

**Generative AI Engineering**

**Course Number:** AI-106WA  
**Duration:** 5 days

**Overview**

This Generative AI Engineering training course teaches attendees how to integrate LLMs (Large Language Models) into their AI applications. In addition, participants learn how to ensure their applications are secure and private. By the end of this course, students will confidently build and evaluate Generative AI models for various tasks such as text generation, image synthesis, and summarization.

**Prerequisites**

* Extensive prior Python development experience
* Core Python Data Science skills, including the use of NumPy and Pandas
* Inferential statistics

**Materials**

All Generative AI training students receive comprehensive courseware.

**Software Needed on Each Student PC**

All attendees must have a modern web browser and an Internet connection.

**Objectives**

* Implement various Generative AI architectures, such as Variational Autoencoders (VAE), Generative Adversarial Networks (GAN), and Transformers
* Tune Generative AI models to achieve optimal performance on specific tasks
* Build Generative AI models using pre-training and fine-tuning techniques
* Evaluate the performance of Generative AI models using standard evaluation metrics
* Design and develop Generative AI applications using prompt engineering and other techniques
* Secure Generative AI applications from security risks, such as data privacy leaks and malicious use of AI
* Explore the future directions of Generative AI products and model development

**Outline**

* Introduction to Generative AI
  + Generative AI’s Roots in Machine Learning
  + Understanding Generative models
  + Contrasting Generative and Discriminative Models
  + The original LLM models – from BERT to GPT
  + Current Cloud- and Offline-Based LLM’s
* Generative AI Architecture
  + Variational Autoencoders (VAE)
  + Generative Adversarial Networks (GAN)
  + Reinforcement Learning from Human Feedback (RLHF)
  + Transformers
  + Generative Pre-Trained Transformers (GPT)
* Tuning Generative AI Models
  + Building Generative AI Models
  + How Pre-Training Works
  + Data Preparation and Preprocessing
  + Fine Tuning Generative AI Models
  + Formatting Data for LLM Fine Tuning
  + Fine Tuning GPT
  + Transfer learning Techniques
* Evaluation and Optimization of Generative AI Models
  + Evaluating model performance
  + Common evaluation metrics for generative AI models
* Building Generative AI Applications (part 1)
  + Application Design Building Blocks
  + Use Cases of LLM Based Applications
  + Prompt Engineering Basics
  + Prompt Templates
  + RAG with Llama Index
* Case Studies and Real-World Applications
  + Generative AI for Text
  + Generative AI for Media
  + Generative AI for Code
* Building Generative AI Applications (part 2)
  + Customizing with Prompt Engineering
  + Advanced Prompt Types
  + Customizing with RAG
  + Customizing with SYSTEM/CONTEXT Arguments and Prompt Templates
  + Customizing with Fine Tuning
  + Design Considerations and Tradeoffs for Customizing
  + Tying It Together with LangChain
* ChatBots
  + Chat Bot Basics
  + Building LLM-Based Chat Bots
* Security
  + Security Risks with Generative AI
  + Secure Software Development
  + Connectivity
  + Exploitation of AI Systems (Jailbreaks)
  + Infrastructure Concerns
  + System Vulnerabilities
  + Data Privacy and Leaks
  + Malicious Use of AI
  + Obscuring Data for Privacy and Security
  + Best Practices for Security with Generative AI in Enterprises
* Future Directions in Generative AI Products and Model Development
  + Best Practices, Limitations, other Considerations
  + Future of Work
  + Future Evolution of Gen AI
* Conclusion