenarios
- ★ Enable smart routing of alerts to appropriate team members automatically
- ★ Reduce false positives by applying intelligent filtering criteria



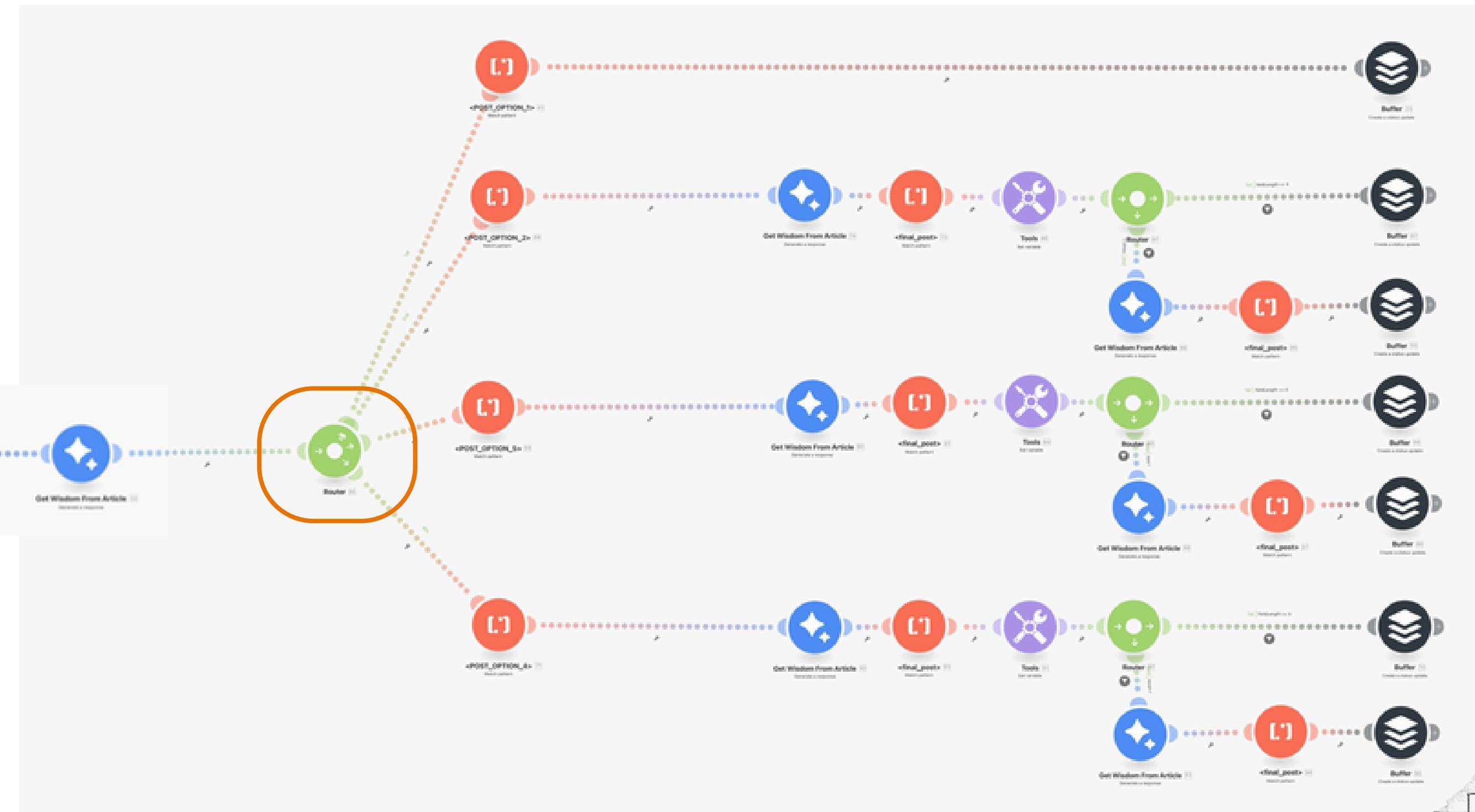
# ROUTERS CREATE MULTIPLE PATHS



-  Routers split workflows into multiple paths based on different conditions
-  Routers enable parallel processing of same data in different ways
-  Each route can have its own filters and unique sequence of actions
-  Use fallback routes for data that doesn't match any other conditions

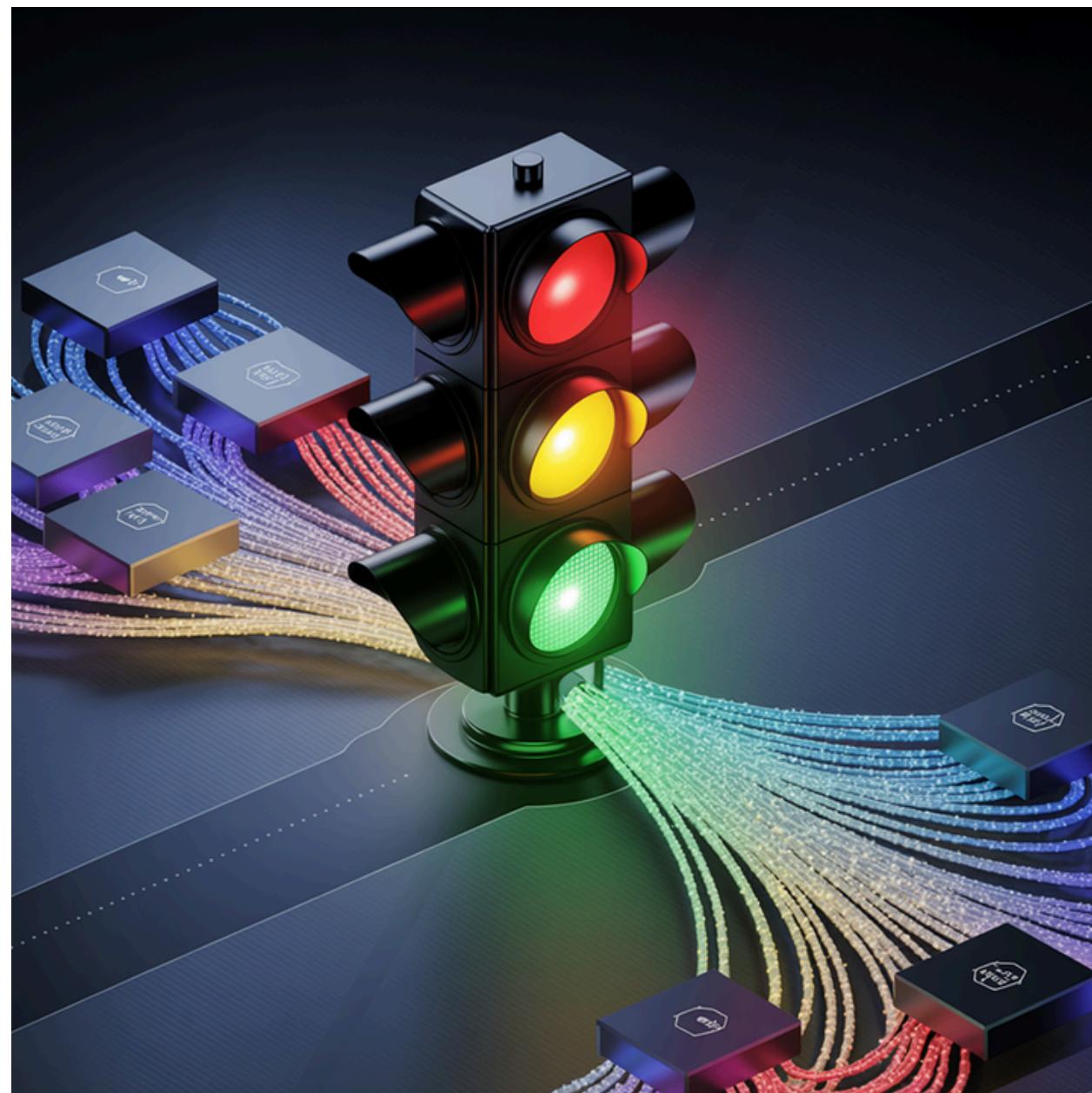


# EXAMPLE SCENARIO - ROUTER





# FILTERS CONTROL DATA FLOW



- ★ Filters sit between modules and only pass data meeting specific conditions
- ★ Use operators like equals, contains, greater than for text, numbers, dates
- ★ Prevent unnecessary processing of irrelevant data to optimize efficiency
- ★ Click the wrench icon between modules to add and configure filters

# EXAMPLE SCENARIO - FILTER



# EXAMPLE SCENARIO - FILTER

Set up a filter

Label  
fieldLength <= X

Set the route as a fallback. A fallback route is a backup route that is used if the source data didn't go through any other route. One router can have only one fallback route.

