

INFOSEC Boot Camps

CERTIFICATION TRAINING 

Get live, expert
instruction from anywhere.



Certified Offensive AI Security Professional (C|OASP) Boot Camp

Master the tactical methodology to hack LLMs and secure agentic AI. EC-Council's C|OASP credential validates that you can red-team AI systems, exploit vulnerabilities in LLMs and agents, and build defenses that survive real-world attacks. This is the first credential built specifically for AI red teamers.

Course description

C|OASP is a hands-on, practitioner-level credential that validates your ability to ethically attack AI systems so you can defend them with engineering-grade controls. C|OASP is not about building AI models or running AI programs. It is about proving you can think like an attacker inside AI systems, uncover weaknesses across models and pipelines, validate security controls, and reduce operational risk before deployment.

This is the only credential built for offensive AI security work with outcomes you can demonstrate. C|OASP trains you to perform end-to-end adversarial testing and deliver defensive validation evidence.

Who should attend

- » Penetration Tester/Ethical Hacker
- » Red Team Operator/Red Team Lead
- » Offensive Security Engineer
- » Adversary Emulation/Purple Team Specialist
- » SOC Analyst (Tier 2/3)/Detection Engineer
- » Incident Responder (IR)/DFIR Analyst
- » ML Engineer/Applied AI Engineer
- » Secure AI Engineer/AI Security Architect

Boot camp at a glance



What you'll learn

- ✓ AI system hacking methodology
- ✓ Prompt injection and jailbreaking attacks
- ✓ Adversarial ML and model extraction
- ✓ Data poisoning and pipeline attacks
- ✓ Agentic AI exploitation
- ✓ AI supply chain attacks
- ✓ AI incident response and forensics



Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite



Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Boot Camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to hundreds of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.



Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.



Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.



Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.



1,800+ IT and security courses

Earn CPEs and build new skills with hundreds of additional training courses.

What's included

- » Five days of expert, live instruction
- » Exam Pass Guarantee
- » Exam voucher
- » Unlimited practice exam attempts
- » 100% Satisfaction Guarantee
- » Free 90-day Infosec Skills subscription (access to 1,800+ additional courses and lab)
- » 90-day extended access to Boot Camp components, including class recordings
- » Knowledge Transfer Guarantee

Prerequisites

2 years of cybersecurity experience. C|OASP is designed for security professionals who wish to master offensive and defensive AI security techniques.

Certification details

The C|OASP exam covers 10 module areas:

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

INFOSEC Boot Camps

CERTIFICATION TRAINING 

Enroll today: 866.471.0059 | infosecinstitute.com

Exam information

- » Exam Title: Certified Offensive AI Security Professional (C|OASP)
- » Exam Code: 312-52
- » Number of Questions: 70 (65 MCQ + 5 PBQ)
- » Duration: 6 hours
- » Passing Score: 70-80%
- » Test Format: Multiple Choice Questions and Performance-Based Questions
- » Availability: ECC Exam Portal

Key features of C|OASP certification

- » Hands-on Labs First: 30 practical exercises across modules covering prompt injection, model extraction, adversarial attacks, and red vs. blue scenarios
- » DCWF-aligned Learning Path: Labs map to DoD/NICE DCWF KSAs such as reconnaissance, exploitation, extraction, and threat hunting
- » Full Adversarial Life Cycle Coverage: Progress from recon and prompt exploitation to memory manipulation, supply-chain compromise, and risk reporting
- » First credential built specifically for AI red teamers
- » 20+ key tools covered including Garak, PyRIT, Burp Suite, CleverHans, ART, Foolbox, and more
- » 15+ MITRE ATLAS techniques covered in the program
- » Offensive AI Security Methodology: RECON → EXPLOIT → DEFEND

What's new in the C|OASP Program

- » First credential built specifically for AI red teamers
- » Aligned to OWASP LLM Top 10 (2025), OWASP ML Security Top 10 (2025), and OWASP Top 10 for Agentic Applications
- » Coverage of 15+ MITRE ATLAS techniques
- » 20+ key offensive AI security tools covered (Garak, PyRIT, CleverHans, ART, Foolbox, and more)
- » Full adversarial life cycle coverage: reconnaissance to exploitation to hardening

- » Capstone: Full-Scope AI Red Team Engagement
- » DCWF-aligned learning path mapped to DoD/NICE DCWF KSAs
- » Coverage of agentic AI attacks including memory corruption, tool misdirection, and checkpoint manipulation

Hands-on lab environment

- » 30 practical exercises across modules covering prompt injection, model extraction, adversarial attacks, and red vs. blue scenarios
- » Labs map to DoD/NICE DCWF KSAs such as reconnaissance, exploitation, extraction, and threat hunting
- » Progress from recon and prompt exploitation to memory manipulation, supply-chain compromise, and risk reporting

Recommendations and accreditations

- » MITRE ATLAS Framework - Program aligned to MITRE ATLAS adversarial threat landscape for AI systems
- » OWASP LLM Top 10 (2025) - Comprehensive coverage of LLM-specific vulnerabilities and threats
- » OWASP ML Security Top 10 (2025) - Machine learning security risk mapping
- » OWASP Top 10 for Agentic Applications - Coverage of autonomous AI agent vulnerabilities
- » DoD AI Test & Evaluation Specialist (672) Framework - Aligned to Department of Defense AI T&E practices
- » NIST AI Risk Management Framework - Compliance artifacts mapped to NIST AI RMF

