C|OASP
Certified Offensive AI Security Professional

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

OFFENSIVE AI SECURITY AND RED TEAM OPERATIONS

CERTIFIED OFFENSIVE AI SECURITY PROFESSIONAL

DEAC DISTANCE EDUCATION ACCREDITING COMMISSION
CHEA A CHEA-recognized Accrediting Organization
ANAB ANSI National Accreditation Board ACCREDITED PERSONNEL CERTIFICATION BODY
RANKED AMONG TOP 10 BY FORTUNE® FOR IT'S ONLINE CYBERSECURITY MASTER'S DEGREE
FORTUNE BEST ONLINE MASTER'S CYBERSECURITY DEGREES

Course Description

As AI becomes increasingly embedded into organizational workflows, it presents new cyberattack vectors through language models, prompts, data pipelines, agentic functions, APIs, and other integrations. This course equips you with specialized offensive cybersecurity skills to red-team AI systems end-to-end. From prompt injection to model exploitation and everything in between, you'll master offensive cybersecurity techniques to detect compromises in AI systems before cybercriminals do. You'll deepen your understanding of AI and machine learning fundamentals from an offensive security perspective, while learning how to identify AI attack surfaces, threat landscapes, and adversary techniques.

Course Learning Outcomes

Upon successful completion of this course, you will be able to:

01 Apply AI system hacking methodologies, frameworks, and risk implications.

Apply OSINT tools and techniques to identify and profile AI assets. 02

03 Discover and map AI attack surfaces using intelligence gathered from AI data sources, training pipelines, and publicly available intelligence.

Identify and analyze AI models and vector stores from an attacker's perspective. 04

05 Use tools and techniques for scanning vulnerabilities in AI models, pipelines, and deployments.

Who is it for?

This course is ideal for:

Offensive cybersecurity professionals like ethical hackers, penetration testers, cybersecurity engineers, red team specialists, and more.

Defensive cybersecurity professionals like SOC analysts, incident responders, IT security analysts, and more.

Cyber threat intelligence specialists like threat intelligence analysts, threat researchers, risk assessment experts, and more

Professionals involved in AI & ML engineering, AI application development, Gen AI training, AI/ML Ops, LLM systems engineering, and more

Professionals specializing in DevSecOps, AI product security, secure application development, and cloud security

Program Highlights

DURATION
10 weeks

STUDY HOURS
Students need to put in about 13.5 hours a week

LIVE CLASSES
Once a week

FACULTY
Industry Experts

The ECCU Impact

93% of graduates get jobs at leading organizations after completing the program

82% of graduates report career enhancement.

2 out of 3 graduates get new job roles within 6 months of program completion.

1 out of 2 graduates secure job roles paying $100K+ annual salaries.

**Source: ECCU Consumer Information Disclosure Form*

C|OASP Certified Offensive AI Security Professional

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

A Trusted Methodology for Offensive AI Security

The C|OASP certification course emphasizes a 3-step methodology for a systematic approach to securing AI systems against adversarial threats:

Step 1
RECON

Map AI system architectures, enumerate exposed endpoints, and build threat models. Profile training pipelines, data flows, and inference APIs to identify where defenses are weakest.

Step 2
EXPLOIT

Execute prompt injection, jailbreaking, data poisoning, and model extraction attacks to validate AI system vulnerabilities and document exploitation gaps.

Step 3
DEFEND

Implement guardrails, detection mechanisms, and incident response procedures to harden AI systems and ensure resilient, secure deployments.

Why Traditional Cybersecurity is Inadequate to Protect AI Systems

Evolving AI systems introduce novel attack vectors that traditional cybersecurity tools and techniques cannot detect or prevent:

Prompt Injection	Attackers manipulate LLMs to bypass safety protocols and access sensitive data
Model Extraction	Adversaries steal proprietary AI models through careful querying
Data Poisoning	Attackers manipulate training data to create backdoors that activate under specific conditions
Jailbreaking	Sophisticated prompts override safety mechanisms and cause AI to produce harmful outputs

C|OASP Certified Offensive AI Security Professional

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Why the Demand for Offensive AI Security Experts is Soaring

85% of tech companies worldwide have already adopted AI.
(Source: Investopedia)

53% of manufacturers report using AI in at least one business function.
(Source: Markets and Markets)

The value of AI solutions for banking and finance is projected to reach **$190 billion** by 2030.
(Source: Capgemini)

70+ countries have developed and implemented AI strategies or policies.
(Source: OECD)

70% of healthcare providers are using AI in some capacity in business operations.
(Source: McKinsey & Co.)