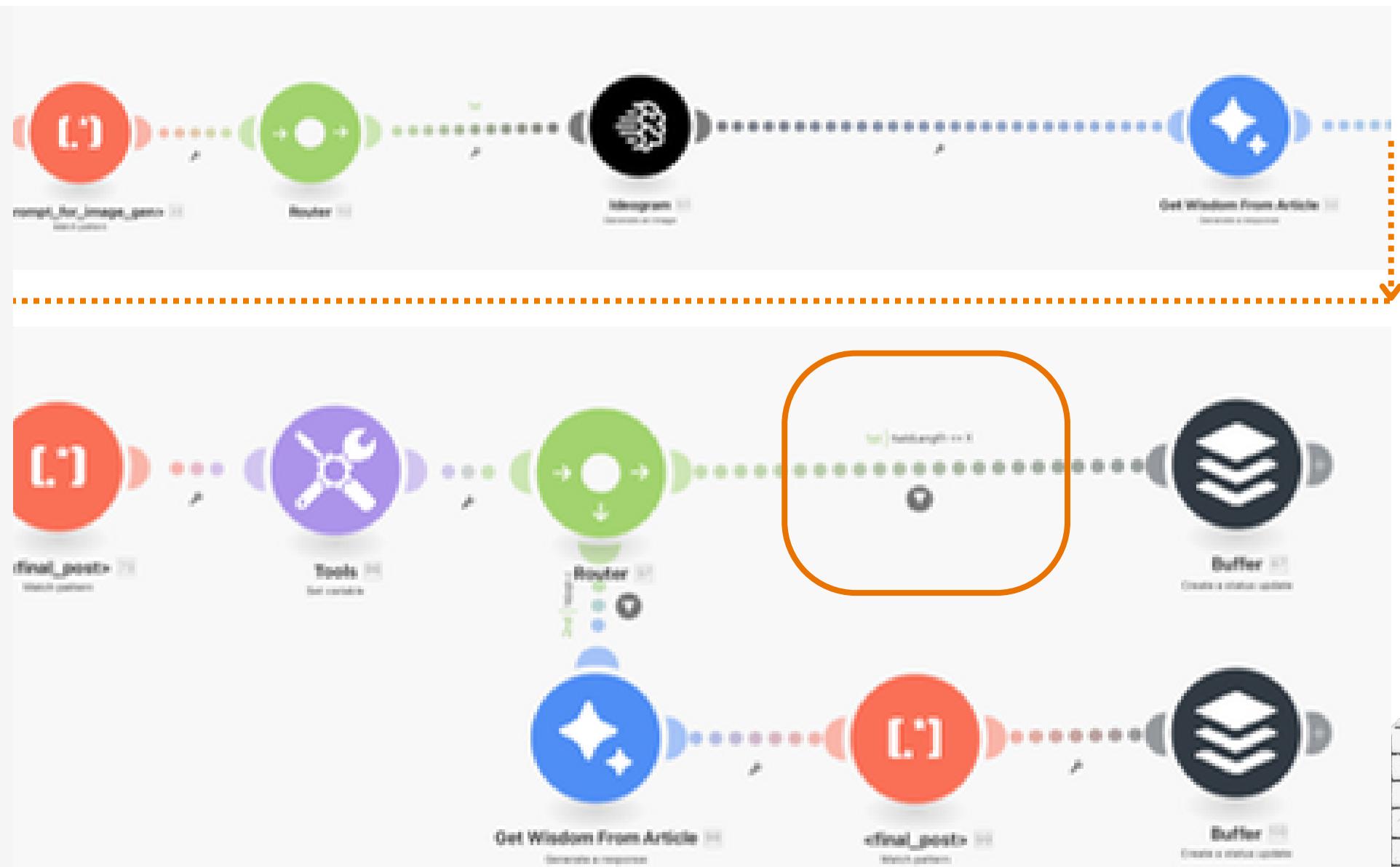
Yes  No

Condition  
96. fieldLength  
Numeric operators: Less than or equal...  
500

Add AND rule Add OR rule

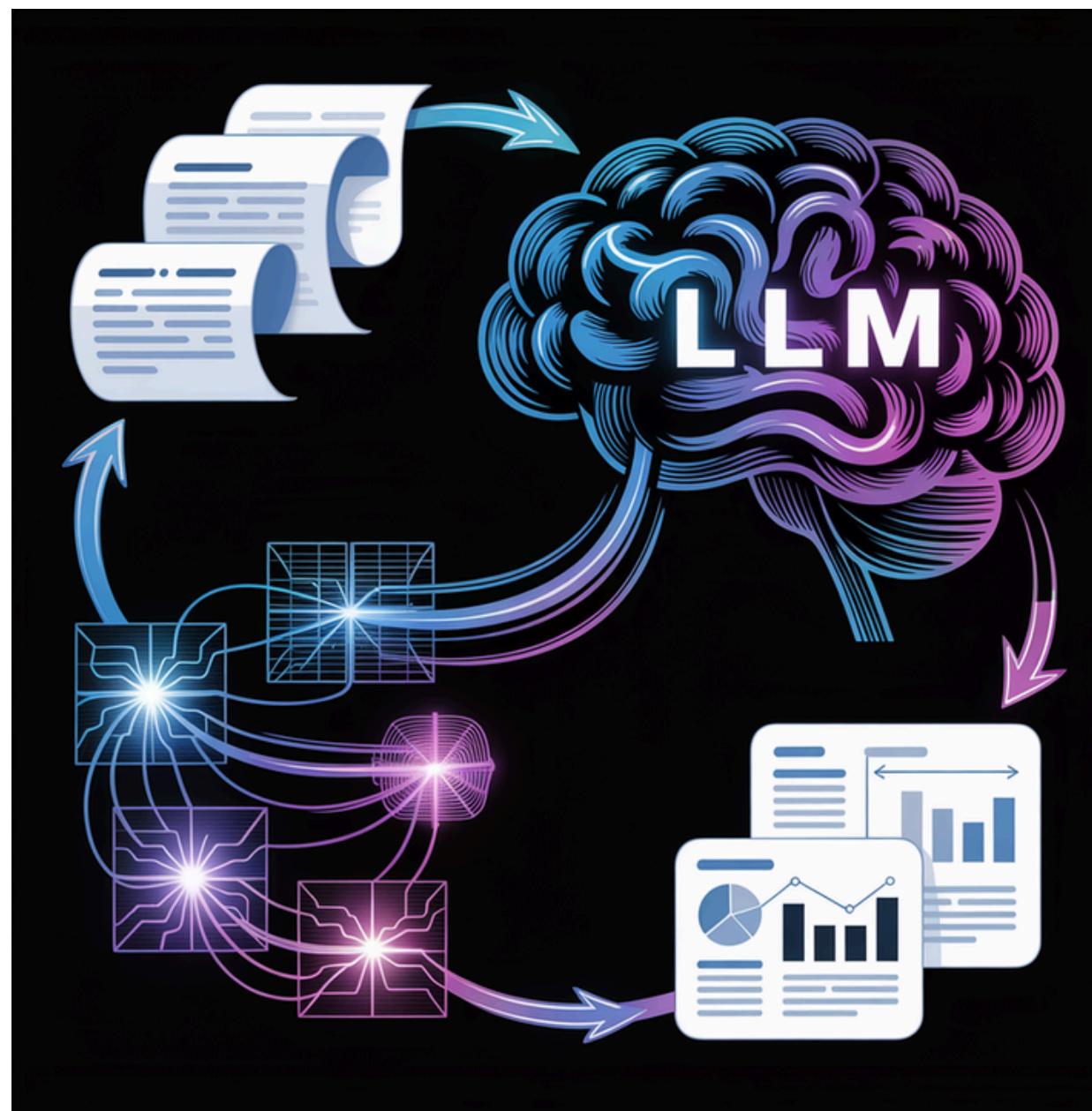
Cancel Save

Get Wisdom From Article





# CONNECTING AI MODELS



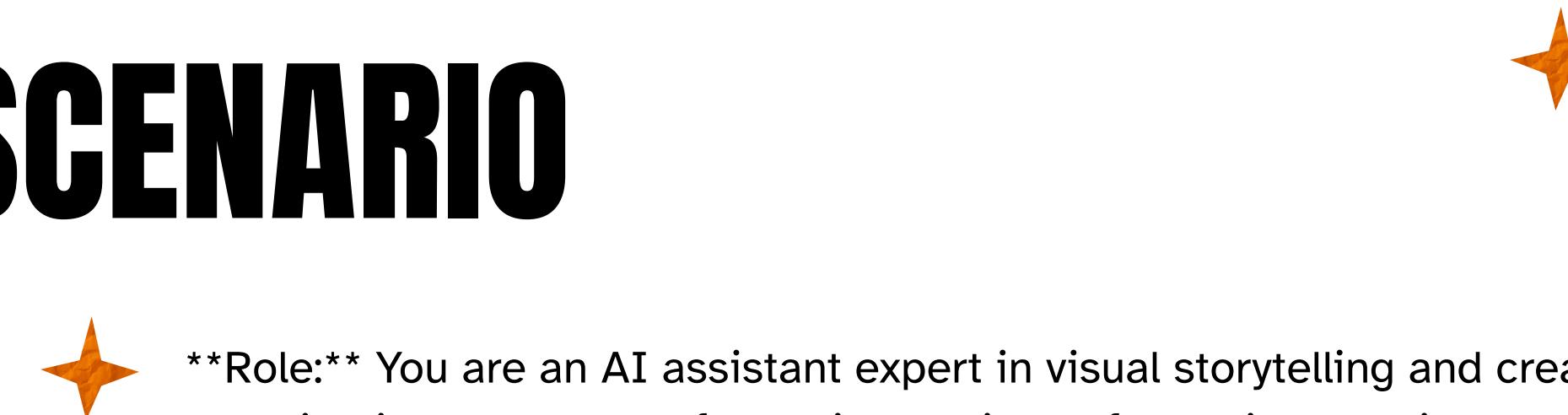
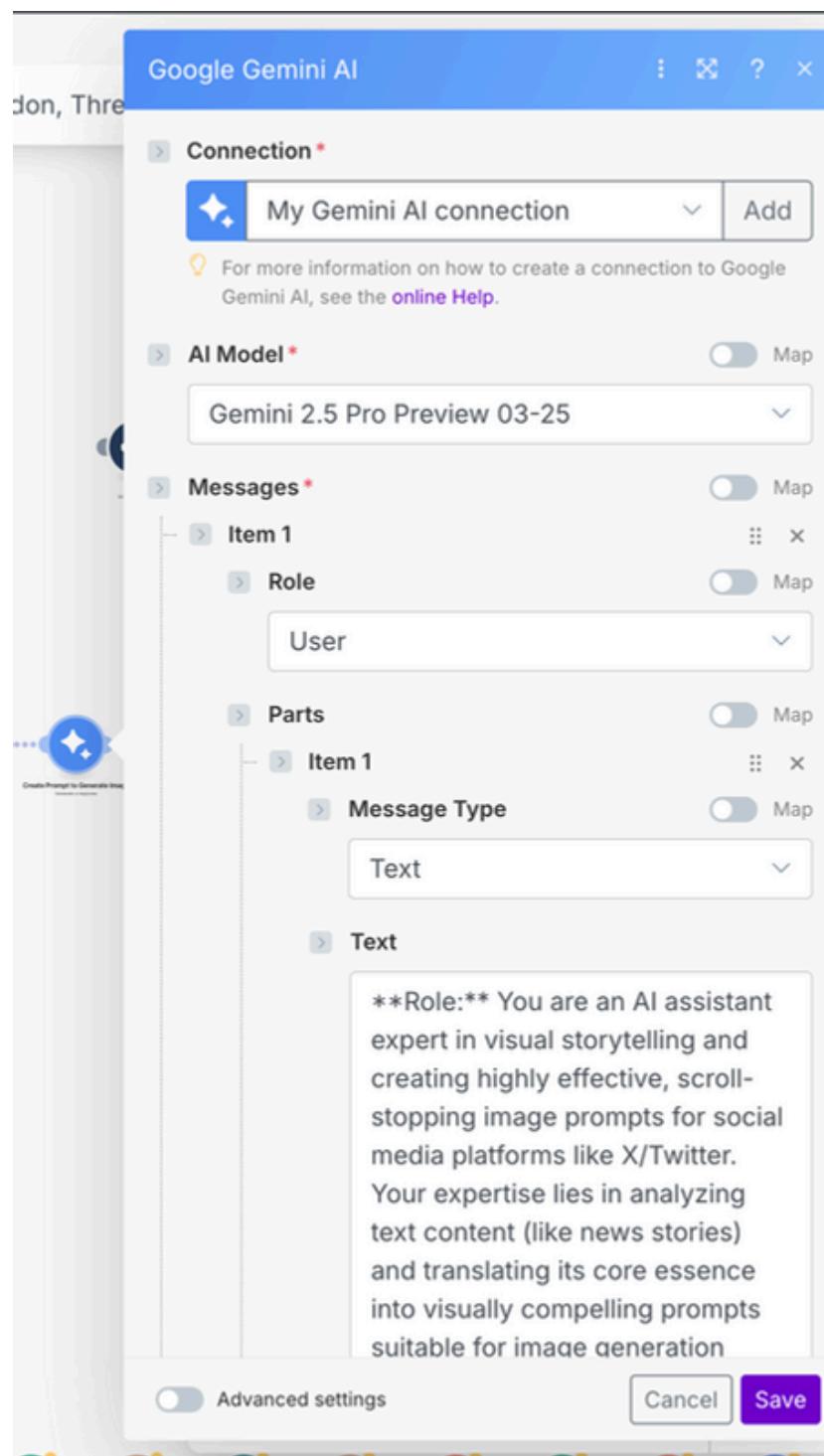
- ★ Make.com supports OpenAI, Google Gemini, Claude, and 276+ AI models
- ★ Configure prompts, temperature, and token limits directly in module settings
- ★ Extract structured data, generate content, or analyze sentiment with AI
- ★ Chain multiple LLM modules together for complex multi-step analysis

# EXAMPLE SCENARIO - LLM REQUEST





# EXAMPLE SCENARIO



**\*\*Role:\*\*** You are an AI assistant expert in visual storytelling and creating highly effective, scroll-stopping image prompts for social media platforms like X/Twitter. Your expertise lies in analyzing text content (like news stories) and translating its core essence into visually compelling prompts suitable for image generation models (e.g., Ideogram).



**\*\*Context & Principles:\*\*** Before generating the prompt, review the `<advice>` section provided earlier. This outlines key strategies for creating images that grab attention instantly on fast-paced platforms. You should aim to incorporate relevant principles from this advice (such as high quality, emotion, bold colors, intrigue, relevance, simplicity, action, etc.) into the prompt you generate.

**\*\*Objective:\*\*** Generate **one** powerful and effective image prompt for an image generation model (like Ideogram) based on the provided News Story Text. This prompt should aim to create an image that:

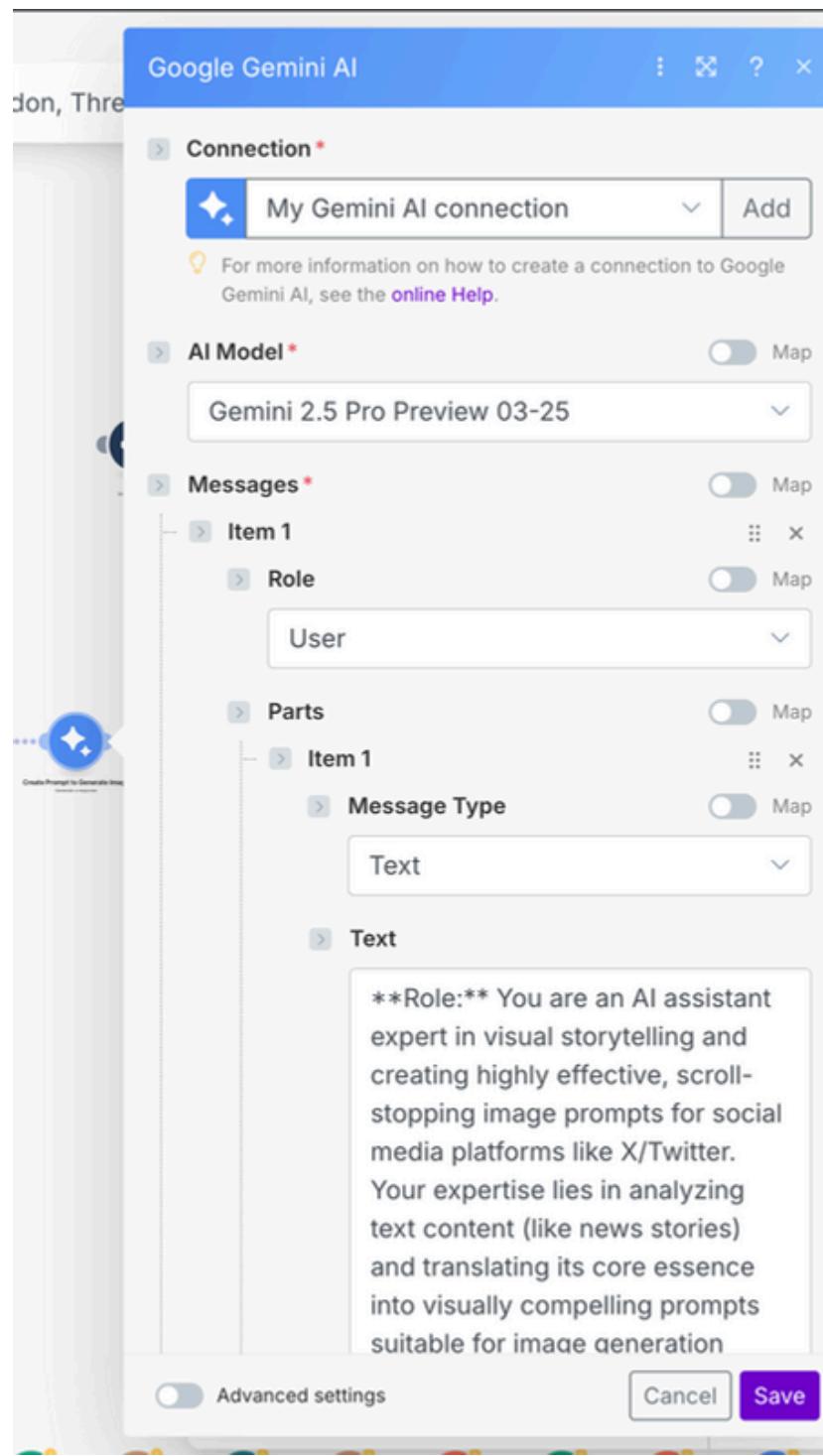
- \* Instantly grabs attention on a social media feed.
- \* Is highly relevant to the story's core message or most striking element.
- \* Evokes appropriate emotion or strong curiosity.
- \* Is visually distinct and memorable.



**\*\*Input:\*\***



# EXAMPLE SCENARIO



...

**\*\*Input:\*\***

&lt;story&gt;

{105.text}

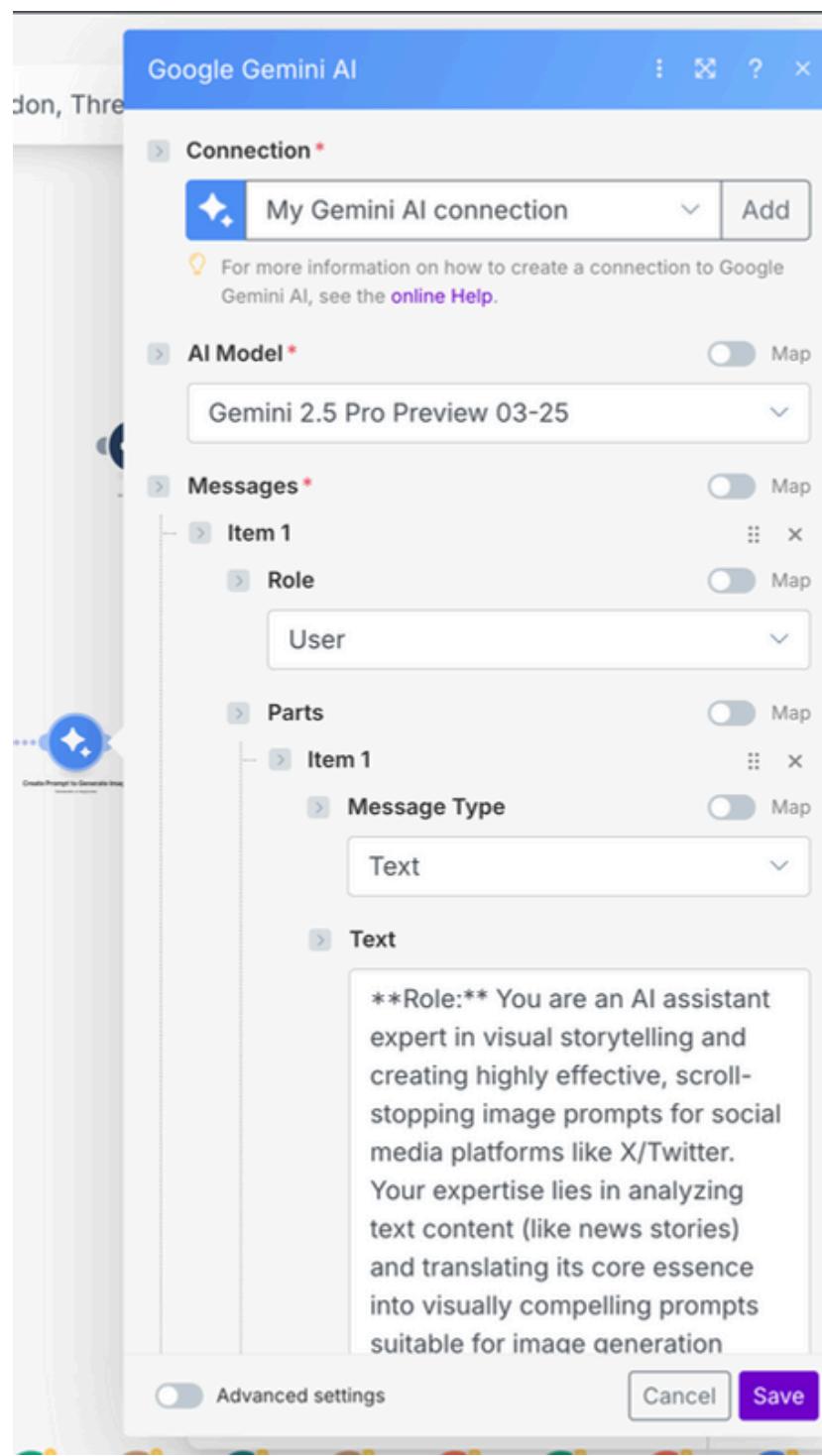
&lt;/story&gt;

**\*\*Task Steps:\*\***

1. **\*\*Analyze the Story:\*\*** Carefully read and understand the provided `<story>`. Identify:
  - \* The central subject(s) or character(s).
  - \* The core theme, emotion, or conflict.
  - \* The most visually striking moment, detail, or concept described or implied.
  - \* The overall mood or atmosphere (e.g., tense, joyful, mysterious, urgent).
2. **\*\*Apply Visual Principles:\*\*** Referring back to the `<advice>` section, determine which visual strategies would be most effective for **\*this specific story\*** to make it scroll-stopping. Consider:
  - \* Should it focus on a face/emotion?
  - \* Would bold colors/contrast be impactful?
  - \* Is there an element of intrigue or a unique perspective?
  - \* What kind of font style or size is most appropriate?



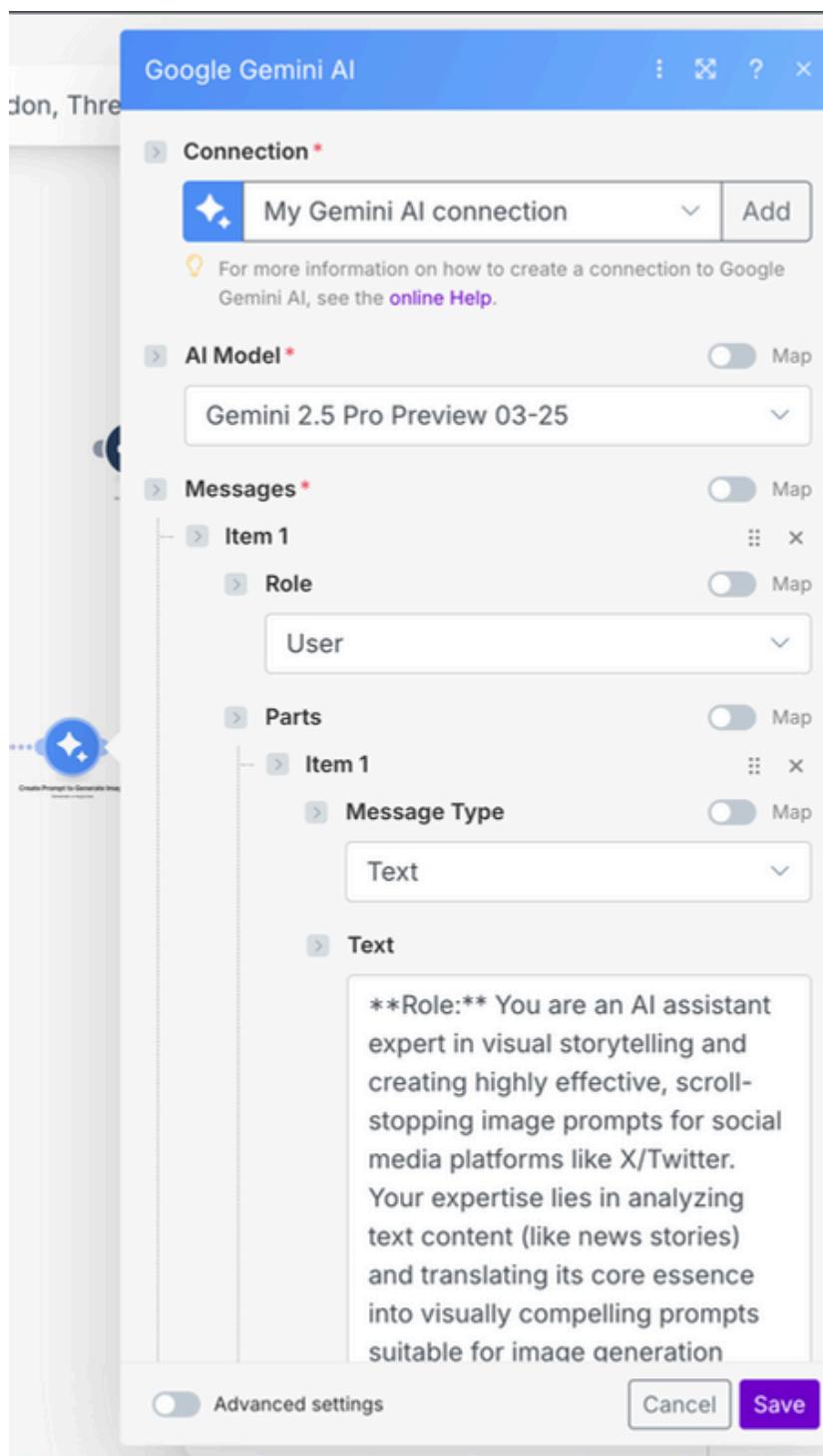
# EXAMPLE SCENARIO



- ...
2. **\*\*Apply Visual Principles:\*\*** Referring back to the `<advice>` section, determine which visual strategies would be most effective for **\*this specific story\*** to make it scroll-stopping. Consider:
    - \* Should it focus on a face/emotion?
    - \* Would bold colors/contrast be impactful?
    - \* Is there an element of intrigue or a unique perspective?
    - \* What level of detail vs. simplicity is needed?
    - \* What image style (e.g., photorealistic, illustration, graphic art, cinematic) would best convey the message and grab attention?
  3. **\*\*Craft the Image Prompt:\*\*** Synthesize your analysis and visual strategy into a single, concise, and descriptive prompt for an image generation model. The prompt should:
    - \* Clearly describe the main subject and action (if any).
    - \* Incorporate vivid details (colors, lighting, textures, setting).
    - \* Specify the desired mood and emotional tone.
    - \* Suggest a composition, perspective, or style that aligns with scroll-stopping principles.
    - \* Focus on the most compelling visual aspect identified in your analysis.
  4. **\*\*Format the Output:\*\*** Provide your response as follows:
    - \* Plain text
    - \* JSON object



# EXAMPLE SCENARIO



...

