4-Week Low-Code Agentic AI Curriculum

Goal: Students learn how to create **ONE powerful no-code AI agent** that solves a real problem, integrating a cybersecurity theme.

Week 1: Foundations of Agents & No-Code Orchestration

Focus: Defining agents, mastering instruction (prompt engineering), and connecting to non-automation tools.

Class 1 (3 Hours): Advanced Prompt, Context Engineering & Spec Engineering

- **Concept:** What is an AI Agent? (A "Self-managed digital assistant" that executes tasks, not just a chatbot).
- **Skill:** Prompt Engineering using the **Six-Part Framework** (Command, Strategies, RolePlay, Output, Game Changer).
- **Skill:** Context Engineering (Uploading "Knowledge" to make the agent a specialist).

✅ Lab Activity: Build ONE Expert GPT Agent

- **Create a Custom GPT:** Log into OpenAI/ChatGPT and select "Create a GPT".
- **Define Role:** Name it "Cybersecurity Analyst" and upload specific knowledge files (PDFs/Articles).
- **Apply Framework:** Write a system prompt using the Six-Part Framework.
    - *Constraint:* Set a strict output format (e.g., JSON or specific headers).
- **Test Tone:** Verify the agent speaks in a professional "American friendly" tone.

Class 2 (3 Hours): Intro to n8n (The Orchestrator)

- **Tool:** n8n (No-Code Platform).
- **Concept:** "Trigger + Action" logic.
- **Integration:** Connecting an AI Agent to external storage (Google Sheets).

✅ Lab Activity: Connect the Expert Agent

- **Set up Trigger:** Create a Webhook node in n8n to receive user input.
- **Connect AI:** Add an OpenAI node and connect it to your "Cybersecurity Analyst" assistant.
- **Connect Storage:** Add a Google Sheets node.
- **Test Workflow:** Send a test question.
    - Verify the question goes to the Agent.
    - Verify the answer appears in your Google Sheet automatically.

Week 2: Building Agentic Workflows with a Cybersecurity "Touch"

Focus: Building multi-step "Agentic Loops" (Plan → Act → Observe) in n8n.

Class 3 (3 Hours): Building Agentic Loops in n8n

- **Concept:** The Agentic Loop (Plan, Act, Observe).
- **Skill:** Tool Calling (Using n8n nodes as "tools" for the agent).
- **Skill:** Memory (Enabling the agent to remember context).

✅ Lab Activity: Build a Research Agent

- **Start Workflow:** Create a generic chat trigger.
- **Add Tool (Google Search):** Configure an HTTP Request node to query Google.
- **Scrape Content:** Configure a node to read the text of the top search result.
- **Summarize:** Send the scraped text to your OpenAI Agent with the instruction: *"Summarize this for a security briefing."*
- **Final Output:** Ensure the summary is returned to the user.

Class 4 (3 Hours): Cyber Use Case 1: Phishing Detector Agent

- **Theory:** The Cyber Threat Landscape (Malware, Phishing, DDoS).
- **Concept:** No-Code Threat Detection (Replacing Python models with AI Agents).

✅ Lab Activity (Project): Phishing Analyzer Workflow

- **Simulate Email:** Create a Webhook that accepts a JSON body (simulate an incoming email).
- **Configure Brain:** Prompt your Agent to analyze text and output **JSON ONLY**:
  - {"is_phishing": true/false, "reason": "..."}
- **Logic Gate:** Add an If node in n8n to check json.is_phishing.
- **Branch True:** If true, send an alert to Slack/Discord.
- **Branch False:** If false, log the email to Google Sheets as "Safe".

Week 3: Practical Business Automation & Advanced Agent Engineering

Focus: Automating business channels (LinkedIn, WhatsApp) and using the OpenAI Agent Kit.

Class 5 (3 Hours): Practical Automation with n8n (Social & Business)

- **Goal:** Managing real-world business communications.

- **Channels:** Gmail (Trigger/Extraction), WhatsApp (Business API), LinkedIn (Content).

✅ **Lab Activity: The "Executive Assistant" Workflow**

- **Gmail Trigger:** Set n8n to watch for emails with the Label "Lead".
- **Data Extraction:** Use an AI node to extract `Name`, `Company`, and `Request` from the email body.
- **Draft Reply:** Generate a polite, personalized email response using your Agent.
- **Notify Owner:** Send a WhatsApp message to your phone: *"New Lead: [Name] from [Company]. Draft reply prepared."*

Class 6 (3 Hours): OpenAI Agent Kit & Agent Builder

- **Tool:** OpenAI Agent Kit (Assistants API).
- **Concept:** Agents vs. Chat Completions (Stateful vs. Stateless).
- **Skill:** Guardrails (Preventing jailbreaks and off-topic chat).

✅ **Lab Activity: Build a "Customer Support Agent" with Guardrails**

- **Build Assistant:** Create a new Assistant in the OpenAI Playground.
- **Upload Knowledge:** Upload a mock "Product Manual" PDF.
- **Define Tools:** specific functions (e.g., `check_order_status`).
- **Implement Guardrails:** Write system instructions to decline competitor questions.
- **Jailbreak Test:** Try to trick your agent into being rude or discussing competitors.
- **Patch:** Update instructions to fix any weaknesses found.

Week 4: Building a Full-Stack Low-Code Agentic App

Focus: Combining Front-End, Back-End, and AI into a shipped application.

Class 7 (3 Hours): Intro to Lovable & Supabase

- **Full Stack:** Lovable (UI) + n8n (Logic) + Supabase (Database).
- **Architecture:** Understanding how the UI talks to the Orchestrator.

✅ **Lab Activity: Build the UI & Database**

- **Database Setup:** Create a Supabase project and a table named `security_alerts`.
- **UI Design:** Use Lovable to build a simple chat interface.
- **Connection:** Connect the Lovable chat component to your n8n Webhook URL.

Class 8 (3 Hours): Final Project: "Cybersecurity Triage Bot"

- **Goal:** A "Professional Grade" AI-driven incident response system.
- **Role:** The AI acts as a Tier-1 SOC Analyst.

✅ **Lab Activity (Final Project)**

- **Front-End:** Create an input field in Lovable for "Raw Security Logs".
- **Orchestrator (n8n):**
    - Receive log data.
    - **Analyze:** Agent identifies Indicators of Compromise (IoC) and assigns Priority (Low/Med/High).
    - **Store:** Write the Log + Analysis + Priority to Supabase.
- **Display:** Show the AI's analysis and recommended "Next Steps" in the UI.
- **Final Polish:** Adjust prompts until the output sounds like a senior cybersecurity expert.