# Certified Offensive AI Security Professional (COASP)

**Category:** AI, Data & Analytics | **Vendor:** EC-Council

**Duration:** 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

## Course Information

| | |
|---|---|
| **Delivery Format:** | Instructor Led - Online |
| **Certification:** | Certified Offensive AI Security Professional (COASP) |
| **Related Exam:** | COASP |

## Course Overview

AI is transforming products, operations, and decision-making across industries. But when AI systems move into production, they open new attack paths, through models, prompts, data pipelines, agent workflows, APIs, and integrations, creating vulnerabilities adversaries are already targeting. Traditional pentesting doesn’t fully cover LLM vulnerabilities. Prompt injection, data poisoning, and model manipulation require specialized offensive skills. Certified Offensive AI Security Professional is the first credential built specifically for AI red teamers.

## Who Should Attend

Penetration Testers / Ethical Hackers, Red Team / Offensive Security Specialists, Security Engineers / DevSecOps Engineers, SOC Analysts / Incident Responders, AI/ML Engineers focused on security

## Prerequisites & Entry Requirements

**General Prerequisites:**

Strong technical background recommended, Requires: 2–3 years of cybersecurity experience, with understanding of security operations, networks or application security and offensive security experience

# Detailed Course Outline

## Module 01: Offensive AI and AI System Hacking Methodology

- AI & ML Fundamentals
- AI Attack Surface and Threat Landscape (ATLAS-Aligned)
- AI Attack Taxonomy and Classification
- OWASP LLM and ML Top 10 (2025) – Overview & Mapping
- AI System Hacking Methodology
- Securing AI Systems – Foundations (Defensive Anchor)
- AI Security Governance and Compliance

## Module 02: AI Reconnaissance and Attack Surface Mapping

- OSINT for AI Assets
- Tools and Techniques for AI OSINT
- Data & Training Pipeline Intel Gathering
- Mapping AI Attack Surfaces from OSINT
- Discovering AI Endpoints & Services
- AI API & Parameter Enumeration
- Model & Vector Store Enumeration
- Defensive – Reducing AI OSINT Exposure
- Defensive – Hardening Enumerated Surfaces
- AI Threat Intelligence & Continuous Monitoring

## Module 03: AI-Specific Vulnerability Scanning and Fuzzing

- Fundamentals of AI Vulnerability Assessment
- Tools and Techniques for Vulnerability Scanning
- Fuzzing Techniques for AI Systems
- Defensive – Integrating Scanning & Fuzzing

## Module 04: Prompt-Based and LLM Application Attacks

- LLM Architecture & Trust Boundaries
- Prompt Injection & Jailbreaking
- Sensitive Information Disclosure and System Prompt Leakage
- Improper Output Handling and Misinformation
- Advanced Prompt Attack Techniques
- Defensive – Secure LLM Application Design

## Module 05: Adversarial Machine Learning and Model Privacy Attacks

- Adversarial ML Attacks
- Practical Adversarial Input Attacks
- Privacy & Model Extraction Attacks
- Evaluating Robustness & Trustworthiness
- Emerging Model Attack Techniques
- Defensive – Privacy & Robustness Mitigations

## Module 06: Data and Training Pipeline Attacks

- Understanding AI Data & Training Pipelines
- Data Poisoning Attacks
- Backdoor / Trojan Attacks in Training Pipelines
- AI Supply Chain Attack Vectors
- Defensive – Securing Data & Training Pipelines

## Module 07: Agentic AI and Model-to-Model Attacks

- Agentic AI Architecture & Attack Surface
- Excessive Agency & Autonomy
- Model-to-Model and Cross-LLM Attacks
- Unbounded Consumption and Denial of Wallet
- AI Workflow and Orchestration Attacks
- Defensive – Securing Agentic Applications

## Module 08: AI Infrastructure and Supply Chain Attacks

- AI Infrastructure & Integration Landscape
- System and Framework Exploits
- Tool and API Abuse in AI Apps
- Supply Chain Threats (Deep Dive)
- Defensive – Hardening AI Infra & Supply Chain

### Module 09: AI Security Testing, Evaluation, and Hardening

- AI Security Test & Evaluation Fundamentals
- Designing AI Security Test Plans
- Executing AI Security Tests
- Reporting, Assurance & Risk Management
- Defensive – Embedding T&E into MLOps/DevSecOps

### Module 10: AI Incident Response, Forensics, and Capstone Red Team

- Detecting & Responding to AI-Specific Incidents
- Logging, Telemetry & Evidence Collection
- AI Forensics & Post-Incident Analysis
- Capstone: Full-Scope AI Red Team Engagement
- Course Wrap-Up & Professional Practice

### □□ Certification Path

Certified Offensive AI Security Professional (COASP)

Exam: COASP

# Frequently Asked Questions

### Q: What delivery options are available for Certified Offensive AI Security Professional (COASP)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

---

### Q: What certification does this course prepare me for?

The Certified Offensive AI Security Professional (COASP) course helps prepare you for the Certified Offensive AI Security Professional (COASP) certification path.

---

### Q: Which exam does this course prepare me for?

This course prepares you for the COASP official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

---

### Q: How many CPD hours does this course provide?

The 5-day Certified Offensive AI Security Professional (COASP) course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

---

### Q: What is the duration of the Certified Offensive AI Security Professional (COASP) training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

---

### Q: Do you provide corporate training for Certified Offensive AI Security Professional (COASP)?

Yes, we provide corporate training, dedicated training, and closed classes for Certified Offensive AI Security Professional (COASP). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

---

### Q: Why choose Nexus Human for Certified Offensive AI Security Professional (COASP)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

---

### Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Certified Offensive AI Security Professional (COASP) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.


## Nexus Human

**Professional Training & Development**

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)


© 2026 Nexus Human. All rights reserved. This brochure was generated on 13/11/2026.