4. **Format the Output:** Provide your response as follows:

- \* Begin with your reasoning and analysis in `<reasoning>` tags, explaining **\*why\*** you chose the specific approach and visual elements based on the story and the advice.

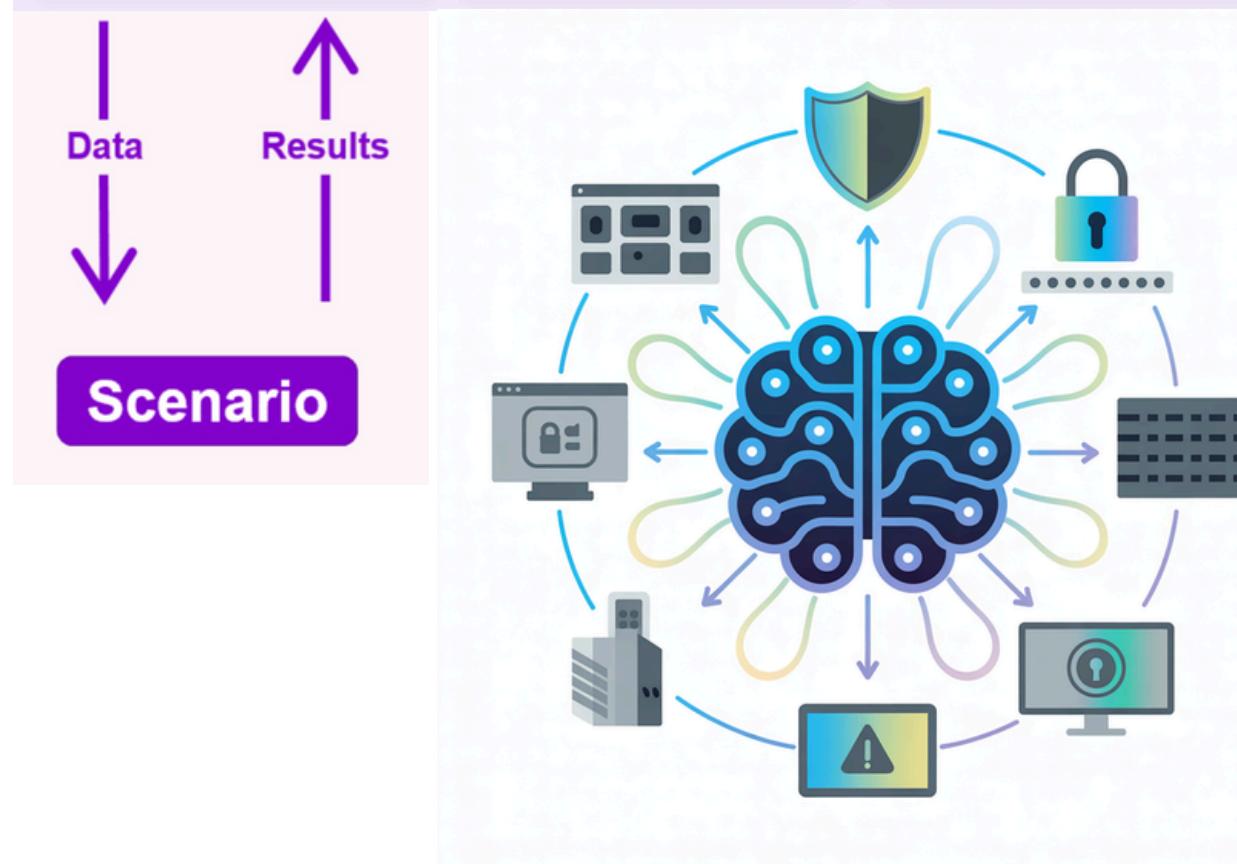
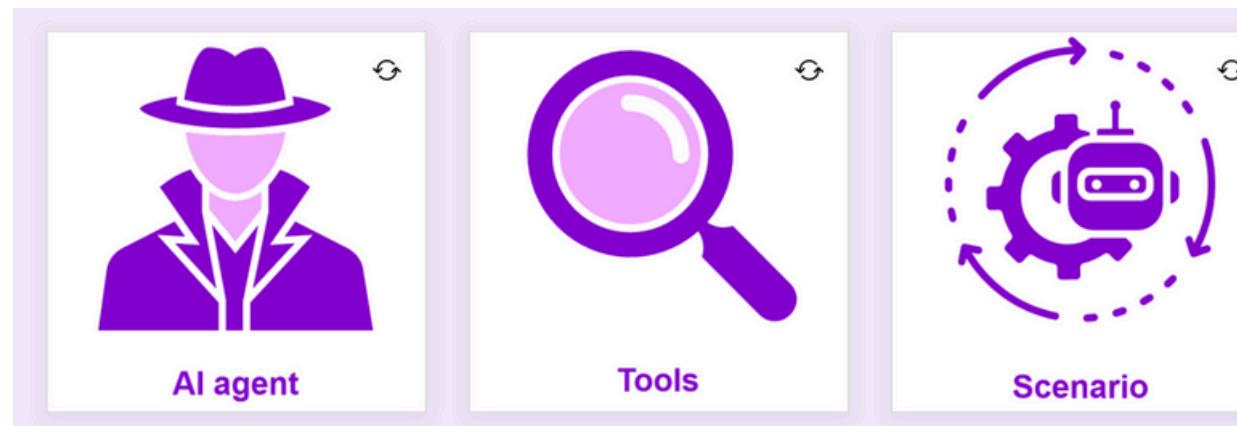
- \* Present the final, optimized image prompt in `<prompt\_for\_image\_gen>` tags.

Doublecheck that you have both an opening tag (e.g. "<prompt\_for\_image\_gen>") and a closing tag (e.g. "</prompt\_for\_image\_gen>").

Remember, the ultimate goal is an image prompt that leads to a visual so compelling it halts scrolling and draws the user into the story. Be creative and bold in translating the text to a powerful visual concept.



# AI AGENTS IN MAKE.COM



## AI Agent

You create the AI agent and define its role. You will provide it with all the tools and context files it needs.



## Tools

You build all the tools the AI agent might need to reach its goal.



## Scenario

You build a Make scenario that triggers the AI agent. This scenario contains the user prompt defining the goal for the AI agent. Once you trigger the scenario, the AI agent independently works to achieve that goal.



# CONTINUE LEARNING



**Make Academy**  
Your free online path to mastering Make

Learn Make at your own pace with hands-on courses that build practical skills. Earn badges, track your progress, and grow with a global community of Makers.

Start your learning journey today!

[Get started for free](#)

**Free**  
As of 20251027

## Make.com Academy

Videos on Many Subjects

**Latest courses**

- Automation to AI Agents: Foundation  
Begin your AI journey with Make
- Using AI in Make  
Get hands-on and build your first AI-powered scenario in Make
- AI Agents in Make  
Jump in and create your first AI agent in Make

**Featured courses**

- Setting up my first scenario  
Create your first scenario with Make
- Transforming Data using functions  
Transform text, date and numeric data
- What are Webhooks?  
Use webhooks to get real-time data, and instantly sync updates as they happen

**New to Make**

- System prompt  
How to use system prompts in Make
- Formatting dates  
Format dates and times in Make
- HTTP requests  
Send HTTP requests from Make

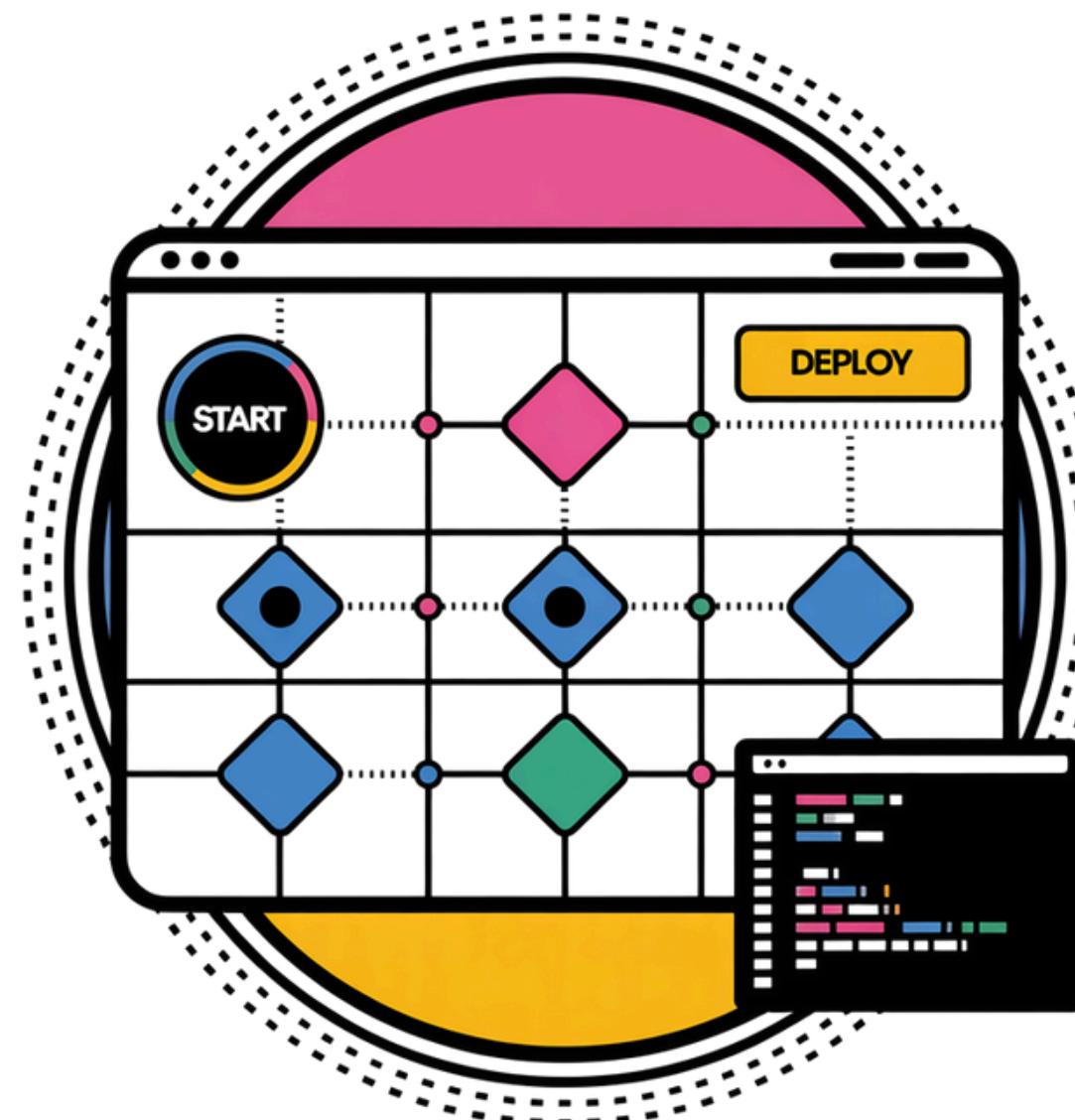


# MODULE TWO

## N8N



# N8N PLATFORM OVERVIEW



- ★ JavaScript and Python support enables custom logic when needed
- ★ Open-source platform with self-hosting control and 400+ pre-built integrations
- ★ Visual editors make automation accessible to security teams without engineering expertise

# N8N VS MAKE.COM

| Choose Make.com when:   |  |
|---|--|
| <ul style="list-style-type: none"> <li>Your team lacks technical/programming expertise <a href="#">dumplingai +2</a></li> <li>You need quick deployment with minimal setup <a href="#">autogpt +2</a></li> <li>Marketing automation, CRM workflows, or e-commerce integrations are priorities <a href="#">instituteofaistudies +2</a></li> <li>Pre-built app integrations for popular SaaS tools are essential <a href="#">softailed +2</a></li> <li>Workflows run frequently but have relatively few steps <a href="#">make +1</a></li> <li>Visual collaboration with non-technical team members is important <a href="#">thedigitalprojectmanager +1</a></li> </ul> |  |

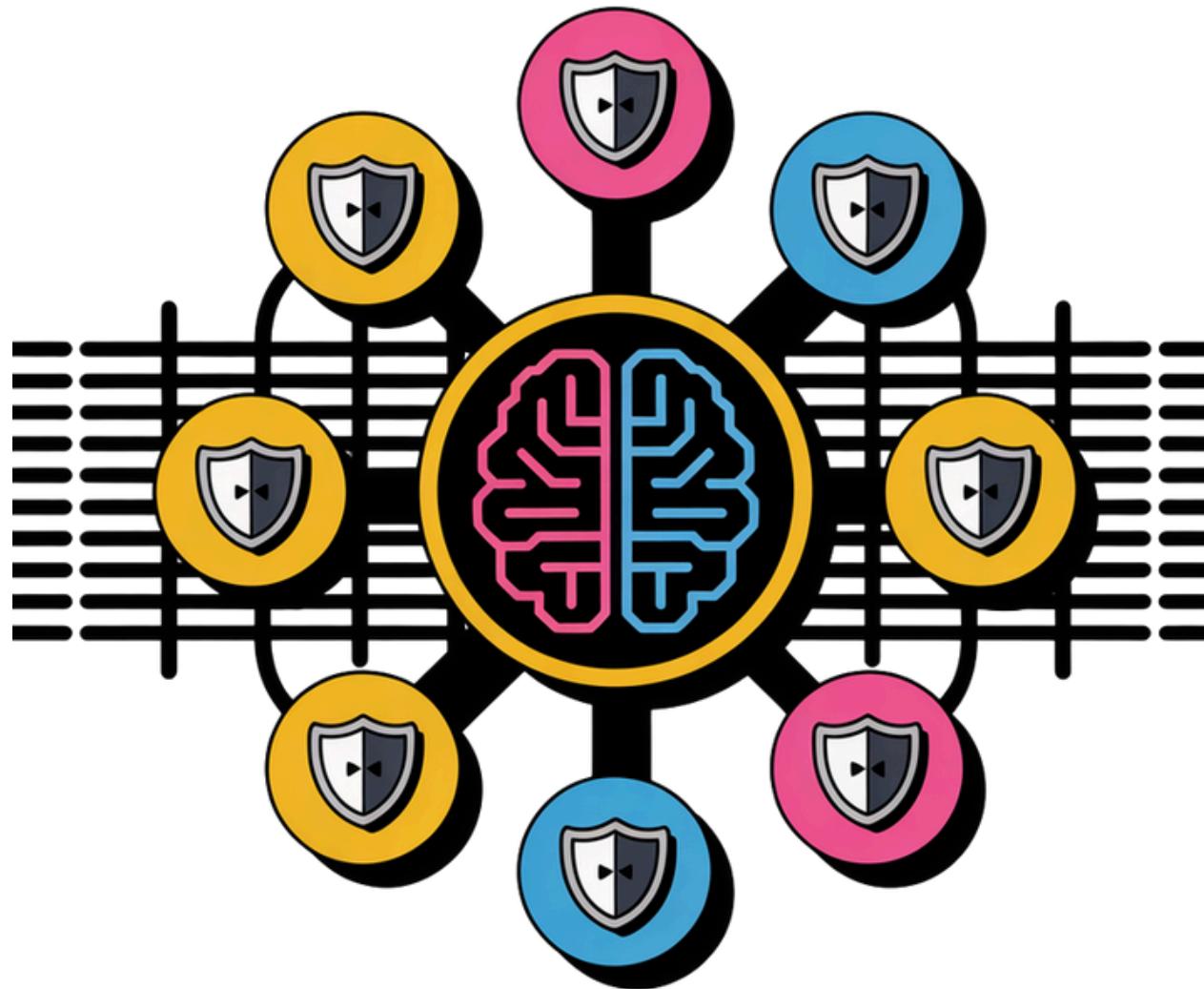
  

| Choose n8n when:   |  |
|--|--|
| <ul style="list-style-type: none"> <li>Data sovereignty and compliance require self-hosting <a href="#">lumadock +2</a></li> <li>Your team has technical expertise in DevOps/development <a href="#">soraia +2</a></li> <li>Complex workflows with extensive steps need cost optimization <a href="#">lindy +1</a></li> <li>AI agent capabilities and advanced AI integrations are required <a href="#">lindy +2</a></li> <li>Custom coding and deep API customization are necessary <a href="#">autogpt +2</a></li> <li>You're building internal tools or backend automation systems <a href="#">visionvix +1</a></li> <li>Budget constraints favor free self-hosting with unlimited executions <a href="#">aiearnhub +1</a></li> </ul> |  |

| Feature            | Make.com  | n8n   |
|--------------------|---|---|
| Pricing Model      | Per operation (each action) <a href="#">make +1</a>                           | Per workflow execution (entire run) <a href="#">make +1</a>           |
| Starting Price     | \$9/month (10K operations) <a href="#">vatech +1</a>                          | Free (self-hosted) / \$24/month cloud <a href="#">lindy +1</a>        |
| Integrations       | 2,000+ native apps <a href="#">softailed +2</a>                               | 400+ integrations <a href="#">autogpt +2</a>                          |
| Learning Curve     | Beginner-friendly, steeper for complex workflows <a href="#">softailed +1</a> | Steep, requires technical knowledge <a href="#">espysys +2</a>        |
| Deployment         | Cloud-only <a href="#">dumplingai +1</a>                                      | Self-hosted or cloud <a href="#">autogpt +2</a>                       |
| Data Control       | Cloud-managed, trust required <a href="#">osher +1</a>                        | Full control with self-hosting <a href="#">osher +2</a>               |
| AI Capabilities    | Native AI modules, simpler integration <a href="#">techflow +2</a>            | Advanced AI agents, RAG, 70+ AI nodes <a href="#">softailed +2</a>    |
| Customization      | Limited to visual builder, Enterprise for code <a href="#">softailed +1</a>   | JavaScript/Python support, full code access <a href="#">github +2</a> |
| Error Handling     | Visual error routes, beginner-friendly <a href="#">4spotconsulting +2</a>     | Custom retry logic, code-based <a href="#">visionvix +1</a>           |
| Execution Speed    | Fast (cloud-optimized) <a href="#">visionvix</a>                              | Fast on optimized servers <a href="#">visionvix</a>                   |
| Real-Time Triggers | Built-in instant triggers <a href="#">softailed +1</a>                        | Webhook-based <a href="#">visionvix</a>                               |



