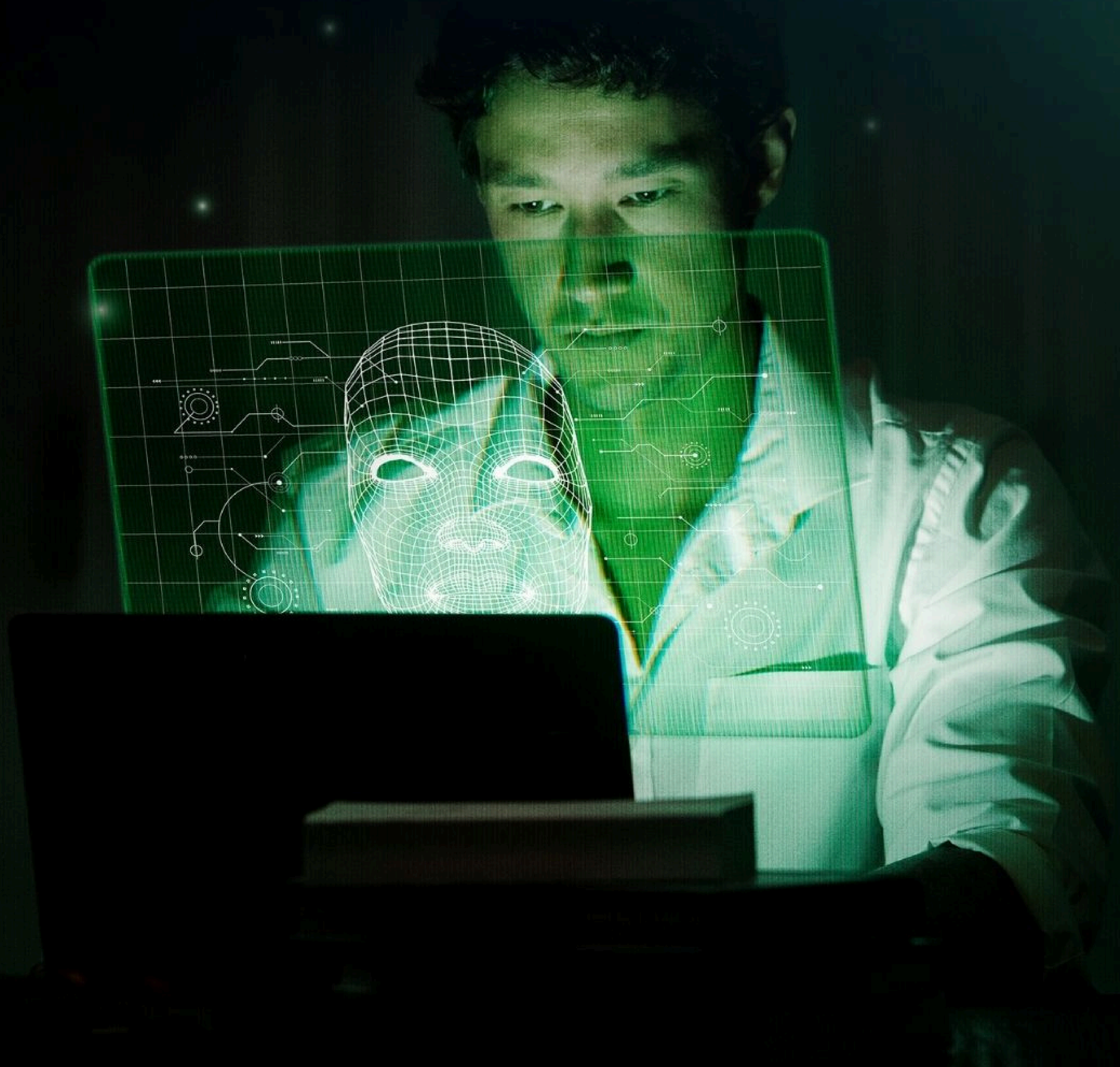
AI CERTs™

AI+ Ethical Hacker™

Certification



Introduction to AI CERTs

AI CERTs™ is at the forefront of AI and blockchain certification, offering premier programs designed to equip individuals for success in these rapidly evolving fields. Our certifications are specifically crafted to bridge the gap between theoretical knowledge and practical application, ensuring that learners are well-prepared to make an immediate impact in their careers.

