AI CERTs™

AI Certification Program

AI+ Ethical Hacker™

Executive Summary

The AI+ Ethical Hacker certification delves into the intersection of cybersecurity and artificial intelligence, a pivotal juncture in our era of rapid technological progress. Tailored for budding ethical hackers and cybersecurity experts, it offers comprehensive insights into AI's transformative impact on digital offense and defense strategies. Unlike conventional ethical hacking courses, this program harnesses AI's power to enhance cybersecurity approaches. It caters to tech enthusiasts eager to master the fusion of cutting-edge AI methods with ethical hacking practices amidst the swiftly evolving digital landscape. The curriculum encompasses four key areas, from course objectives and prerequisites to anticipated job roles and the latest AI technologies in Ethical Hacking.

Certification Prerequisites

- Programming Proficiency: Knowledge of Python, Java, C++, etc for automation and scripting.
- Networking Fundamentals: Understanding of networking protocols, subnetting, firewalls, and routing.
- Operating Systems Knowledge: Proficiency in using Windows and Linux operating systems.
- Cybersecurity Basics: Familiarity with fundamental cybersecurity concepts, including encryption, authentication, access controls, and security protocols
- Machine Learning Basics: Understanding of machine learning concepts, algorithms, and basic implementation.
- Web Technologies: Understanding of web technologies, including HTTP/HTTPS protocols, and web servers.