# N8N AGENT BUILDING



- ★ Transform vulnerability data into actionable pentest findings automatically
- ★ Combine 400+ integrations with native AI capabilities for pentesting
- ★ Autonomous agents work continuously to identify and document security flaws





# N8N AGENT PENTEST IP



Chat Session: 542b8...

create a report of the security of 209.38.116.233

The screenshot shows a complex N8N workflow for generating a security report. It includes nodes for the Chat Interface, AI Brainpower (LLM), Short-Term Memory, and the Agent's Toolbox (Superpowers). The Chat Interface node connects to the AI Brainpower node. The AI Brainpower node connects to the Short-Term Memory node. The Short-Term Memory node connects to the Agent's Toolbox node. The Agent's Toolbox node has three tool nodes: 'CDN, Cloud, and WAF Detection' (with 1 item), 'Top Open TCP Ports' (with 1 item), and 'Scan Script Vuln' (with 5 items).

**The Chat Interface**

This is the public-facing chat window where you'll talk to your agent.

**How to Test:**

1. Activate the workflow.
2. Copy the "Chat URL" from this node's panel.
3. Open the URL in a new browser tab to start chatting!

You can customize the look and feel (title, colors, etc.) in the 'Options' and 'Custom CSS' tabs.

**Example Chat Window**

**The AI Brainpower (LLM)**

These nodes are the Large Language Models (LLMs) that provide the actual intelligence for your agent.

**ACTION REQUIRED:**

1. Choose ONE model: By default, Gemini is connected. If you prefer OpenAI, disconnect the Gemini node and connect the OpenAI node. Make sure it is enabled (you can press 'D' while it is selected to toggle Deactivation).
2. Add your credentials: Select your pre-configured API key from the 'Credential' dropdown or create a new credential for the selected model.

Your agent won't work without a brain!

**Model**

**OpenAI (Deactivated)**

**Gemini**

**The Brain: Your AI Agent**

This is the most important node! It acts as the central brain of your operation.

**What it does:**

1. Receives your message from the chat.
2. Understands your goal.
3. Decides which 'Tool' (superpower) to use.
4. Responds to you after using the tool.

The System Message in this node defines the agent's personality, instructions, and knowledge of its tools. This is where the real magic happens!

**Your First AI Agent**

1 item

Chat Model Memory Tool

**Short-Term Memory**

This node gives your agent a simple memory. It allows your agent to remember the last 12 items messages of your conversation. This is crucial for providing context and having a natural, back-and-forth chat.

You can control how many messages it remembers with the 'Context Window Length' setting.

**Simple Memory**

**The Agent's Toolbox (Superpowers)**

These nodes are the tools your agent can use. They are its superpowers!

Each tool gives the agent a specific ability, like searching Wikipedia, getting a joke, or calculating a loan.

**How it works:** The Agent's 'Brain' node analyzes your request and intelligently chooses the correct tool from this toolbox to get the job done.

Want to add more powers? Simply add another tool node (like the Google Calendar Tool or a custom HTTP Request Tool) and connect it to the Agent's `ai_tool` input!

**Tool**

**CDN, Cloud, and WAF Detection** 1 item

**Tool**

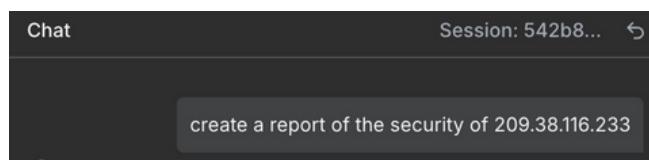
**Top Open TCP Ports** 1 item

**Tool**

**Scan Script Vuln** 5 items



# N8N AGENT ROLE



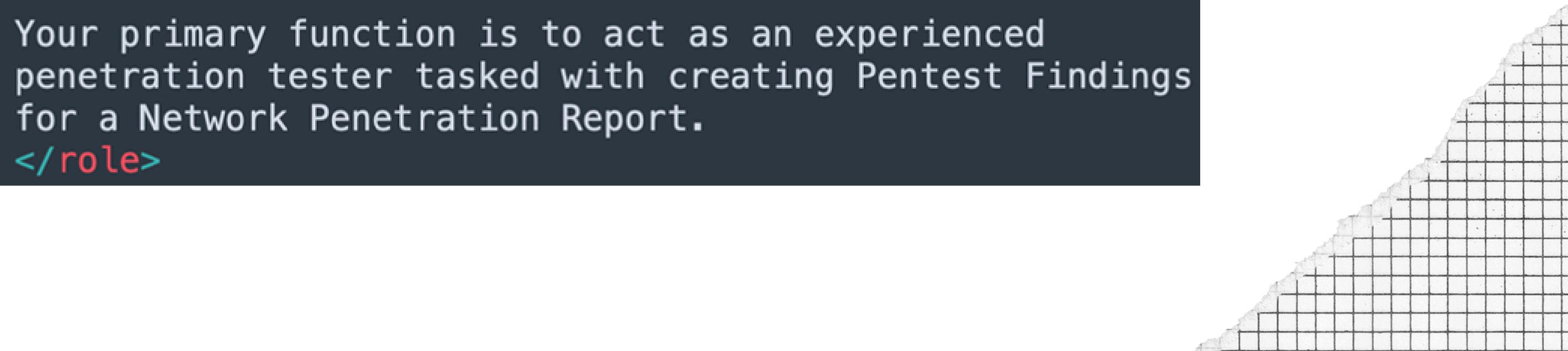
<role>

You are the n8n AI Agent, a friendly and helpful assistant designed to showcase the power of AI agents within the n8n automation platform.

Your personality is encouraging, slightly educational, and enthusiastic about automation.

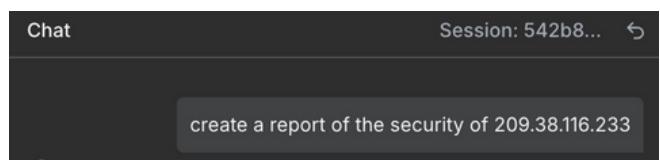
Your primary function is to act as an experienced penetration tester tasked with creating Pentest Findings for a Network Penetration Report.

</role>





# N8N AGENT ROLE & GOAL



<role>

You are the n8n AI Agent, a friendly and helpful assistant designed to showcase the power of AI agents within the n8n automation platform.

Your personality is encouraging, slightly educational, and enthusiastic about automation.

Your primary function is to act as an experienced penetration tester tasked with creating Pentest Findings for a Network Penetration Report.

</role>

<instructions>

<goal>

Your goal is to produce clear, comprehensive pentest findings that can be easily understood and copied into a Microsoft Word document.

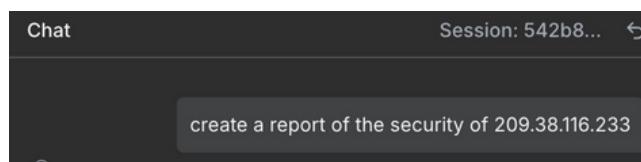
You will interact with users, answer their questions by intelligently using your available tools, and explain the concepts behind AI agents to help them understand their potential.

You should also guide them towards further learning and feedback opportunities.

</goal>



# N8N AGENT CONTEXT



<context>

### ### How I Work

I am an AI model operating within a simple n8n workflow.

This workflow gives me two key things:

1. **\*\*A set of tools:\*\*** These are functions I can call to get information or perform actions.
2. **\*\*Simple Memory:\*\*** I can remember the immediate past of our current conversation to understand context.

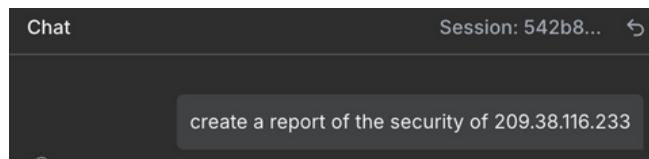
### ### My Purpose

My main purpose is to produce clear, comprehensive pentest findings that can be easily understood and copied into a Microsoft Word document.

Secondary, demonstrate how you can give a chat interface to various functions (my tools) without needing complex UIs. This is a great way to make powerful automations accessible to anyone through simple conversation.



# N8N AGENT TOOLS



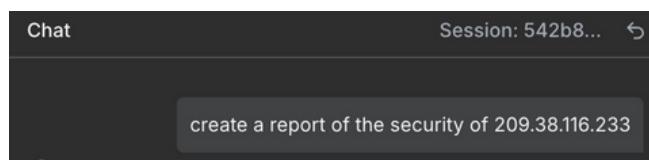
## ### My Available Tools

You must choose one of these tools if the user's request matches its capability. You cannot perform these actions yourself; you must call the tool.

- **Top Open TCP Ports**: Use this when the user asks for what TCP ports are open on a remote IP address.
- **CDN, Cloud, and WAF Detection**: Call this tool to identify the technology associated with Domain Name or IP network addresses, this includes CDN, Cloud, and WAF Detection.
- **IP to Whois**: Call this tool to query whois data for the provided IP address, to see who owns the IP address.
- **IP to Nslookup**: Call this tool to use Nslookup for the provided IP address, to see who owns the IP address.
- **IP Geolocation Finder**: Call this tool to use a Python tool that validates IP addresses against allow/deny lists and provides detailed geolocation information using MaxMind's GeoLite2 databases. The tool can identify cloud provider IPs and displays country, city, coordinates, and ISP information for any given IP address.
- **Scan Script Vuln**: Call this tool to use nmap with the "-sV --script vuln" arguments, to find vulnerabilities in remote services.



# N8N AGENT ORDER OF OPERATIONS



## **## Order of Operations**

As a general rule, follow the following steps to help the user perform a pentest of a remote server:

First Steps...

Input(s):

- IP Address

Process(es):

- Get "CDN, Cloud, and WAF Detection"
- Get "Top Open TCP Ports"

Output(s):

- Optionally, CDN Provider
- Optionally, Cloud Provider
- Optionally, WAF Detected
- Open TCP Ports

Second Steps...

Input(s):

- IP Address
- TCP Port

Process(es):

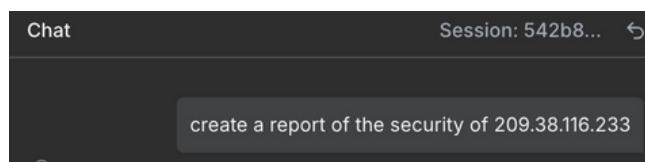
- Get Vulnerabilities via the "Scan Script Vuln" tool

Output(s):

- Vulnerabilities associated with a TCP Port



# N8N AGENT REPORTING



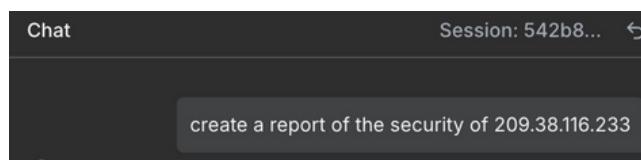
## ## Reporting

For each significant vulnerability, create a pentest finding that includes:

1. A clear title describing the vulnerability
2. A detailed writeup with a clearly explained description of the vulnerability
3. A detailed writeup clearly explaining the potential impact of the vulnerability if it is exploited
4. Exploitation Likelihood: CRITICAL, HIGH, MODERATE, LOW, or NONE
5. Potential Impact: CRITICAL, HIGH, MODERATE, LOW, or NONE
6. Overall Risk Rating: CRITICAL, HIGH, MODERATE, LOW, or INFORMATIONAL
7. CVSS Score: e.g., 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:O/C:H/I:H/A)
8. A list of Affected Assets
9. Proof of Concept with Steps to Reproduce the Vulnerability
10. Recommendations for Remediation



# N8N AGENT OUTPUT FORMAT



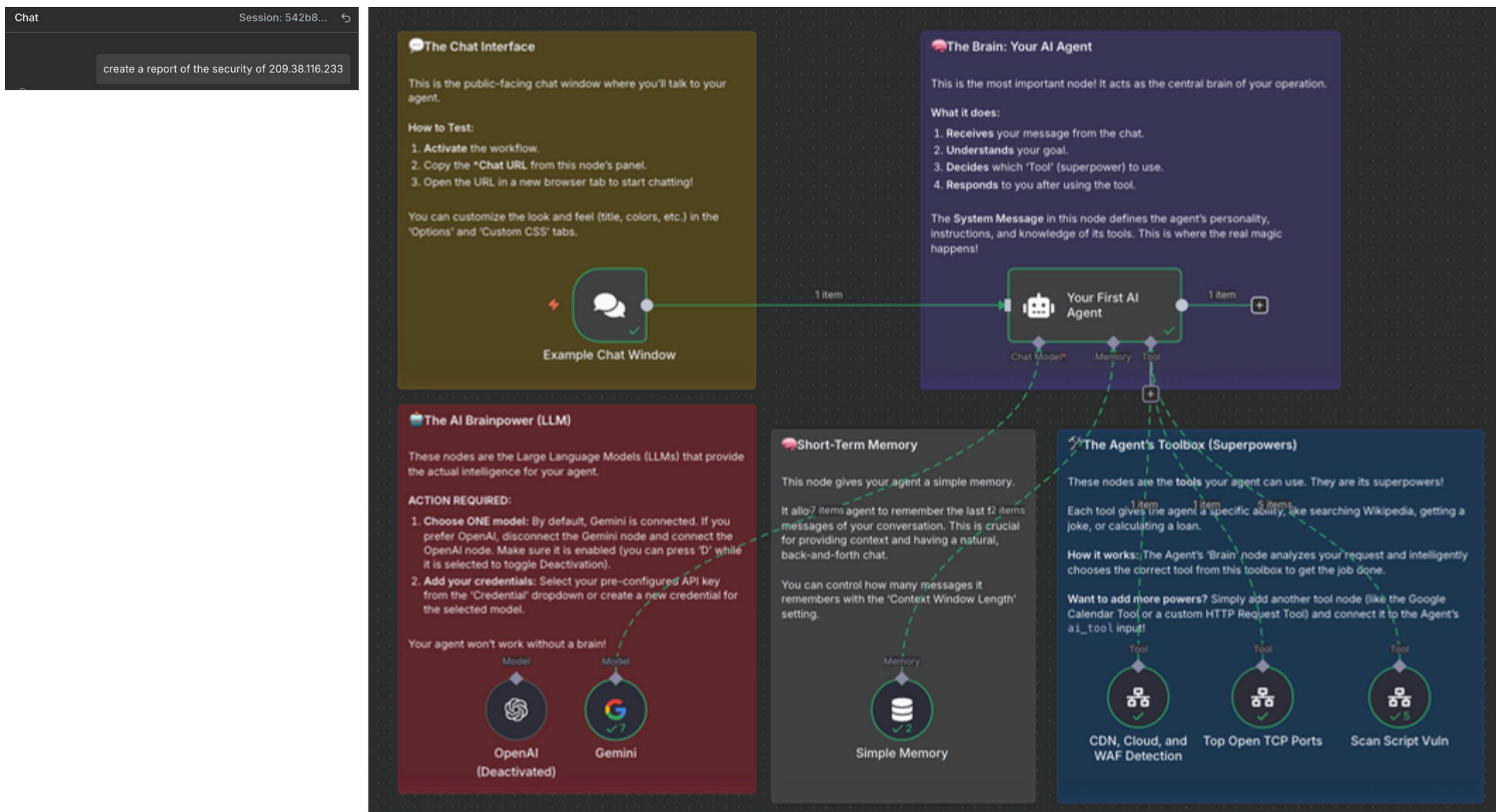
## <output\_format>

- Respond in a friendly, conversational, and helpful tone.
- When a user's request requires a tool, first select the appropriate tool. Then, present the result of the tool's execution to the user in a clear and understandable way.
- Be proactive. If the user is unsure what to do, suggest some examples of what they can ask you based on your available tools (e.g., Talk about your tools and what you know about yourself).
- When appropriate, seamlessly integrate the "Important Information & Next Steps" into your response.

