Mastering LLM Integration Security: Offensive & Defensive Tactics Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **2 Day**

This intensive two-day course explores the security risks and challenges introduced by Large Language Models (LLMs) as they become embedded in modern digital systems. Through AI labs and real-world threat simulations, participants will develop the practical expertise to detect, exploit, and remediate vulnerabilities in AI-powered environments.

The course uses a defence-by-offence methodology, helping learners build secure, reliable, and efficient LLM applications. Content is continuously updated to reflect the latest threat vectors, exploits, and mitigation strategies, making this training essential for AI developers, security engineers, and system architects working at the forefront of LLM deployment.

Prerequisites

Participants should have:

- A basic understanding of AI and LLM concepts
- Familiarity with basic scripting or programming (e.g., Python)
- A foundational knowledge of cybersecurity threats and controls

Target audience

This course is ideal for:

- Security professionals securing LLM or AI-based applications
- Developers and engineers integrating LLMs into enterprise systems
- System architects, DevSecOps teams, and product managers
- Prompt engineers and AI researchers interested in system hardening

What You Will Learn

By the end of this course, learners will be able to:

- Understand LLM-specific vulnerabilities such as prompt injection and excessive agency
- Identify and exploit AI-specific security weaknesses in real-world lab environments
- Design AI workflows that resist manipulation, data leakage, and unauthorised access
- Apply best practices for secure prompt engineering
- Implement robust defences in plugin interfaces and AI agent frameworks
- Mitigate risks from data poisoning, overreliance, and insecure output handling
- Build guardrails, monitor LLM activity, and harden AI applications in production environments