

EC-Council Certified Offensive AI Security Professional (COASP) + Exam voucher

Duration: 5 Days Course Code: COASP

Overview:

Certified Offensive AI Security Professional (COASP) validates the competencies required for practitioners who need to demonstrate offensive AI security skills, emulating adversaries, validating defenses, and leading red-team/blue-team exercises to keep AI resilient, reliable, and auditable.

The Certified Offensive AI Security Professional (COASP) equips you to identify and neutralize AI-specific threats before attackers do. And Bridges security, engineering, and data science so controls exist across the full AI life cycle.

Participants will gain hands-on experience to perform end-to-end adversarial testing and deliver defensive validation evidence including the ability to simulate adversarial AI kill chains, Harden AI architectures by secure system prompts, context windows, tool integrations, RAG pipelines, and agent memory, Conducting AI security assessments aligned to MITRE ATLAS, OWASP LLM/ML Top 10, NIST AI RMF, and DoD Test & Evaluation practices, This course covers how to build SOC-ready capabilities for AI-focused detection logic, incident playbooks, and forensic procedures, & how to execute prompt injection, adversarial prompting, Assess AI supply-chain risk, Implement defensive engineering controls and Produce assurance and compliance artifacts.

By the end of the course, learners will be well-prepared to take the Certified Offensive AI Security Professional (COASP) exam and demonstrate the ability to exploit vulnerabilities in LLMs and agents, and build defense that survive real world attacks, learners will master offensive techniques that break AI before the attackers do

This course includes an exam voucher.

Target Audience:

This course is ideal for security professionals who wish to master offensive and defensive AI security techniques:

OFFENSIVE SECURITY

- Penetration Tester/Ethical Hacker
- Red Team Operator/Red Team Lead
- Offensive Security Engineer
- Adversary Emulation/Purple Team Specialist

DEFENSIVE SECURITY

- SOC Analyst (Tier 2/3)/Detection Engineer
- Blue Team Engineer/Threat Detection Engineer
- Incident Responder (IR)/DFIR Analyst
- Security Operations Manager (SOC Lead)

THREAT INTELLIGENCE

- Malware Analyst/Threat Researcher
- Cyber Threat Intelligence (CTI) Analyst – AI Focus
- Fraud/Abuse Detection Analyst (AI-enabled threats)

AI/ML ENGINEERING

- ML Engineer/Applied AI Engineer
- GenAI Engineer (RAG/Agents)
- AI/LLM Application Developer
- MLOps/AI Platform Engineer

SECURITY ENGINEERING

- DevSecOps/Secure DevOps Specialist
- Application Security Engineer (LLM Apps/APIs)
- Product Security Engineer/AI Product Security

AI SECURITY ARCHITECTURE

- Secure AI Engineer/AI Security Architect
- LLM Systems Engineer

Objectives:

- After this course participants should be able to:
 - Apply OWASP LLM Top 10 and MITRE ATLAS frameworks
 - Execute prompt injection, jailbreaking, and prompt chaining attacks
 - Conduct adversarial ML attacks, including data poisoning and model extraction
 - Red-team AI agents, including memory corruption, tool misdirection, and checkpoint manipulation
 - Build detection rules and hardening strategies for AI systems

Prerequisites:

- EC-AIE - EC-Council Artificial Intelligence Essentials (AIE) + Exam voucher

Testing and Certification

Certified Offensive AI Security Professional COASP certification equips candidates to validate advanced skills in offensive testing, assessment, and defense of artificial intelligence systems. It is designed for cybersecurity professionals who are responsible for identifying, exploiting, and mitigating vulnerabilities unique to AI driven technologies, including machine learning models, generative AI systems, and AI supply chains.

- Certified Offensive AI Security Professional (COASP)
-

Follow-on-Courses:

Learners can progress to EC-Council's Certified AI Program Manager (C|AIPM) or Certified Responsible AI Governance & Ethics (C|RAGE), depending on career goals.

- CAIPM - EC-Council Certified AI Program Manager (CAIPM) + Exam voucher
 - CRAGE - EC-Council Certified Responsible AI Governance & Ethics (CRAGE) + Exam voucher
-

Content:

Module 1 Offensive AI and AI System Hacking Methodology	Module 5 Adversarial Machine Learning and Model Privacy Attacks	Module 9 AI Security Testing, Evaluation, and Hardening
Module 2 AI Reconnaissance and Attack Surface Mapping	Module 6 Data and Training Pipeline Attacks	Module 10 AI Incident Response and Forensics
Module 3 AI Vulnerability Scanning and Fuzzing	Module 7 Agentic AI and Model-to-Model Attacks	
Module 4 Prompt Injection and LLM Application Attacks	Module 8 AI Infrastructure and Supply Chain Attacks	

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo