AI Threat Modelling Certificate Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

This hands-on practical three-day course empowers AI engineers, developers, and security professionals to design secure AI systems by mastering AI-specific threat modelling. Using the DICE methodology (Diagramming, Identification, Countermeasures, Evaluation), participants gain practical skills in identifying vulnerabilities, applying countermeasures, and conducting structured security assessments across the AI lifecycle.

Attendees engage in hands-on labs and a red vs. blue team exercise simulating attacks on a rogue AI research assistant. The course addresses real-world AI threats, including prompt injection, data poisoning, adversarial manipulation, and model abuse, while aligning with emerging standards such as the EU AI Act and OWASP Top 10 for LLM applications.

Prerequisites

Participants should have:

- A basic understanding of AI principles (e.g. neural networks, training processes, common architectures)
- Familiarity with general security fundamentals
- No prior threat modelling experience is required
- Pre-course materials are provided to ensure readiness

Target audience

This course is intended for:

- AI engineers and machine learning developers
- Software engineers building AI-powered systems
- Solution architects integrating AI into enterprise applications
- Security professionals securing AI pipelines and APIs
- Security architects responsible for risk and compliance in AI deployments

What You Will Learn

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

- Model AI threats using the DICE methodology
- Assess AI components for vulnerabilities and attack surfaces
- Develop countermeasures for threats like prompt injection, data leakage, and poisoning
- Integrate threat modelling into AI/ML development pipelines
- Apply design patterns to build secure, privacy-aware AI systems
- Conduct risk assessments for AI projects with business and regulatory context
- Lead security discussions and implement governance frameworks aligned with AI compliance