Exam Blueprint

Number of Questions

50

Passing Score

35/50 or 70%

Duration

90 Minutes

Format

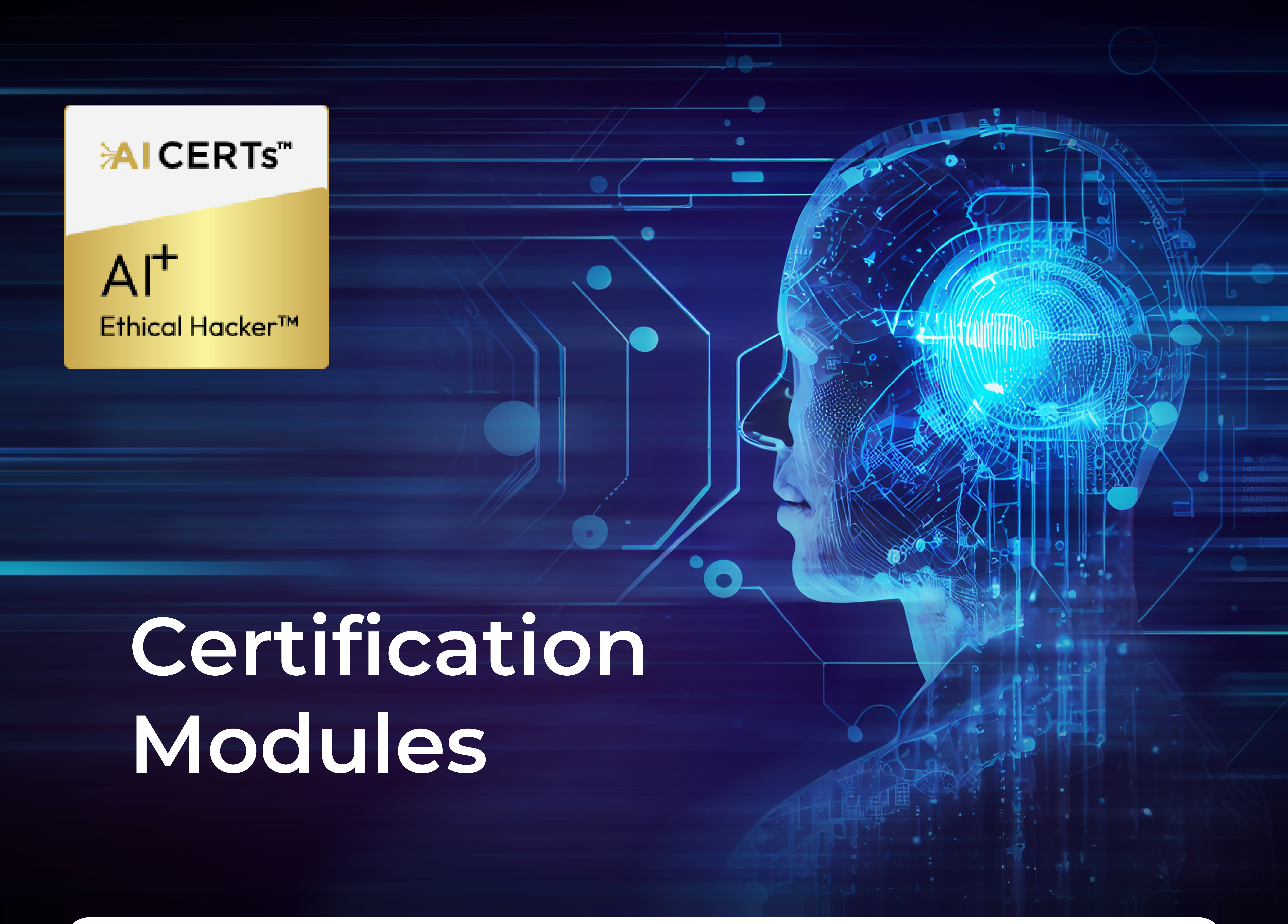
Online via AI Proctoring platform

Question Type

Multiple Choice/Multiple Response

Exam Overview

Module	Weight
Foundation of Ethical Hacking Using Artificial Intelligence (AI)	5%
Introduction to AI in Ethical Hacking	9%
AI Tools and Technologies in Ethical Hacking	9%
AI-Driven Reconnaissance Techniques	9%
AI in Vulnerability Assessment and Penetration Testing	9%
Machine Learning for Threat Analysis	9%
Behavioral Analysis and Anomaly Detection for System Hacking	9%
AI Enabled Incident Response Systems	9%
AI for Identity and Access Management (IAM)	9%
Securing AI Systems	9%
Ethics in AI and Cybersecurity	9%
Capstone Project	5%
	100%



AI CERTs™

AI+ Ethical Hacker™

Certification Modules

Module 1

Foundation of Ethical Hacking Using Artificial Intelligence (AI)

1.1 Introduction to Ethical Hacking

1.2 Ethical Hacking Methodology

1.3 Legal and Regulatory Framework

1.4 Hacker Types and Motivations

1.5 Information Gathering Techniques

1.6 Footprinting and Reconnaissance

1.7 Scanning Networks

1.8 Enumeration Techniques

Module 2

Introduction to AI in Ethical Hacking

2.1 AI in Ethical Hacking

2.2 Fundamentals of AI

2.3 AI Technologies Overview

2.4 Machine Learning in Cybersecurity

2.5 Natural Language Processing (NLP) for Cybersecurity

2.6 Deep Learning for Threat Detection

2.7 Adversarial Machine Learning in Cybersecurity

2.8 AI-Driven Threat Intelligence Platforms

2.9 Cybersecurity Automation with AI

Module 3

AI Tools and Technologies in Ethical Hacking

3.1 AI-Based Threat Detection Tools

3.2 Machine Learning Frameworks for Ethical Hacking

3.3 AI-Enhanced Penetration Testing Tools

3.4 Behavioral Analysis Tools for Anomaly Detection

3.5 AI-Driven Network Security Solutions

3.6 Automated Vulnerability Scanners

3.7 AI in Web Application

3.8 AI for Malware Detection and Analysis

3.9 Cognitive Security Tools

Module 4

AI-Driven Reconnaissance Techniques

4.1 Introduction to Reconnaissance in Ethical Hacking

4.2 Traditional vs. AI-Driven Reconnaissance

4.3 Automated OS Fingerprinting with AI

4.4 AI-Enhanced Port Scanning Techniques

4.5 Machine Learning for Network Mapping

4.6 AI-Driven Social Engineering Reconnaissance

4.7 Machine Learning in OSINT

4.8 AI-Enhanced DNS Enumeration & AI-Driven Target Profiling

Module 5

AI in Vulnerability Assessment and Penetration Testing

5.1 Automated Vulnerability Scanning with AI

5.2 AI-Enhanced Penetration Testing Tools

5.3 Machine Learning for Exploitation Techniques

5.4 Dynamic Application Security Testing (DAST) with AI

5.5 AI-Driven Fuzz Testing

5.6 Adversarial Machine Learning in Penetration Testing

5.7 Automated Report Generation using AI

5.8 AI-Based Threat Modeling

5.9 Challenges and Ethical Considerations in AI-Driven Penetration Testing

Module 6

Machine Learning for Threat Analysis

6.1 Supervised Learning for Threat Detection

6.2 Unsupervised Learning for Anomaly Detection

6.3 Reinforcement Learning for Adaptive Security Measures

6.4 Natural Language Processing (NLP) for Threat Intelligence

6.5 Behavioral Analysis using Machine Learning

6.6 Ensemble Learning for Improved Threat Prediction

Module 7

Behavioral Analysis and Anomaly Detection for System Hacking

Module 8

AI Enabled Incident Response Systems

8.1 Automated Threat Triage using AI

8.2 Machine Learning for Threat Classification

8.3 Real-time Threat Intelligence Integration

8.4 Predictive Analytics in Incident Response

8.5 AI-Driven Incident Forensics

8.6 Automated Containment and Eradication Strategies

8.7 Behavioral Analysis in Incident Response

8.8 Continuous Improvement through Machine Learning Feedback

8.9 Human-AI Collaboration in Incident Handling

Module 9

AI for Identity and Access Management (IAM)