Course Outline

Module 01:
Offensive AI and AI System Hacking Methodology

Week 1

Module 02:
AI Reconnaissance and Attack Surface Mapping

Week 2

Module 03:
AI Vulnerability Scanning and Fuzzing

Week 3

Module 04:
Prompt Injection and LLM Application Attacks

Week 4

Module 05:
Adversarial Machine Learning and Model Privacy Attacks

Week 5

Module 06:
Data and Training Pipeline Attacks

Week 6

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

Week 7

Module 08:
AI Infrastructure and Supply Chain Attacks

Week 8

Module 09:
AI Security Testing, Evaluation, and Hardening

Week 9

Module 10:
AI Incident Response and Forensics

Week 10

(Pre-requisite: Students must have at least 3 years of cybersecurity experience)

C|OASP Certified Offensive AI Security Professional

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Attaining the C|OASP Certification

Number of Questions
70

Test Format
Multiple-Choice and Performance-Based Questions

Duration
6 hours

Availability:
ECCU Exam Portal

Earning Potential with the C|OASP Certification

Annual salary range for an AI Security Engineer in the U.S.

$144,000
to
$227,000

(Salary figures are influenced by experience and the industrial sector – Source: Glassdoor)

Common Job Roles

- AI Security Engineer
- AI Red Team Specialist
- Offensive Security Engineer (AI/LLM)
- Adversarial AI Security Analyst
- AI Threat Hunter
- AI Incident Response Engineer
- AI Forensics Analyst
- MLOps/AIOps Security Specialist
- LLM Systems Engineer
- AI Model Risk/AI Risk & Assurance Specialist
- AI Product Security Manager
- AI Security Program Manager
- Cyber Threat Intelligence Analyst (AI Focus)
- AI Risk Advisor
- And Many More!

Unveil the True University Experience!

- Flexible Online Learning
- Hands-On Experience
- Faculty of Experts
- Industry Aligned Curriculum
- Globally Respected Certifications
- Credit Transfers
- Scholarships & Payment Plans
- 24/7 Access to Learning Resources
- International Networking

Meet Our Faculty

Jason Clark, Ph.D.

Yuri Diogenes, MS

Dr. Kanchan Panta, D.Sc.

Adrianna Davis, MS

Brian McDaniel, MS

Julie Beck, MS

Franklin Orellana, DBA

Dr. Donnel Hinkins, Ph.D.

Holistic Education at ECCU

Acquire in-depth knowledge through ECCU's vast library of resources.

Master technical skills with hands-on practice in ECCU's virtual labs.

Enhance soft skills, such as business communication and problem-solving.

What Our Students Say

My experience at ECCU has been very positive and empowering. I found that studying here is very flexible and friendly. The learning environment is responsive and supports challenging coursework, which is good because I like to be challenged. The MCS program combines technical depth with practical applications, which allows you to be postured for your next promotion. That's what I love most about ECCU.

