AI Assisted Secure Software Development Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This intensive **three-day course** is designed to help software developers use artificial intelligence effectively and securely within modern software development workflows.

Throughout the training, participants will explore AI-assisted development tools such as**GitHub Copilot, Amazon Q, and Tabnine**, while gaining practical experience with prompt engineering, AI-supported coding workflows, and the security considerations associated with adopting these technologies.

Hands-on labs give participants the opportunity to build an intelligent application using foundation models, run and deploy machine learning models both locally and in cloud environments, and practise red team techniques to better understand common attacks against AI systems.

The course is designed not only to improve developer productivity but also to provide the practical skills required to build AI-enabled applications and adopt artificial intelligence responsibly and securely within software development environments.

Prerequisites

Participants should have:

- A solid understanding of software development principles and practices
- Experience working with IDEs and version control systems
- Familiarity with cloud environments such as Azure, AWS, or GCP is beneficial

Who Should Attend

This course is particularly suitable for:

- Professional software developers and technical leads looking to integrate AI into development workflows
- DevOps and security engineers who want to understand AI-related risks and defensive techniques
- Development teams aiming to improve productivity and create intelligent applications using AI
- Organisations beginning to adopt AI-assisted development tools and workflows

AI Assisted Secure Software Development Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of the course, participants will be able to:

- Explain core AI concepts and their relevance to modern software development.
- Apply prompt engineering techniques to communicate more effectively with language models.
- Use AI-assisted development tools to accelerate and streamline coding workflows.
- Add AI-powered capabilities and services to new or existing applications.
- Train and deploy machine learning models in both local and cloud environments.
- Recognise common AI attack techniques, including prompt injection and model jailbreaks, and apply appropriate mitigation strategies.
- Incorporate AI securely into production-oriented software development processes.

Outline

Day 1 – AI Foundations and Developer Productivity Tools

AI in Software Development

- The impact of AI on the software industry and emerging trends
- Improving developer productivity with AI
- Overview of AI-assisted development workflows

The AI Development Tool Landscape

- GitHub Copilot: features, use cases, and demonstrations
- Amazon Q Developer: code generation and code security
- Tabnine: privacy, team collaboration, and coding efficiency
- Setting up the cloud-based lab environment and introductory exercises

Prompt Engineering Fundamentals

- Essential prompt engineering techniques and strategies
- Using SudoLang for structured prompting
- Managing AI model limitations and hallucinations
- Guided conversion of natural language into structured prompts

Day 2 – Building AI-Powered Intelligent Applications

Advanced Coding with Copilot

- Code completion, unit testing, and boilerplate generation
- Combining prompt engineering with Copilot Chat
- Practical exercises using unfamiliar environments and frameworks

Comparing AI Tools and Applying Best Practices

- Using ChatGPT within IDE environments

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Comparing AI development tools by features and performance
- Selecting the appropriate AI assistant for different requirements

Application Development with AI Integration

- Overview of the Fresh Cart project
- Integrating LLM-based chatbots
- Prompt routing and orchestration
- Semantic search and state mutation
- Logging and self-correction approaches for AI operations

Security in AI Systems

- Prompt injection risks and practical red team exercises
- Model jailbreak attacks and defensive techniques
- Prompt extraction techniques
- Defensive strategies using ReBuff, Llama Guard, and Lakera

Day 3 – Working with Models and Deployment

Foundation Models and Inference

- Open-source models including Llama 3 and Stable Diffusion
- Running models locally and inside containers
- Hugging Face: Transformers, Pipelines, AutoTrain, and Inference Endpoints

Deploying AI in Cloud Environments

- Microsoft Azure: OpenAI Studio and hosting
- Google Cloud: Vertex AI and Model Garden
- Amazon AI: Bedrock and machine learning toolkits
- Replicate and Cog for containerised model deployment

Machine Learning Essentials

- TensorFlow and Keras workflows
- Model training, tuning, and deployment
- Serving machine learning models with Docker

Advanced AI Concepts

- Fine-tuning models with OpenAI, Vertex AI, and AWS
- Embedding techniques and similarity search
- Building Retrieval Augmented Generation (RAG) applications
- Research tools and embedding workflows within the Fresh Cart project