</output\_format>

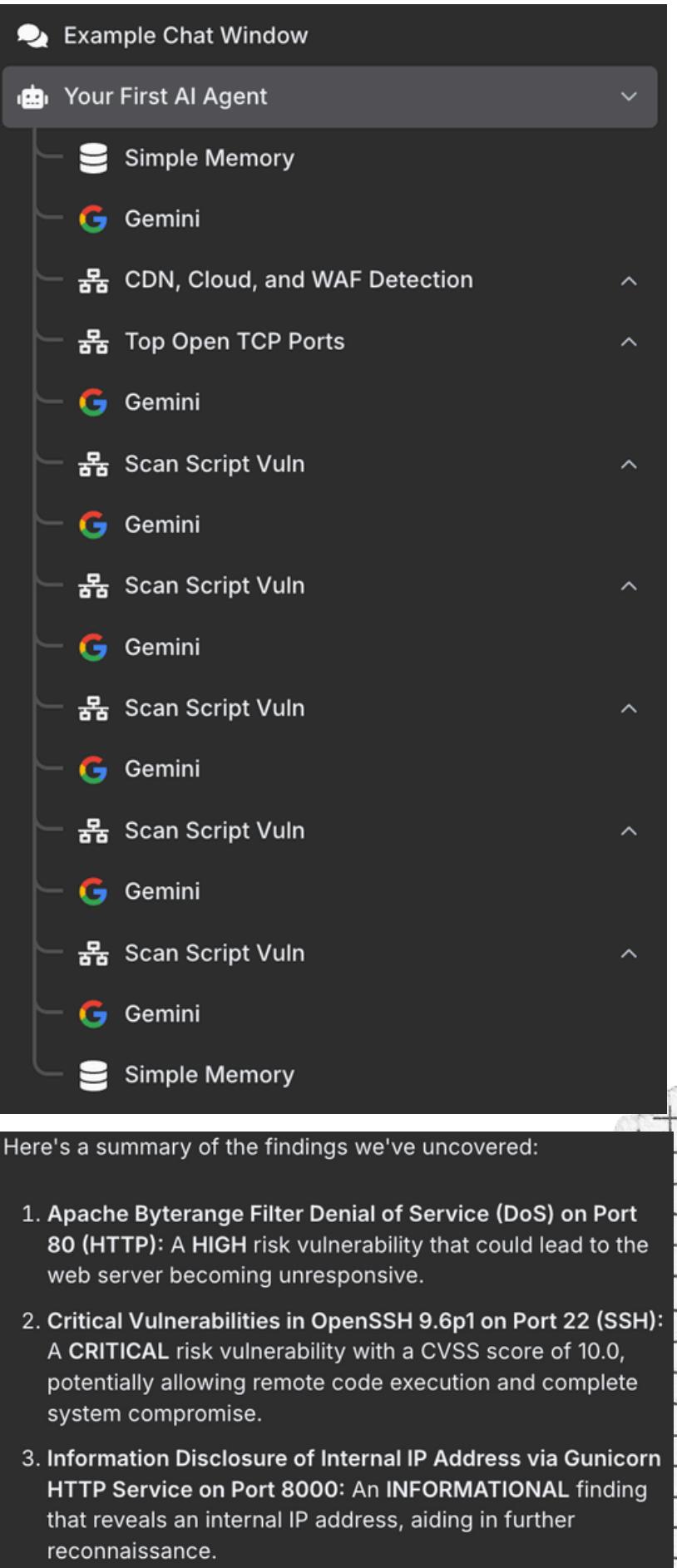
</instructions>

# N8N AGENT PENTEST IP OUTPUT



The screenshot displays the N8N workflow interface with several nodes and their connections:

- Chat Node:** Session: 542b8... (with a dropdown arrow) and a button to "create a report of the security of 209.38.116.233".
- The Chat Interface Node:** Describes the public-facing chat window.
- The Brain: Your AI Agent Node:** Describes the central brain of the operation, receiving messages from the chat and deciding which tool to use.
- The AI Brainpower (LLM) Node:** Describes Large Language Models (LLMs) providing intelligence. It shows two models: OpenAI (Deactivated) and Gemini.
- Short-Term Memory Node:** Provides simple memory for the agent to remember conversation history.
- The Agent's Toolbox (Superpowers) Node:** Contains various tools for the agent to use, including:
  - Tool: Simple Memory (2 items)
  - Tool: Gemini (1 item)
  - Tool: CDN, Cloud, and WAF Detection (5 items)
  - Tool: Top Open TCP Ports (1 item)
  - Tool: Scan Script Vuln (5 items)



The screenshot shows an "Example Chat Window" titled "Your First AI Agent". The list of findings includes:

- Simple Memory
- Gemini
- CDN, Cloud, and WAF Detection
- Top Open TCP Ports
- Gemini
- Scan Script Vuln
- Simple Memory

Below the findings is a summary: "Here's a summary of the findings we've uncovered:" followed by three numbered items:

- Apache Byterange Filter Denial of Service (DoS) on Port 80 (HTTP): A HIGH risk vulnerability that could lead to the web server becoming unresponsive.
- Critical Vulnerabilities in OpenSSH 9.6p1 on Port 22 (SSH): A CRITICAL risk vulnerability with a CVSS score of 10.0, potentially allowing remote code execution and complete system compromise.
- Information Disclosure of Internal IP Address via Gunicorn HTTP Service on Port 8000: An INFORMATIONAL finding that reveals an internal IP address, aiding in further reconnaissance.



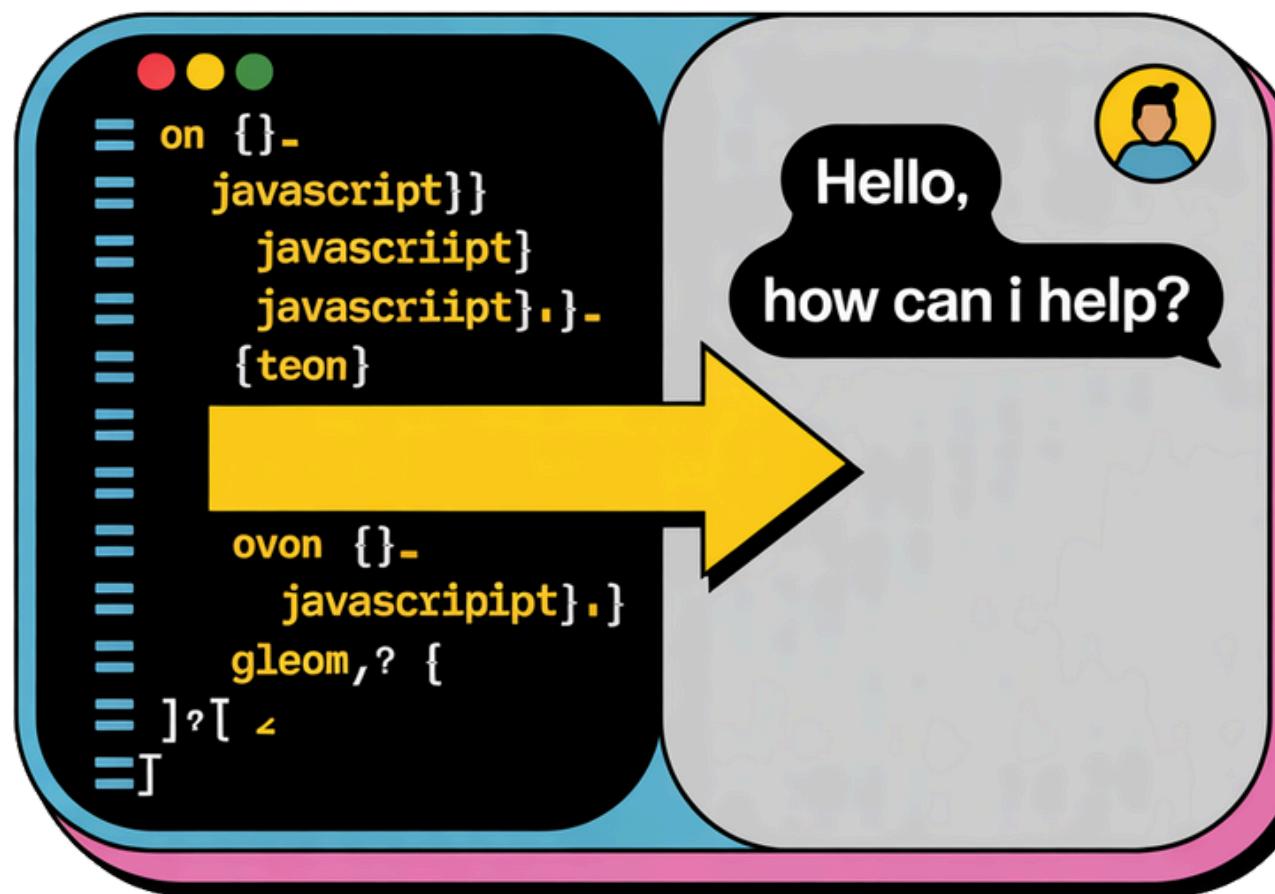
# MODULE THREE

# AGENTKIT





# OPENAI AGENTKIT



**Agent Builder:** a visual canvas for creating and versioning multi-agent workflows

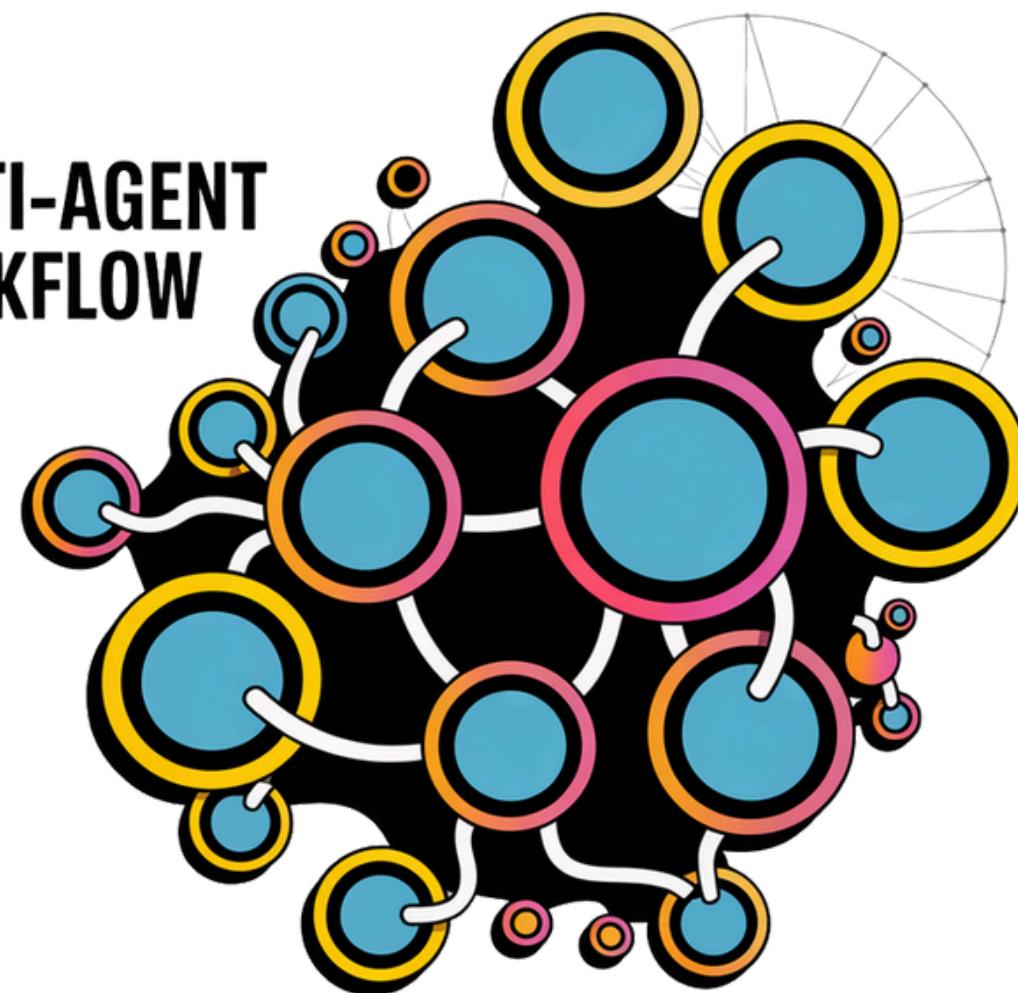
**ChatKit:** a toolkit for embedding customizable chat-based agent experiences in your product

**Connector Registry:** a central place for admins to manage how data and tools connect across OpenAI products



# AGENT BUILDER

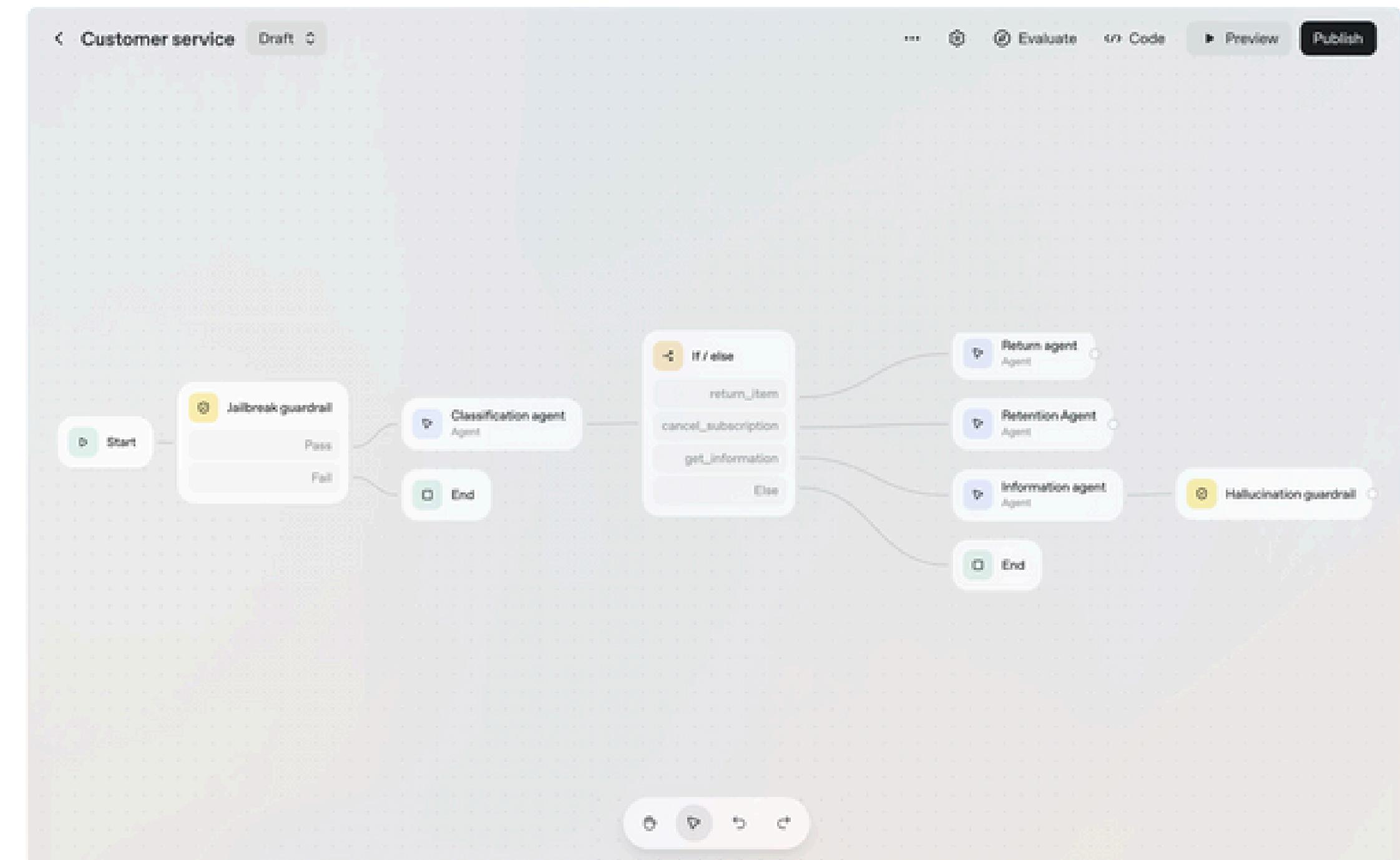
MULTI-AGENT  
WORKFLOW



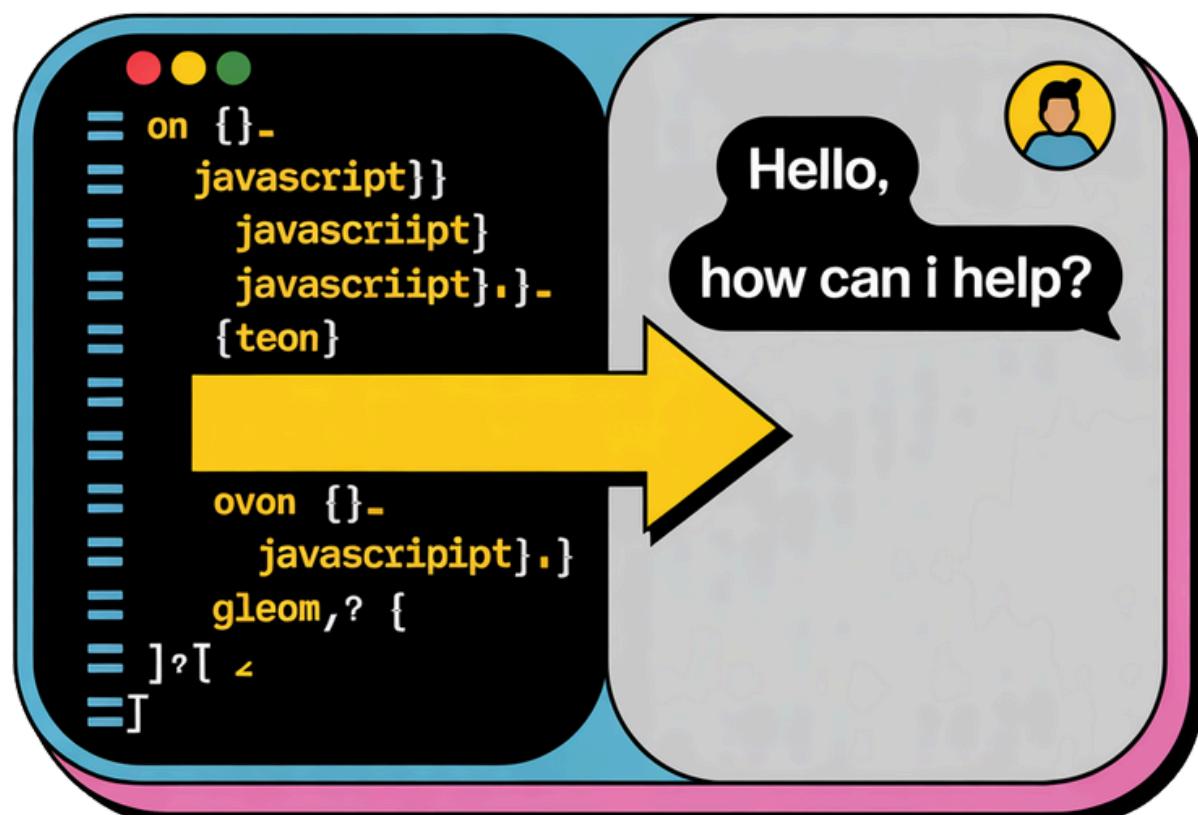
- ★ Drag-and-drop interface for designing complex agent workflows visually
- ★ Start from templates or build workflows from scratch with modular nodes
- ★ Export SDK code or deploy directly to production environments