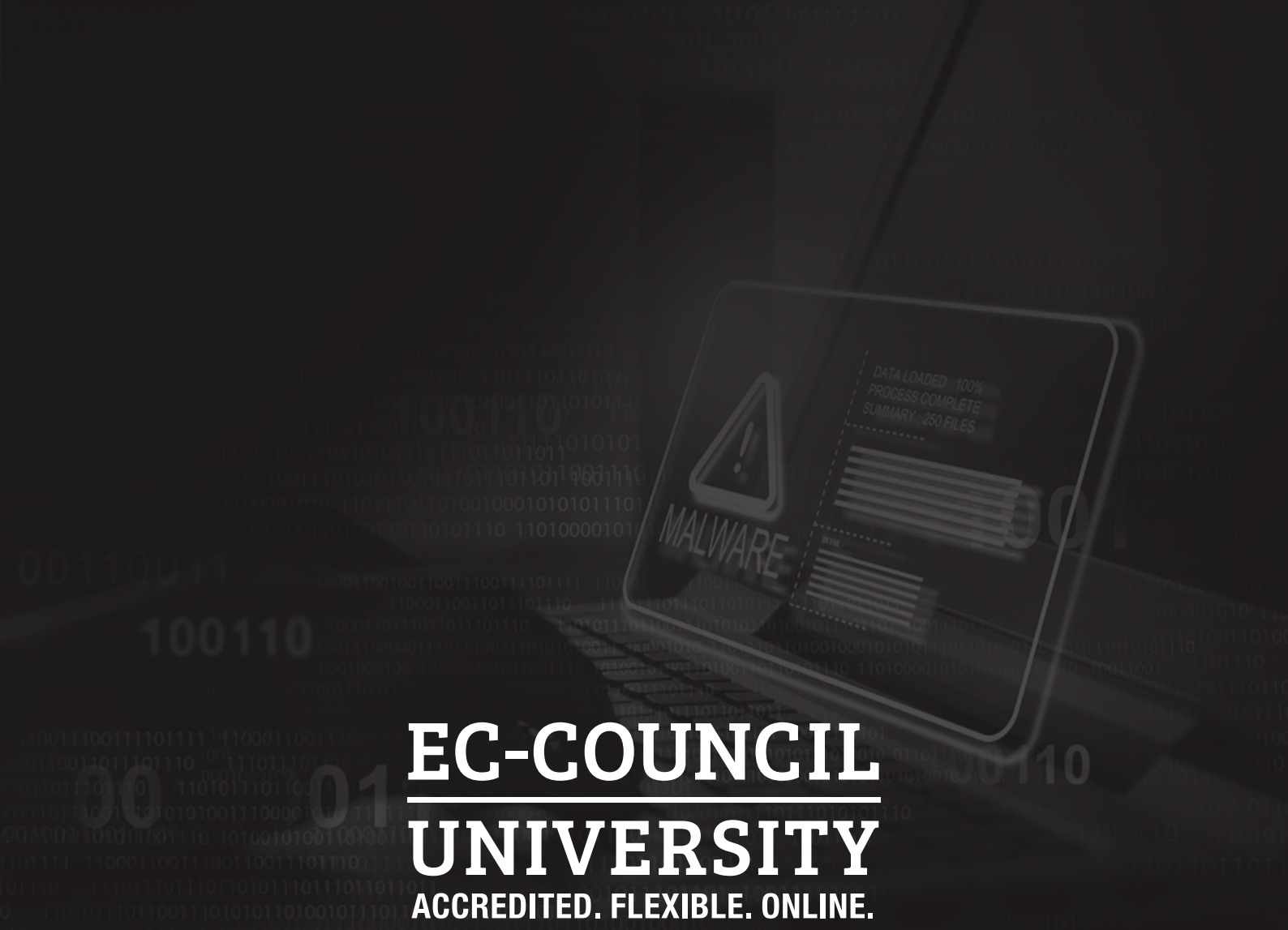
Unlike programs that focus solely on theory, ECCU emphasizes resume-boosting experience. The lab projects mirror real-world scenarios, which can add value to your resume. I think that's pretty awesome.

I absolutely recommend ECCU to anyone who wants a successful career in cybersecurity or computer science.

Retired Major Timothy Amerson
Master of Science in Computer Science Graduate
U.S.A.

It was a pretty easy choice to select EC-Council University. The master's degree significantly advanced my career in a way that really opened my eyes. Deepening my knowledge of cybersecurity equipped me to be ready for advanced roles. I think it's the best decision I've made in my life.

Xerxes Phillip
Master of Science in Cybersecurity Graduate
Hong Kong



EC-COUNCIL UNIVERSITY

ACCREDITED. FLEXIBLE. ONLINE.

EC-Council University 101 Sun Ave NE #C Albuquerque, NM 87109, United

info@eccu.edu www.eccu.edu