AI CERTs™ was established to provide high-quality, accessible certifications that empower individuals to excel in the digital age. We are committed to developing a new generation of tech leaders who will be innovators, not just participants, in the industry.

Acknowledgements

We sincerely appreciate the contributions of all the Subject Matter Experts (SMEs), industry professionals, and teams who invested their time, expertise, and insights in developing the AI CERTs™ Certification Scheme. The collaborative efforts of individuals from diverse fields, including cybersecurity, artificial intelligence, education, and professional training, have been vital in ensuring the certification program's relevance, rigor, and alignment with industry standards.

Contributors

The successful development and validation of the certification scheme were made possible through the contributions of the following key stakeholders and teams:

- **Subject Matter Experts (SMEs):** A diverse group of AI and cybersecurity professionals contributed their expertise to ensure that the certification content is comprehensive and aligned with current industry standards.
- **Academic Partners:** We appreciate the valuable contributions from esteemed academic institutions, whose research and frameworks helped shape the theoretical foundations of the certification.
- **Industry Advisors:** We extend our gratitude to our partners from leading organizations for providing insights into the latest market trends and emerging technologies, ensuring that the certification addresses real-world challenges faced by AI professionals today.

- **Compliance and Accreditation Teams:** Their careful work in aligning the certification with ISO/IEC 17024:2012 standards has ensured that the scheme meets the highest levels of international accreditation.

- **Internal Development Teams:** Our instructional designers, content creators, and technical staff worked diligently to translate expert knowledge into a structured and accessible certification scheme for professionals worldwide.

Exam Information

- The AI+ Ethical Hacker Certification equips cybersecurity professionals and ethical hackers with the skills needed to secure the ever-evolving digital landscape. This certification offers an in-depth exploration of ethical hacking practices alongside cutting-edge Artificial Intelligence (AI) technologies, highlighting how AI is reshaping both offensive and defensive cybersecurity strategies. Learners will dive into the legal and ethical foundations of ethical hacking, master core techniques, and acquire essential skills.

- This certification includes AI-driven threat analysis, leveraging tools such as Machine Learning (ML), Natural Language Processing (NLP), and Deep Learning (DL) for enhanced cybersecurity. Through a blend of academic learning and hands-on activities, learners will apply AI-enhanced methods to real-world scenarios. This certification goes beyond teaching new technologies—it prepares learners for the future of cybersecurity. As cyber threats become increasingly complex, AI's role in proactive defense and rapid response becomes crucial. By engaging with interactive modules and case studies, you will develop a robust skill set, positioning them to tackle modern cyber threats using innovative AI solutions.

Exam Prerequisites

This certification aims to help individuals improve their skills in combining AI techniques with ethical hacking practices. To get the most out of this certification, please ensure you meet the following prerequisites:

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

Exam Specifications

Number of Questions

50

Passing Score

35/50 or 70%

Duration

90 Minutes

Exam Options

Online, Remotely Proctored

Question Type

Multiple Choice/Multiple Response

Item Format Details

- **The exam will primarily consist of multiple-choice questions with single-response options.**
- **Additional item types may be included as necessary, such as:**
  - Manipulating snippets of code (e.g., SQL)
  - Interpreting data visualizations

- The exam will be administered using Proctoring 365, AI CERTs' proprietary remote proctoring solution, ensuring a secure and reliable testing environment for all candidates.
- (**Note:** exam time includes 5 minutes for reading and signing the Candidate Agreement and 5 minutes for the testing system tutorial.)