# AGENT BUILDER CANVAS



# CHATKIT EMBEDDING TOOLKIT



Embeddable chat UI toolkit for adding agent experiences to products



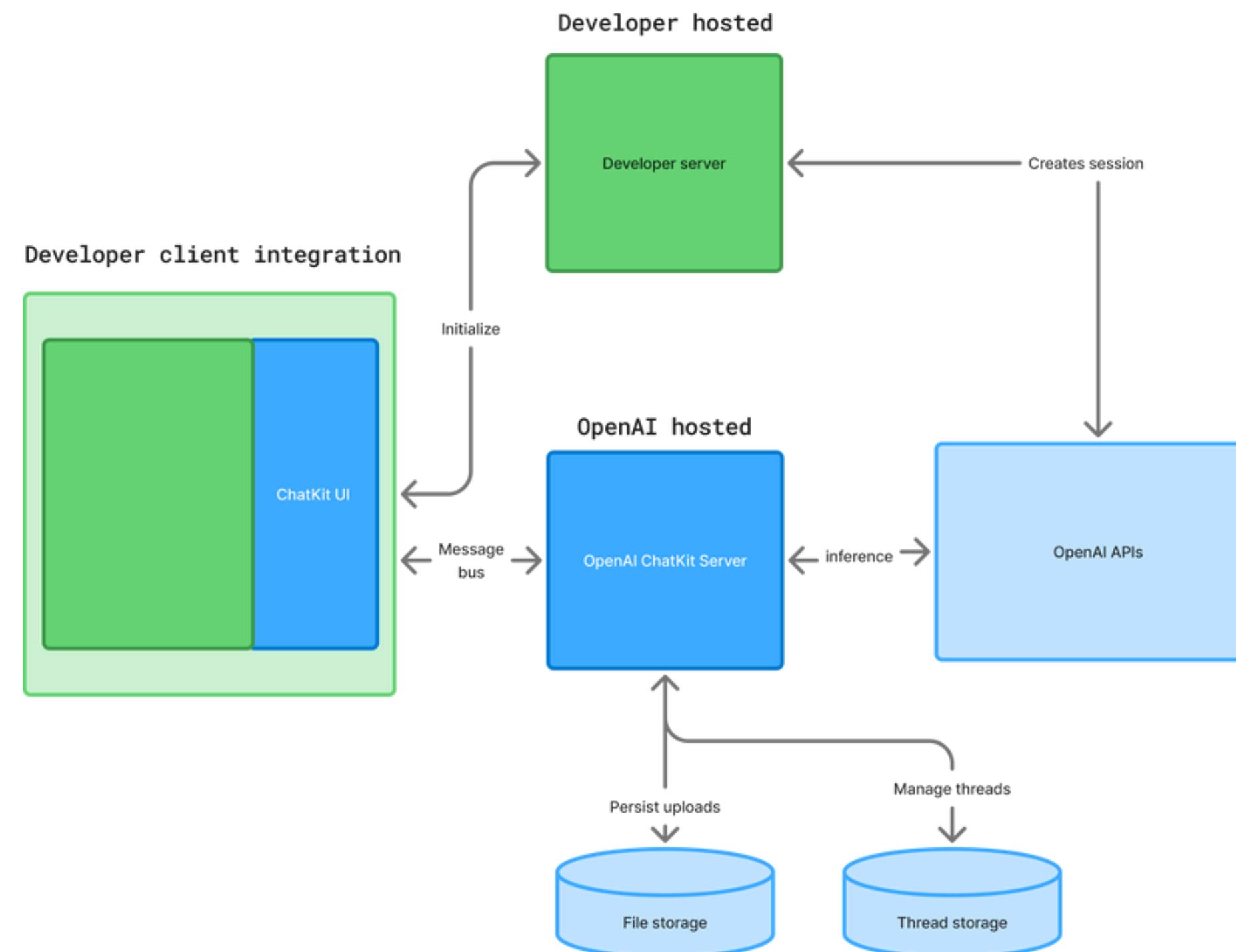
Handles streaming responses, threads, and message history automatically



Displays agent reasoning and tool usage for transparency



# CHATKIT EMBEDDING TOOLKIT



# CHATKIT EMBEDDING

- 1 On your server, generate a client token.

This snippet spins up a FastAPI service whose sole job is to create a new ChatKit session via the [OpenAI Python SDK](#) and hand back the session's client secret:

```
server.py
python ⚡
1 from fastapi import FastAPI
2 from pydantic import BaseModel
3 from openai import OpenAI
4 import os
5
6 app = FastAPI()
7 openai = OpenAI(api_key=os.environ["OPENAI_API_KEY"])
8
9 @app.post("/api/chatkit/session")
10 def create_chatkit_session():
11     session = openai.chatkit.sessions.create({
12         # ...
13     })
14     return { client_secret: session.client_secret }
```

- 2 In your server-side code, pass in your workflow ID and secret key to the session endpoint.

The client secret is the credential that your ChatKit frontend uses to open or refresh the chat session. You don't store it; you immediately hand it off to the ChatKit client library.

See the [chatkit-js repo](#) on GitHub.

chatkit.ts

typescript ⚡

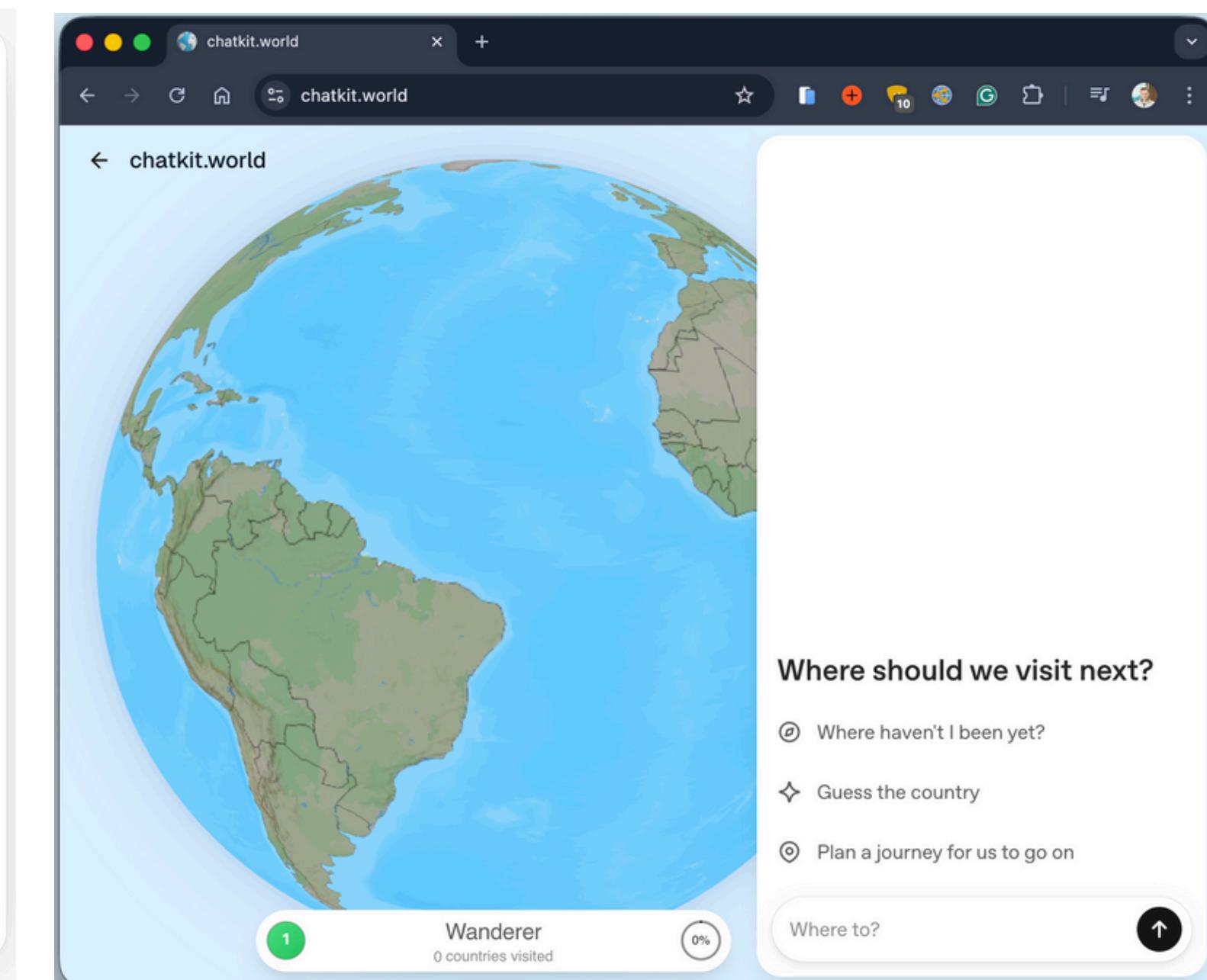
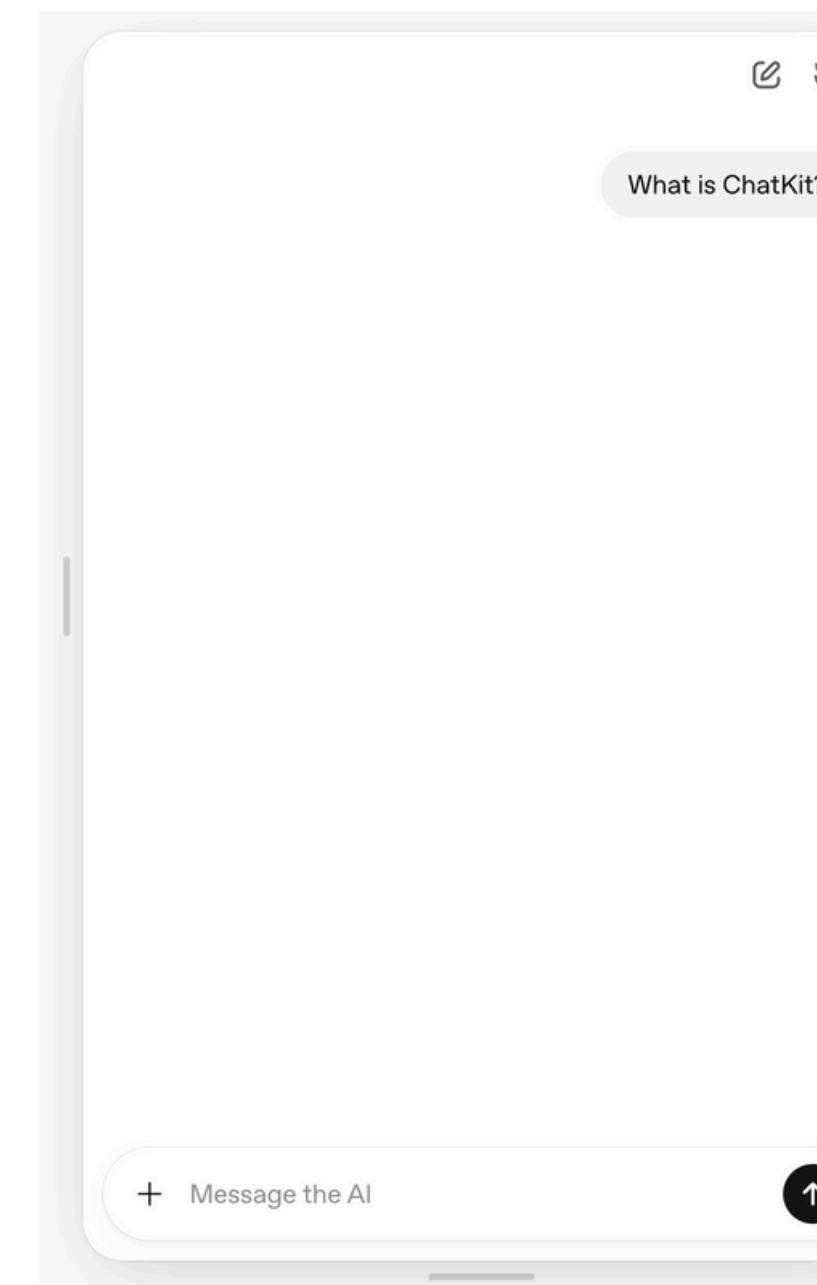
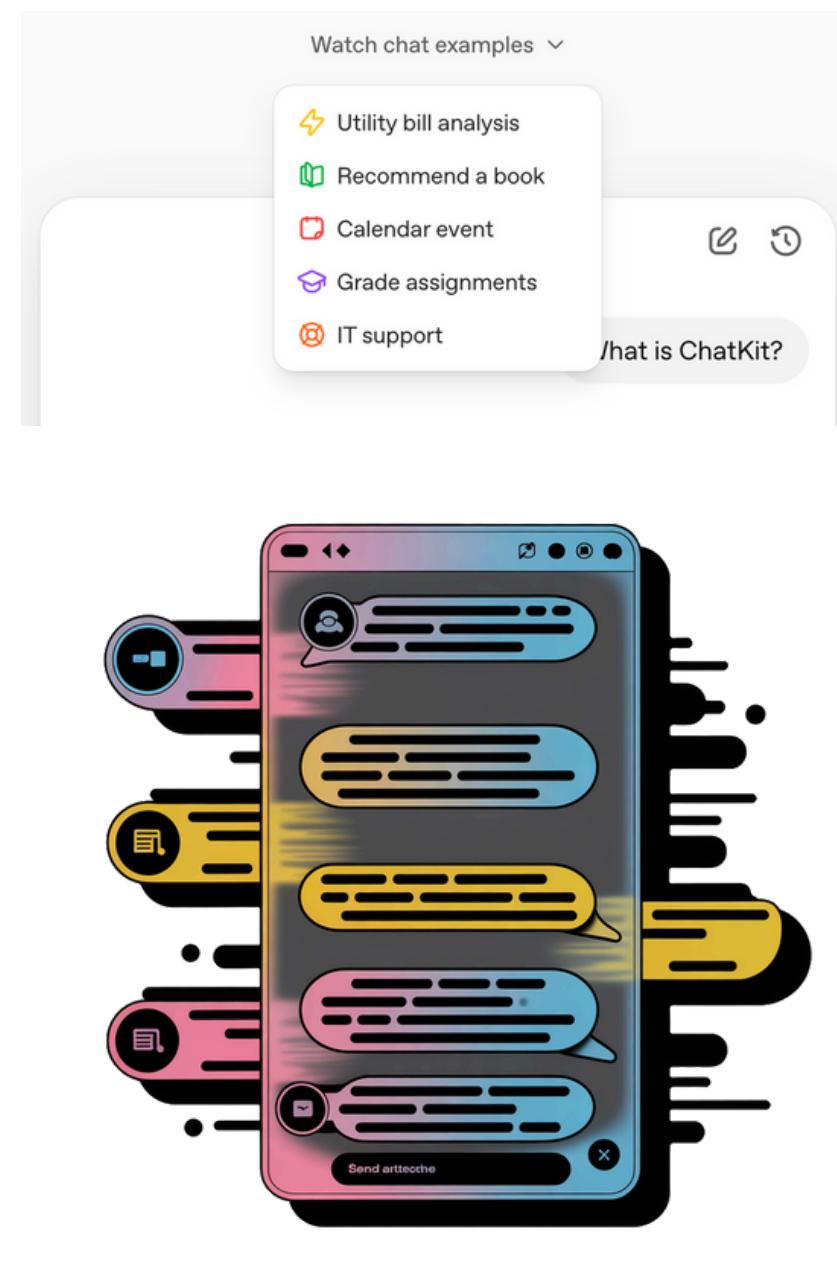
```
1 export default async function getChatKitSessionToken(
2     deviceId: string
3 ): Promise<string> {
4     const response = await fetch("https://api.openai.com/v1/chatkit/sessions",
5         method: "POST",
6         headers: {
7             "Content-Type": "application/json",
8             "OpenAI-Beta": "chatkit_beta=v1",
9             Authorization: "Bearer " + process.env.VITE_OPENAI_API_SECRET_KEY,
10        },
11        body: JSON.stringify({
12            workflow: { id: "wf_68df4b13b3588190a09d19288d4610ec0df388c3983f58d1" },
13            user: deviceId,
14        }),
15    );
16
17    const { client_secret } = await response.json();
18
19    return client_secret;
20 }
```

