AI Accelerator Program: Building Secure In-House Intelligence

Duration 15 days

Course Objective

To equip participants with elite skills in Python and cutting-edge AI frameworks including **Ollama, LangChain, CrewAI, AutoGen, and LangGraph**. The program is designed to enable the architecture, deployment, and maintenance of a secure, in-house AI ecosystem for advanced data analysis and the creation of sophisticated autonomous agents.

Module 1: The AI Development Toolkit (Days 1-3)

- **Day 1: Python & The Local AI Ecosystem**
  - **Core Concepts:**
    - Essential Python: Syntax, data structures, and functions for AI.
    - Environment Setup: Anaconda & Jupyter for iterative development.
    - **Introduction to Ollama:** Setting up and running powerful open-source LLMs entirely in-house.
  - **Hands-on Lab:**
    - Write foundational Python scripts.
    - Install Ollama and interact with a local language model for the first time.
- **Day 2: Data Handling & Visualization**
  - **Core Concepts:**
    - Advanced Data Manipulation with Pandas.
    - Visual Storytelling: Creating compelling charts with Matplotlib & Seaborn.
    - Preparing data for both traditional ML and LLM analysis.
  - **Hands-on Lab:**
    - Perform a complete exploratory data analysis (EDA).
    - Generate insightful charts to present findings from a sample dataset.
- **Day 3: The Open-Source AI Ecosystem: Hugging Face & LangChain**
  - **Core Concepts:**
    - **Introduction to Hugging Face:** Exploring the hub for models, datasets, and the transformers library.
    - Understanding the ecosystem for open-source AI.
    - The LangChain Framework: The "glue" for LLM applications.
    - Connecting LangChain with **Ollama** for secure, local-first development.
  - **Hands-on Lab:**
    - Explore and identify suitable models on the Hugging Face Hub.
    - Build your first LLM chains using LangChain, powered by your local **Ollama** model.

        - Practice advanced prompt engineering techniques within the LangChain framework.

Module 2: Predictive Analytics & RAG (Days 4-6)

- **Day 4: Machine Learning for Data Insights**
    - **Core Concepts:**
        - Supervised Learning: Regression & Classification with Scikit-learn.
        - Unsupervised Learning: Clustering with K-Means.
        - Generating quantitative insights from structured data.
    - **Hands-on Lab:**
        - Build, train, and evaluate a classification model.
        - Interpret performance metrics like Accuracy and the Confusion Matrix.
- **Day 5: Retrieval-Augmented Generation (RAG)**
    - **Core Concepts:**
        - Securely augmenting LLMs with private knowledge using RAG.
        - Vector Databases: Indexing documents for efficient semantic retrieval.
        - Building RAG pipelines with **LangChain**.
    - **Hands-on Lab:**
        - Build a functional RAG system to enable a "chat with your documents" feature, powered by your local **Ollama** model.
- **Day 6: Building Chains & Tool-Using Agents**
    - **Core Concepts:**
        - Creating complex, multi-step workflows with LangChain Expression Language (LCEL).
        - Introduction to AI Agents: The concept of ReAct (Reason + Act).
        - Equipping **LangChain Agents** with "tools" to interact with external systems (e.g., data analysis functions).
    - **Hands-on Lab:**
        - Develop an agent that can dynamically select and use a Python tool to solve a problem.

Module 3: Orchestrating Autonomous AI Agents (Days 7-9)

- **Day 7: Collaborative AI with CrewAI**
    - **Core Concepts:**
        - Introduction to **CrewAI** for orchestrating role-playing, autonomous agents.
        - Defining Agents with specific roles, goals, and backstories.
        - Designing collaborative Tasks and assembling a Crew.
    - **Hands-on Lab:**
        - Build a simple research crew where one agent finds information and another summarizes it.
- **Day 8: Conversational Multi-Agent Systems with AutoGen**
    - **Core Concepts:**
        - Introduction to Microsoft's **AutoGen** framework.

        - Building systems with conversable agents that can solve tasks collectively.
        - Comparing **AutoGen's** conversation-driven approach to **CrewAI's** task-driven approach.
    - **Hands-on Lab:**
        - Create a multi-agent chat environment where agents collaborate to write code or analyze a problem.
- **Day 9: State Management with LangGraph**
    - **Core Concepts:**
        - Introduction to **LangGraph**: Building robust, stateful agentic applications.
        - Defining agent states as nodes and decisions as edges in a graph.
        - Creating cyclical and more complex agent behaviors that go beyond linear chains.
    - **Hands-on Lab:**
        - Build an agent that can loop, self-correct, and modify its plan based on tool outputs, using **LangGraph**.

Module 4: Advanced Applications & Capstone Project Prep (Days 10-12)

- **Day 10: Integrating Agents with Institutional Data**
    - **Core Concepts:**
        - Creating custom tools for agents to securely query institutional data (from NASMS, goAML).
        - Security best practices for agent-based data access.
    - **Hands-on Lab:**
        - Develop a custom Python tool that a **CrewAI** or **LangGraph** agent can use to fetch and analyze sample data.
- **Day 11: Comparing Agentic Frameworks**
    - **Core Concepts:**
        - A deep-dive workshop comparing the strengths and weaknesses of LangChain Agents, **CrewAI**, **AutoGen**, and **LangGraph**.
        - Choosing the right framework for a given problem.
    - **Hands-on Lab:**
        - Implement the same simple task in two different frameworks to directly compare development experience and results.
- **Day 12: Capstone Project Scoping**
    - **Core Concepts:**
        - Defining the final project deliverables.
        - Designing the agentic workflow for the final project.
        - Setting up the secure, in-house development environment for the project.
    - **Hands-on Lab:**
        - Begin developing the data connectors and core agent logic for the capstone project.

Module 5: Capstone Project: Secure Intelligence Synthesis (Days 13-15)

- **Day 13: Project Build Day I - Agent & Tool Development**
    - **Hands-on Lab:**
        - A full day dedicated to building the core agents (using the chosen framework), defining their roles, and developing the custom tools they need to perform their tasks on institutional data.
- **Day 14: Project Build Day II - Workflow Orchestration**
    - **Hands-on Lab:**
        - A full day focused on orchestrating the agents into a cohesive workflow.
        - Connecting the agents' outputs to generate narrative summaries and quantitative findings.
- **Day 15: Automated Reporting & Final Presentation**
    - **Hands-on Lab:**
        - Develop a Python script to automatically generate a polished PDF report from the final output of the agent crew.
        - Finalize and present the end-to-end pipeline that transforms raw data into a finished, insightful report.
        - Discuss strategies for in-house deployment, monitoring, and maintenance.