# AI+ Ethical Hacker Practitioner™

AI CERTs

Com certificação

- **Nível:**
- **Duração:** 40h

---

## Sobre o curso

A certificação **AI+ Ethical Hacker Practitioner™** foi desenvolvida para capacitar profissionais a integrar a Inteligência Artificial em práticas de cibersegurança e ethical hacking, de forma estruturada, prática e alinhada com a evolução das ameaças digitais. O foco está na utilização da IA para identificar vulnerabilidades, automatizar testes de segurança e reforçar mecanismos de defesa em sistemas cada vez mais complexos.

Ao longo do percurso, os participantes exploram como combinar técnicas tradicionais de ethical hacking com capacidades avançadas de IA, incluindo automação de reconhecimento, análise de vulnerabilidades, deteção de ameaças e resposta a incidentes. São também abordados temas como machine learning aplicado à cibersegurança, análise comportamental e proteção de sistemas de IA, permitindo uma visão integrada da segurança no contexto atual.

A componente prática assume um papel central, com exercícios, simulações e um capstone project que permitem aplicar técnicas de ataque e defesa em cenários reais, reforçando a capacidade de atuar num contexto de cibersegurança orientado por IA.

Em parceria com a Rumos, Platinum Gold Partner.

---

## Destinatários

- Profissionais de cibersegurança e ethical hacking;
- Analistas de segurança e penetration testers;
- Profissionais de IT interessados em segurança ofensiva e defensiva com IA;
- Especialistas em redes e sistemas que pretendam reforçar competências em segurança;
- Profissionais interessados em desenvolver carreira em cibersegurança com IA

## Objetivos

- Compreender a integração entre IA e ethical hacking;
- Aplicar técnicas de IA na identificação de vulnerabilidades e testes de penetração;
- Utilizar machine learning para deteção de ameaças e análise comportamental;
- Automatizar processos de cibersegurança e resposta a incidentes;
- Proteger sistemas de IA contra ataques adversariais;
- Aplicar princípios éticos e legais na utilização de IA em cibersegurança;
- Desenvolver competências práticas em cenários reais de segurança digital.

## Condições

**Detalhes do exame**

- Duração: 90 minutos;
- Pontuação mínima de aprovação: 70%;
- Formato: 50 questões de escolha múltipla;
- Realização online com supervisão remota (proctoring).

## Pré-requisitos

- Conhecimentos básicos de cibersegurança e redes;
- Familiaridade com conceitos de ethical hacking;
- Conhecimentos introdutórios de Inteligência Artificial são benéficos, mas não obrigatórios;
- Interesse em segurança informática e proteção de sistemas digitais.

## Metodologia

A formação decorre em formato e-learning, com aproximadamente 40 horas de conteúdos on-demand, incluindo vídeos, e-book, podcasts e atividades práticas interativas. A aprendizagem pode ser realizada em qualquer momento e a partir de qualquer lugar, com quizzes modulares para acompanhar o progresso.

## Programa

- Course Introduction
- Foundations of Ethical Hacking and AI
- AI Tools and Technologies for Ethical Hacking
- AI-Driven Reconnaissance and Intelligence Gathering
- AI-Based Vulnerability Assessment and Penetration Testing

- Machine Learning for Threat and Behavioral Analysis
- AI-Enabled Incident Response and IAM
- Securing AI Systems and Adversarial Defense
- Ethics, Governance, and Capstone Project

**Course Introduction**

**Foundations of Ethical Hacking and AI**

- Core principles of ethical hacking and cybersecurity
- Legal, ethical, and regulatory considerations
- Ethical hacking lifecycle and methodologies
- Role of artificial intelligence in modern ethical hacking

**AI Tools and Technologies for Ethical Hacking**

- Overview of AI, Machine Learning (ML), and Deep Learning (DL) in cybersecurity
- AI-powered security and hacking tools
- Automation of reconnaissance and vulnerability discovery
- Responsible use of AI-driven hacking tools

**AI-Driven Reconnaissance and Intelligence Gathering**

- Automated OSINT using AI
- AI-based network scanning and mapping
- Social engineering analysis and detection with AI
- Intelligence collection using ML-driven techniques

**AI-Based Vulnerability Assessment and Penetration Testing**

- AI-powered vulnerability scanning techniques
- Automated penetration testing workflows
- Dynamic testing, fuzzing, and exploit analysis
- Risk prioritization and remediation insights using AI

**Machine Learning for Threat and Behavioral Analysis**

- Supervised and unsupervised ML for threat detection
- User and Entity Behavior Analytics (UEBA)
- Network and endpoint anomaly detection
- AI-driven threat hunting and predictive analytics

**AI-Enabled Incident Response and IAM**

- Automated incident detection, triage, and response
- AI-driven threat intelligence integration
- AI-powered Identity and Access Management (IAM)
- Adaptive authentication and access control

**Securing AI Systems and Adversarial Defense**

- Threats targeting AI models and pipelines
- Adversarial AI attacks and defense strategies
- Securing AI training, deployment, and data integrity
- Model explainability, privacy, and governance

**Ethics, Governance, and Capstone Project**

- Ethical decision-making in AI-driven cybersecurity
- Bias, transparency, and accountability in AI systems
- Global compliance and legal frameworks
- Capstone project: end-to-end AI-powered ethical hacking scenario