COASP - CERTIFIED OFFENSIVE AI SECURITY PROFESSIONAL

Course Code: 840113

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.

What You'll Learn

By the end of the course, you should be able to:

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

Who Needs to Attend

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

COASP - CERTIFIED OFFENSIVE AI SECURITY PROFESSIONAL

Course Code: 840113

CLASSROOM LIVE	$2,995 USD	5 Day

Classroom Live Outline

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

COASP - CERTIFIED OFFENSIVE AI SECURITY PROFESSIONAL

Course Code: 840113

VIRTUAL CLASSROOM LIVE	$2,995 USD	5 Day

Virtual Classroom Live Outline

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

Jul 20 - 24, 2026 | 9:00 AM - 5:00 PM EDT

Aug 24 - 28, 2026 | 9:00 AM - 5:00 PM EDT

Oct 26 - 30, 2026 | 9:00 AM - 5:00 PM EDT

Nov 30 - Dec 4, 2026 | 9:00 AM - 5:00 PM EST

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/24/2026 4:43:49 AM