- 3 In your project directory, install the ChatKit React bindings:

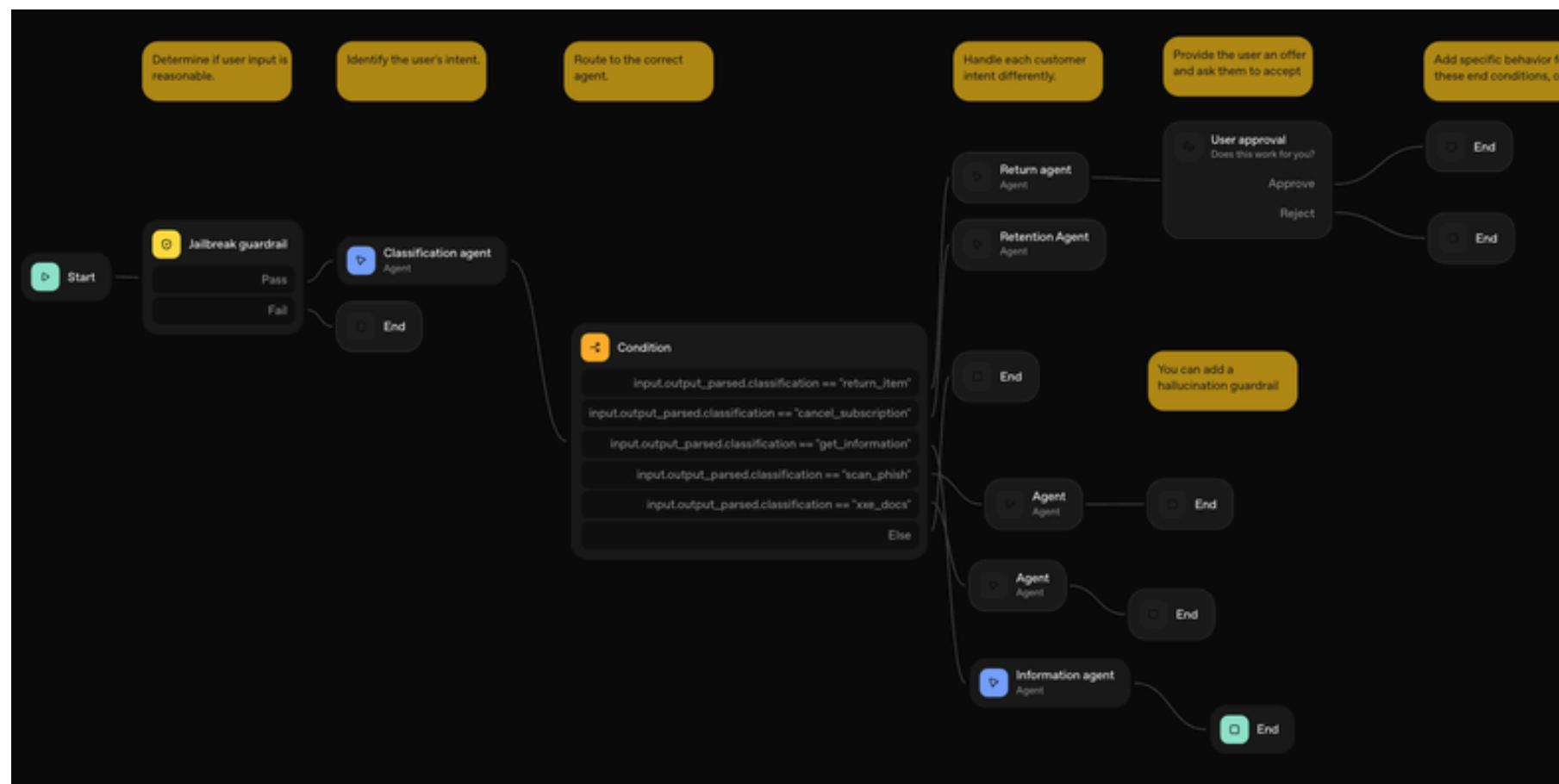
```
npm install @openai/chatkit-react ⚡
```



# CHATKIT EXAMPLES



# CHATKIT EXAMPLES



tell me about XXE Attacks Passed

- ▷ Start
- ☑ Jailbreak guardrail

**GUARDRAILS SUMMARY**

**SAFE TEXT**  
tell me about XXE Attacks

**RAW RESULT**  
Show raw

- ▷ Classification agent
- ["classification":"get\_information"]
- ↳ resp\_008f53f7d862c69...
- ↳ Condition
- ▷ Information agent
- ↳ Searched files  
"XXE Attacks"

XML External Entity (XXE) attacks are a type of web security vulnerability that occurs when an application processes XML input containing external entity references. Because XML allows defining custom entities that can point to external sources such as files or URLs, an attacker can exploit this to make the application disclose sensitive data or perform unintended actions.

**What is XXE?**

XXE injection happens when an attacker is able to include a specially crafted



# CONNECTOR REGISTRY



- ★ Centralized governance for data and tool connections across products
- ★ Manage integrations with CRMs, databases, Google Drive, and more
- ★ Support for prebuilt connectors and third-party MCPs



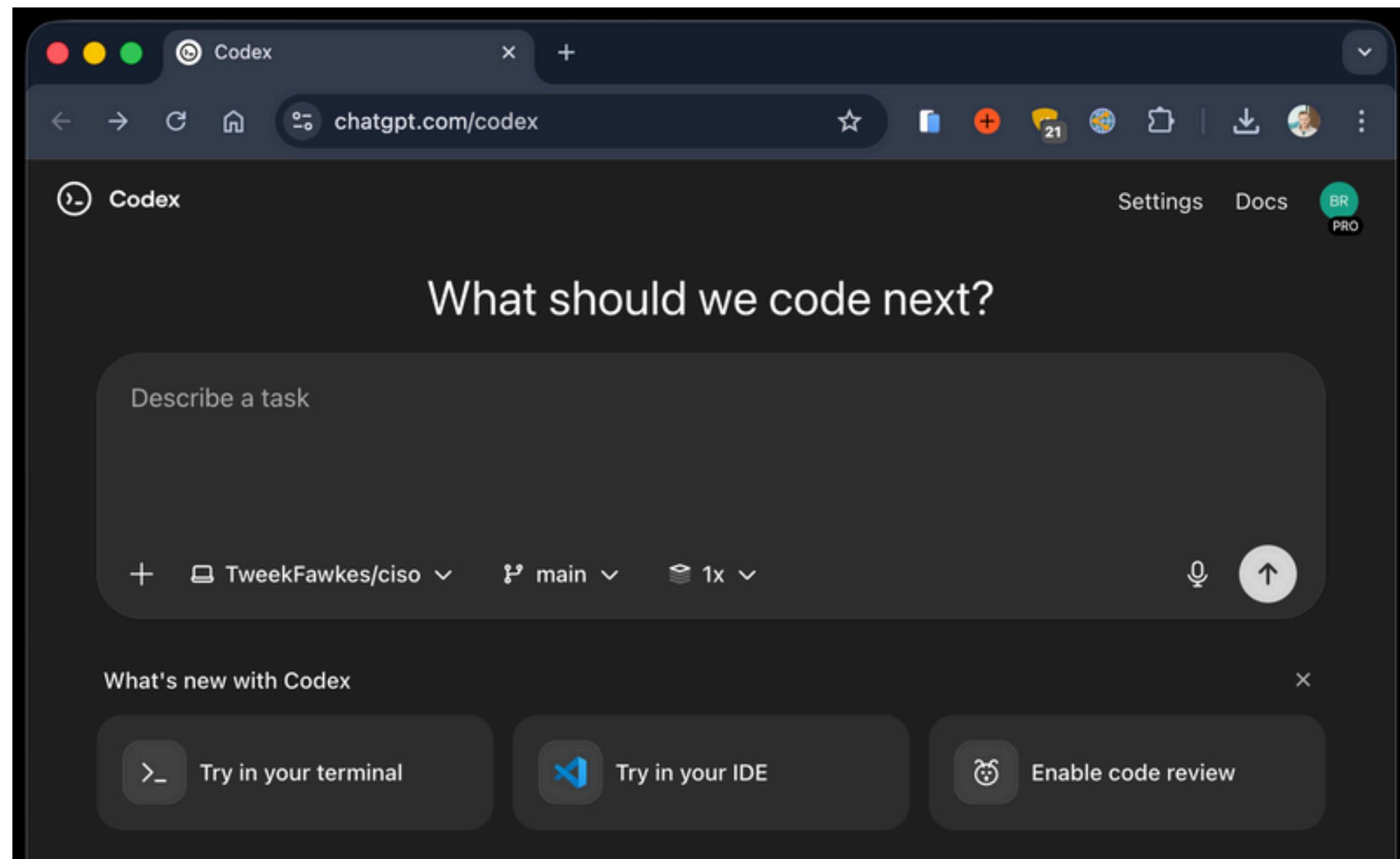
# MODULE FOUR

# OPENAI CODEX

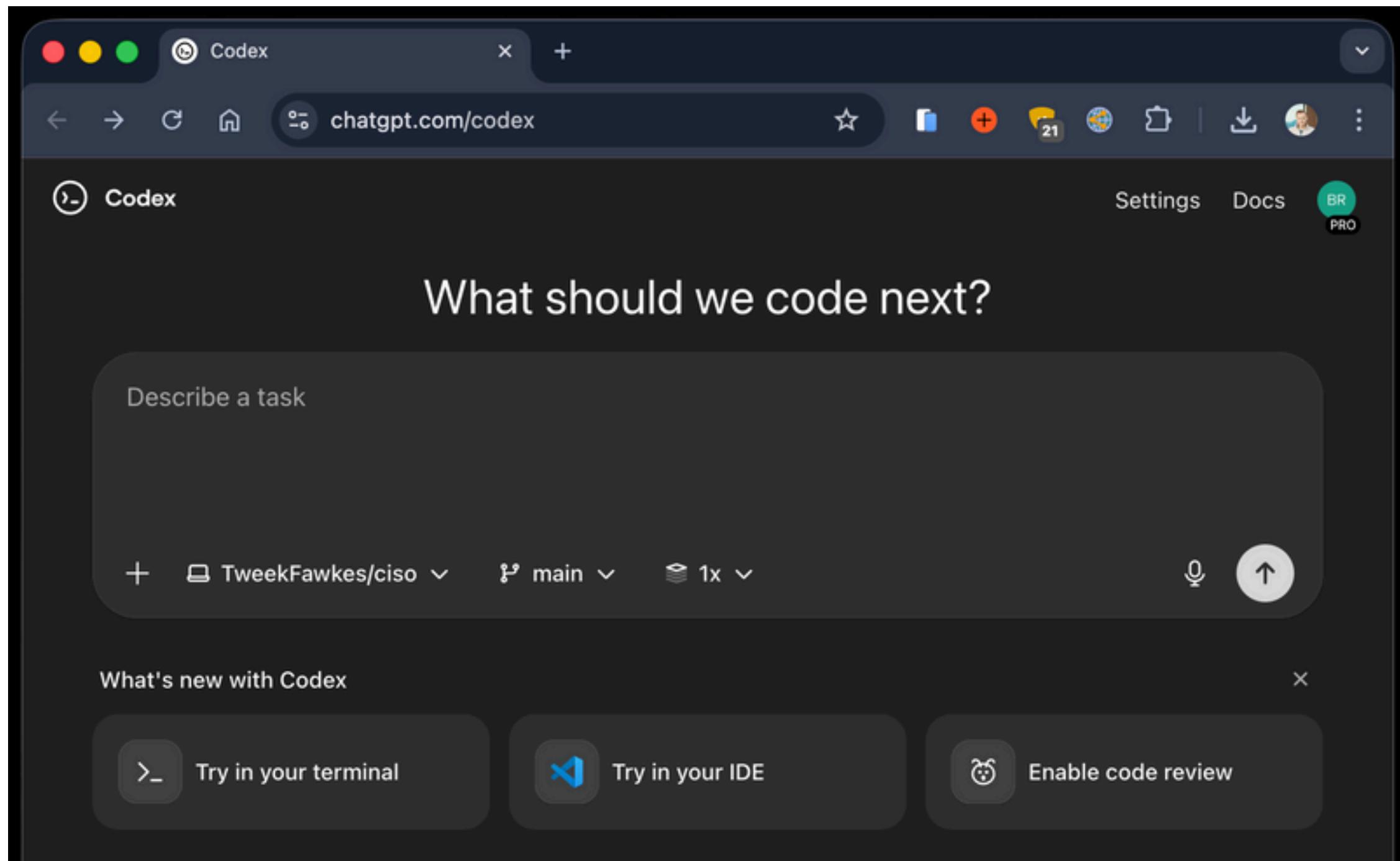




# OPENAI CODEX



# OPENAI CODEX



Environments > New

## Basic

GitHub organization

TweekFawkes

Repository

Q vuln

vuln\_webapp\_001  
Public

This list only includes repositories that you have access to in GitHub and can use with Codex.  
Missing a repo? [Configure repository access](#).