9.1 AI-Driven User Authentication Techniques

9.2 Behavioral Biometrics for Access Control

9.3 AI-Based Anomaly Detection in IAM

9.4 Dynamic Access Policies with Machine Learning

9.5 AI-Enhanced Privileged Access Management (PAM)

9.6 Continuous Authentication using Machine Learning

9.7 Automated User Provisioning and De-provisioning

9.8 Risk-Based Authentication with AI

9.9 AI in Identity Governance and Administration (IGA)

Module 10

Securing AI Systems

10.1 Adversarial Attacks on AI Models

10.2 Secure Model Training Practices

10.3 Data Privacy in AI Systems

10.4 Secure Deployment of AI Applications

10.5 AI Model Explainability and Interpretability

10.6 Robustness and Resilience in AI

10.7 Secure Transfer and Sharing of AI Models

10.8 Continuous Monitoring and Threat Detection for AI

Module 11

Ethics in AI and Cybersecurity

11.1 Ethical Decision-Making in Cybersecurity

11.2 Bias and Fairness in AI Algorithms

11.3 Transparency and Explainability in AI Systems

11.4 Privacy Concerns in AI-Driven Cybersecurity

11.5 Accountability and Responsibility in AI Security

11.6 Ethics of Threat Intelligence Sharing

11.7 Human Rights and AI in Cybersecurity

11.8 Regulatory Compliance and Ethical Standards

11.9 Ethical Hacking and Responsible Disclosure

Module 12

Capstone Project

Certification Outcome

Upon successful completion of the AI+ Ethical Hacker certification, individuals validate their capability in harnessing AI methodologies to bolster cybersecurity measures. They acquire comprehensive skills encompassing core ethical hacking concepts, AI-powered reconnaissance, evaluating vulnerabilities, conducting penetration tests, analyzing threats, responding to incidents, and managing identities within cybersecurity frameworks. By showcasing adeptness in ethically employing AI resources, certified individuals actively bolster cybersecurity defenses and promote the ethical integration of AI, thereby reinforcing organizational resilience against ever-changing cyber risks.

Market Insight

Elevate your cybersecurity game with our Ethical Hacking and AI Integration course. Learn to leverage AI for advanced threat detection and response, ensuring robust protection against evolving cyber threats. Gain a competitive edge and become a leader in the next era of cybersecurity.

Value Proposition

Empower Your Cybersecurity Strategy with Ethical Hacking and AI Integration. Our course equips you with the tools and expertise to leverage AI for advanced threat detection and response, enhancing your organization's resilience against cyber threats. By mastering ethical hacking principles and AI-driven methodologies, you'll unlock new levels of security, safeguarding critical assets and ensuring business continuity. Join us to stay ahead in the ever-evolving landscape of cybersecurity and drive innovation in protecting digital assets.

Additional Features

Immersive Live Simulation Labs to Elevate your learning with hands-on, real-world scenarios. Practice ethical hacking and AI integration techniques in a safe environment, gaining practical insights and honing your skills to confidently tackle cybersecurity challenges. Our live simulation labs provide an unparalleled opportunity to apply classroom knowledge, ensuring you're fully prepared to defend against evolving cyber threats.

AI Experts

Jason Kellington

AI Expert

As a consultant, trainer, and technical writer with more than 25 years of experience in IT, I specialize in the development and delivery of solutions focused on effective and efficient enterprise IT.

Justin Frébault

AI Expert

I'm a boutique data consultant specializing in data mesh and lakehouse solutions. I've dedicated my career to helping organizations transform their approach to data, moving beyond mere knowledge.

J Tom Kinser

AI Expert

I have over forty years of experience in software development, data engineering, management, and technical training. I am a Microsoft Certified Trainer and a software developer, holding multiple certifications.

Terumi Laskowsky

AI Expert

Country Manager for Global Consulting Services in Japan, Specialties: Information Security (Compliance, Policy, Application, Host, Network)

AICERTs™

AI & BITCOIN CERTIFICATIONS!

aicerts.io

Contact

252 West 37th St., Suite 1200W
New York, NY 10018