Certified Offensive AI Security Professional (C|OASP) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

The **Certified Offensive AI Security Professional (C|OASP)** certification by **EC-Council** is the world's leading hands-on program focused on **offensive and defensive AI security**.
It equips cybersecurity professionals with the knowledge and tools to identify, exploit, and defend against vulnerabilities in machine learning and AI systems.

Participants learn to perform **AI Red Team operations**, simulate real-world attacks on AI models, and develop robust security frameworks to safeguard AI-driven environments.

Upon successful completion, participants earn the **EC-Council Certified Offensive AI Security Professional (C|OASP)** credential — validating advanced expertise in **AI penetration testing, adversarial security, and defense**.

Bilginç IT Academy is an **Official Accredited Training Partner of EC-Council**, delivering EC-Council-authorized cybersecurity trainings and certification programs globally.

Who Should Attend

- Cybersecurity professionals and AI security specialists
- Red Team / Blue Team experts
- Machine learning engineers, data scientists
- Ethical hackers and penetration testers

What You Will Learn

By the end of this course, participants will:

- Understand the attack surface of AI systems
- Conduct adversarial, evasion, extraction, and poisoning attacks
- Perform offensive AI Red Team assessments
- Implement security controls for AI models and pipelines
- Apply Secure MLOps principles to protect model integrity
- Integrate ethical hacking methodologies into AI security practices

Training Outline

1. Introduction to AI Security

Certified Offensive AI Security Professional (C|OASP) Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

- Core concepts and threat landscape
- Attack surface analysis of AI and ML systems
- Common vulnerabilities in data, model, and API layers

2. Offensive AI Techniques (Red Team)

- Model inversion and data extraction attacks
- Data poisoning and model corruption
- Crafting adversarial examples and bypass methods
- Evasion and backdoor exploitation

3. Defensive AI Strategies (Blue Team)

- Secure model training and validation
- Model hardening and regularization
- Adversarial detection and mitigation
- Incident response in AI-driven environments

4. Tools and Frameworks

- AI Red Teaming toolkits
- TensorFlow, PyTorch, and ML security frameworks
- Explainable AI (XAI) for security evaluation
- AI security automation and testing tools

5. Legal, Ethical, and Regulatory Aspects

- Responsible AI security practices
- Compliance frameworks (EU AI Act, ISO/IEC, NIST AI RMF)
- AI governance and corporate security policies

6. Practical Labs

- Hands-on adversarial attack simulations
- AI model penetration testing
- Red Team operation exercises in controlled labs