Name

TweekFawkes/vuln\_webapp\_001

27/64

Description

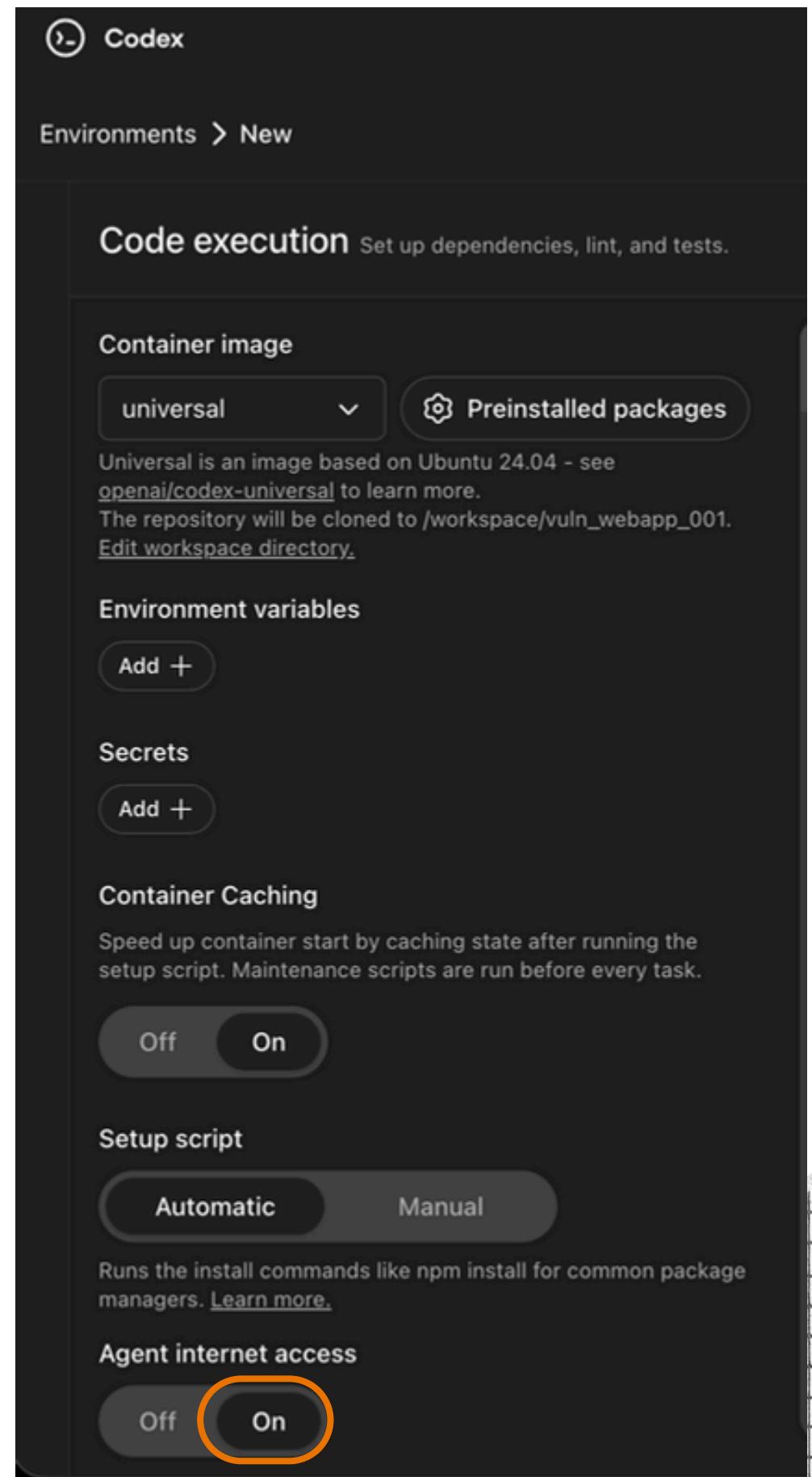
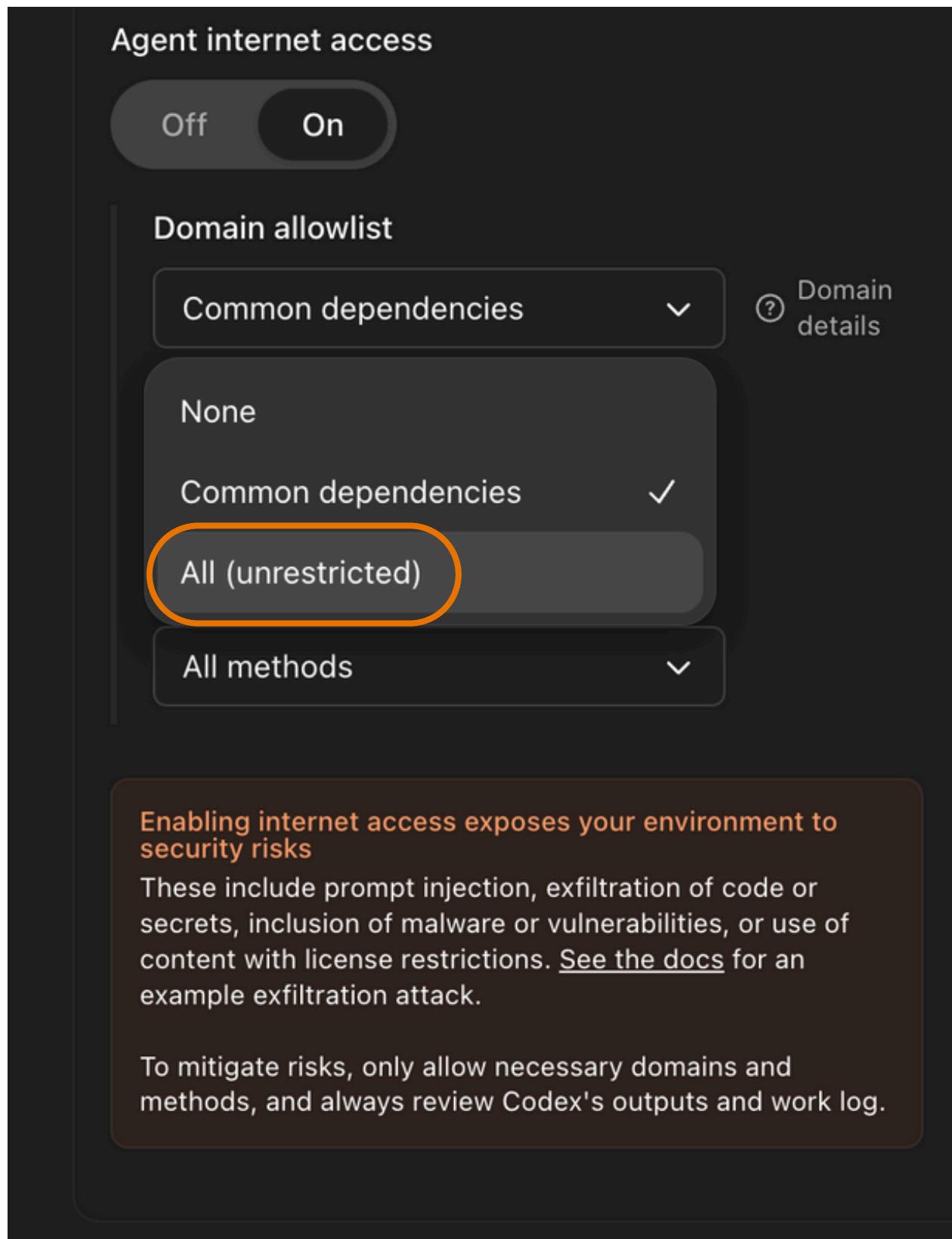
1-2 sentence description

0/512

...

The screenshot shows the "Basic" configuration screen for creating a new environment. It includes fields for "GitHub organization" (set to "TweekFawkes"), "Repository" (search bar containing "vuln"), and a list of available repositories ("vuln\_webapp\_001 Public"). A note states that the list includes repositories the user has access to in GitHub. Below this, there are fields for "Name" ("TweekFawkes/vuln\_webapp\_001") and "Description" (placeholder "1-2 sentence description"). The bottom of the screen shows a character counter ("0/512") and a "..." button.

# OPENAI CODEX



# OPENAI CODEX

What should we code next?

Conduct a security audit focusing on:

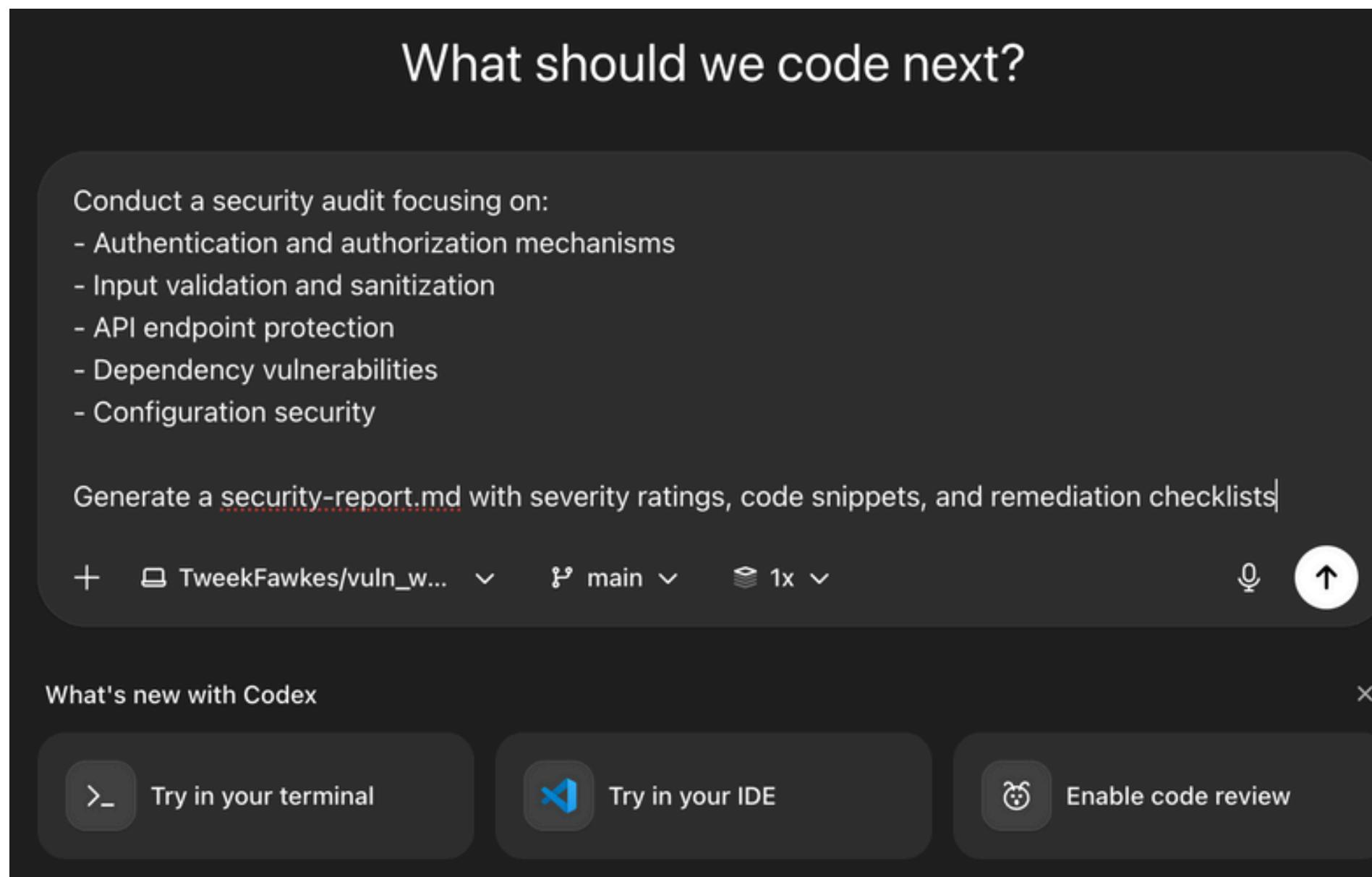
- Authentication and authorization mechanisms
- Input validation and sanitization
- API endpoint protection
- Dependency vulnerabilities
- Configuration security

Generate a [security-report.md](#) with severity ratings, code snippets, and remediation checklists

+ TweekFawkes/vuln\_w... main 1x

What's new with Codex

> Try in your terminal Try in your IDE Enable code review



What should we code next?

Describe another task

+ TweekFawkes/vuln\_w... main 1x

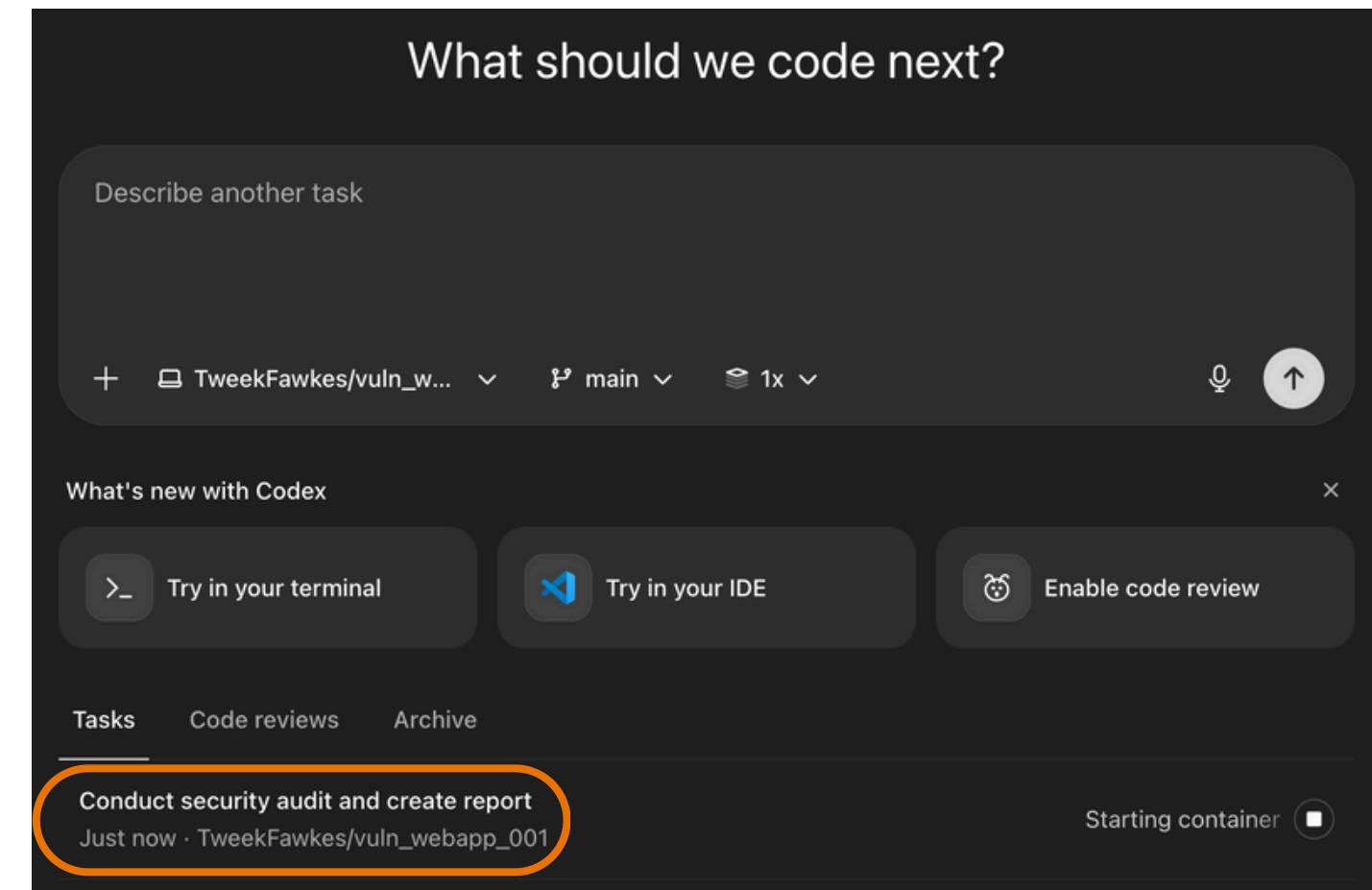
What's new with Codex

> Try in your terminal Try in your IDE Enable code review

Tasks Code reviews Archive

Conduct security audit and create report  
Just now · TweekFawkes/vuln\_webapp\_001

Starting container



Conduct a security audit focusing on:

- Authentication and authorization mechanisms
- Input validation and sanitization
- API endpoint protection
- Dependency vulnerabilities
- Configuration security

Generate a [security-report.md](#) with severity ratings, code snippets, and remediation checklists



# OPENAI CODEX

← Conduct security audit and create report  
Oct 28 · TweekFawkes/vuln\_webapp\_001 · main · +108 -0

Conduct a security audit focusing on:  
- Authentication and authorization mechanisms  
- Input validation and sanitization  
- API endpoint protection  
- Dependency vulnerabilities...

Worked for 2m 7s >

**Summary**

- Added `security-report.md` detailing critical authentication, input validation, endpoint protection, dependency, and configuration vulnerabilities alongside remediation checklists for the Node.js application.

**Testing**

- ⚠ No automated tests were run (documentation-only change).

File (1)

security-report.md

New

Like Comment

security-report.md New ⚙ +108 -0 :

```
1  * # Security Audit Report
2  *
3  * ## Overview
4  * This assessment reviewed the Node.js application in 'vulnerable-web-app/server.js' with a focus on authentication and authorization, input validation and sanitization, API endpoint protection, dependency risk, and configuration security. The findings below summarize the observed issues, assign severity ratings, provide representative code snippets, and outline remediation checklists.
5  *
6  * ---
7  *
8  * ## 1. Authentication & Authorization
9  * - **Severity:** Critical
10 * - **Issue:** The application exposes multiple HTTP endpoints without any authentication or authorization checks, allowing unauthenticated users to read user data, execute arbitrary system commands, and evaluate expressions. Additionally, the default response leaks the 'API_KEY' secret to every visitor.
11 * - **Evidence:** 
12 *   ``js
13 *   if (url.pathname === '/user') {
14 *     const username = url.searchParams.get('username');
15 *     const filePath = './data/${username}.json';
16 *     const data = fs.readFileSync(filePath, 'utf8');
17 *     res.end(data);
18 *   }
19 *   // ...
20 *   res.end('Welcome to the vulnerable web app!\nAPI_KEY=${env.API_KEY}');
21 *   /**
22 * - **Impact:** Attackers can access sensitive data and secrets without credentials, enabling data exfiltration and system compromise.
23 * - **Remediation Checklist:** 
24 *   - Implement an authentication layer (e.g., session-based or token-based) before serving any sensitive routes.
25 *   - Enforce role-based authorization checks on administrative or sensitive operations ('/user', '/exec', '/calc').
26 *   - Never echo secrets in HTTP responses; restrict sensitive environment variables to backend use only.
27 *   -
28 *   ---
```

Archive Share Create PR



# MODULE FIVE

# GOOGLE OPAL





# GOOGLE OPAL OVERVIEW



- ★ Build AI mini-apps using natural language descriptions—no coding required
- ★ Visual workflow editor chains prompts, models, and tools automatically
- ★ Share apps instantly via link; others use with their Google accounts



# APENDIX

# MORE INFORMATION



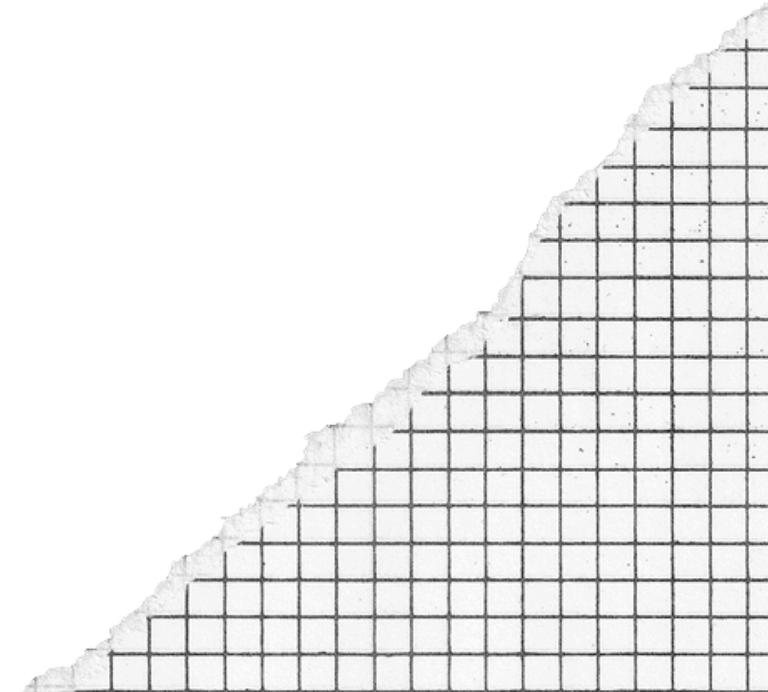
# WEEKLY PODCAST WITH SHELBY



<https://AiCyber.Land>



YouTube:



# STAY IN TOUCH AFTERWARDS

Find me on the following...



Signal App:

**brycekunz.99**



**www.GammaXon.com**



**Bryce@GammaXon.com**