INFOSEC Boot Camps

CERTIFICATION TRAINING 

Enroll today: 866.471.0059 | infosecinstitute.com

Target job roles

- » AI Red Team Specialist/Adversarial AI Engineer
- » Offensive Security Engineer (AI/LLM)
- » Adversarial AI Security Analyst/AI Threat Hunter
- » AI Incident Response Engineer/AI Forensics Analyst
- » Secure AI Engineer/AI Security Architect
- » MLOps/AIOps Security Specialist
- » AI Model Risk/AI Risk & Assurance Specialist
- » LLM Systems Engineer
- » AI Product Security Manager/AI Security Program Manager
- » CTI Analyst (AI Focus)/AI Risk Advisor

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Skill up and get certified, guaranteed



Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.



100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.



Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

INFOSEC Boot Camps

CERTIFICATION TRAINING 

Enroll today: 866.471.0059 | infosecinstitute.com

Certified Offensive AI Security Professional (C|OASP) details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Offensive AI and AI System Hacking Methodology – AI & ML fundamentals Attack surfaces, threat landscape (ATLAS-aligned) OWASP LLM & ML Top 10 (2025) AI system hacking methodology	AI Vulnerability Scanning and Fuzzing – Vulnerability assessment fundamentals Scanning tools and techniques Fuzzing methods for AI systems and model interfaces	Adversarial Machine Learning and Model Privacy Attacks – Adversarial ML attack classes Adversarial input attacks Privacy & model extraction attacks Robustness evaluation	Agentic AI and Model-to-Model Attacks – Agentic AI architecture, excessive agency exploitation Cross-LLM attacks Denial-of-wallet risks AI workflow and orchestration attacks	AI Security Testing, Evaluation, and Hardening – Security testing methodologies Red team frameworks Vulnerability validation and reporting Hardening best practices
Afternoon session	AI Reconnaissance and Attack Surface Mapping – OSINT for AI assets Data & training pipeline intel gathering AI endpoint discovery API enumeration Model & vector store enumeration	Prompt Injection and LLM Application Attacks – LLM architecture & trust boundaries Prompt injection & jailbreaking Sensitive information disclosure System prompt leakage Advanced prompt attack techniques	Data and Training Pipeline Attacks – AI data pipeline architecture Data poisoning attacks Backdoor/trojan insertion AI supply chain attack vectors	AI Infrastructure and Supply Chain Attacks – AI infrastructure components System and framework exploits Tool and API abuse Supply chain threats Hardening strategies	AI Incident Response and Forensics – Detecting AI-specific incidents Logging & telemetry AI forensics Post-incident analysis Capstone: Full-Scope AI Red Team Engagement

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Module 01: Offensive AI and AI System Hacking Methodology

Build a foundation in offensive AI security by learning how AI systems are designed, where they fail, and how adversaries exploit them, using structured

hacking methodologies and globally recognized AI security frameworks.

- » 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

INFOSEC Boot Camps

CERTIFICATION TRAINING 

Enroll today: 866.471.0059 | infosecinstitute.com

Module 02: AI Reconnaissance and Attack Surface Mapping

Learn advanced AI-focused OSINT techniques to identify, enumerate, and analyze AI assets, data pipelines, models, APIs, and attack surfaces, and apply exposure mitigation and hardening strategies.

- » 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
- » AI Threat Intelligence & Continuous Monitoring

Module 03: AI Vulnerability Scanning and Fuzzing

Master AI-specific vulnerability assessment and fuzzing techniques to identify, analyze, and mitigate security weaknesses across modern AI systems and applications.

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

Module 04: Prompt Injection and LLM Application Attacks

Analyze and exploit LLM trust boundaries using advanced prompt injection, jailbreaking, and output manipulation techniques, while identifying risks related to sensitive data exposure and insecure LLM application design.

- » 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

Execute and analyze adversarial machine learning, privacy, and model extraction attacks to assess AI system robustness, trustworthiness, and risk, and apply defensive strategies to mitigate them.

- » 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

Compromise AI systems through data poisoning and backdoor insertion targeting training pipelines and model integrity.

- » 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

Analyze and exploit autonomous AI agents and multi-model architectures by targeting excessive agency, cross-LLM interactions, orchestration workflows, and unbounded resource consumption.

- » 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

INFOSEC Boot Camps

CERTIFICATION TRAINING 

Enroll today: 866.471.0059 | infosecinstitute.com

Module 08: AI Infrastructure and Supply Chain Attacks

Explore offensive techniques targeting AI infrastructure, system integrations, and third-party dependencies, while learning how to identify, exploit, and harden AI supply chain weaknesses.

- » 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

Apply structured AI security testing and evaluation methodologies to assess risk, validate controls, and implement hardening best practices across enterprise AI systems.

- » 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 and Forensics

Master AI-specific incident response and forensics, concluding with hands-on engagement in AI red team activities.

- » 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

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec Institute makes cybersecurity workforce readiness measurable. We help organizations build skills and verify performance across their entire workforce, providing leaders with clear visibility into who's ready to defend, where capability gaps exist and whether training investment is delivering results. By combining expert training with AI-powered verification, we give organizations confidence backed by data. 70% of the Fortune 500 have trusted Infosec for more than two decades. Learn more at infosecinstitute.com.