Exam Description

TARGET CANDIDATE	
ETHICAL HACKERS	• Penetration Tester • Red Team Members
CYBERSECURITY PROFESSIONALS	• Information Security Analysts • Security Engineers
IT PERSONNEL	• System Administrators • Network Administrators
ASPIRING ETHICAL HACKING PRACTITIONERS	• Students and Recent Graduates • Career Changers
IT SECURITY CONSULTANTS	• Professionals looking to expand their knowledge of AI applications in vulnerability assessments, penetration testing, and security auditing.

Exam Objective Statement

- **Understand Ethical Hacking Principles:** Grasp the fundamental concepts of ethical hacking, including legal and ethical considerations, to navigate the cybersecurity landscape responsibly.

- **Conduct Vulnerability Assessments:** Perform thorough assessments to identify and evaluate vulnerabilities in systems, networks, and applications to enhance overall security.

- **Utilize Penetration Testing Techniques:** Apply a variety of penetration testing methodologies and tools to simulate attacks and uncover security weaknesses in real-world scenarios.

- **Leverage Exploit Development:** Gain proficiency in developing and deploying exploits to demonstrate how vulnerabilities can be exploited, reinforcing the importance of remediation.

- **Develop Security Solutions:** Create effective security solutions and countermeasures to address identified vulnerabilities, ensuring robust protection against potential threats.

- **Engage in Incident Response Planning:** Understand and participate in incident response planning and execution, focusing on detection, containment, and recovery from security breaches.

- **Work with Security Tools and Frameworks:** Familiarize yourself with various ethical hacking tools and frameworks, such as Metasploit and Nmap, to enhance testing capabilities.

- **Capstone Project Implementation:** Integrate the knowledge and skills acquired throughout the course into a capstone project, addressing practical ethical hacking challenges and proposing solutions.

To ensure that exam candidates demonstrate the necessary skills, the **AI+ Ethical Hacker** exam (Exam Code: **AIC-ETH-101**) will assess their knowledge across the following domains, along with their respective weightings:

Module	% of Examination
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%

AI CERTs™

AI+ Ethical Hacker™

Objectives

The information provided below is designed to assist you in preparing for your certification exam with AI CERTs. While this information serves as a valuable resource, it does not encompass every concept and skill that may be tested during your exam. The exam domains, previously identified and outlined in the objectives listing, represent the key content areas covered in the exam. Each objective within those domains reflects the specific tasks associated with the job role(s) being assessed. Additional information beyond the domains and objectives illustrates examples of concepts, tools, skills, and abilities relevant to the corresponding domains and objectives. This content is based on industry expert analysis related to the certification job role(s) and may not directly correlate with every aspect of the training program or exam content. We strongly encourage you to engage in independent study to familiarize yourself with any concepts highlighted here that were not explicitly addressed in your training program or materials.

Module 1

Module 1: Foundation of Ethical Hacking Using Artificial Intelligence (AI) (5%)

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 Foot printing and Reconnaissance

1.7 Scanning Networks

1.8 Enumeration Techniques

Module 2

Module 2: Introduction to AI in Ethical Hacking (9%)

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

Module 3: AI Tools and Technologies in Ethical Hacking (9%)

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

Module 4: AI-Driven Reconnaissance Techniques (9%)

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

Module 5: AI in Vulnerability Assessment and Penetration Testing (9%)

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

Module 6

Module 6: Machine Learning for Threat Analysis (9%)

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

6.7 Feature Engineering in Threat Analysis

6.8 Machine Learning in Endpoint Security

6.9 Explainable AI in Threat Analysis

Module 7

Module 7: Behavioral Analysis and Anomaly Detection for System Hacking (9%)

7.1 Behavioral Biometrics for User Authentication

7.2 Machine Learning Models for User Behavior Analysis

7.3 Network Traffic Behavioral Analysis

7.4 Endpoint Behavioral Monitoring

7.5 Time Series Analysis for Anomaly Detection

7.6 Heuristic Approaches to Anomaly Detection

7.7 AI-Driven Threat Hunting

7.7 AI-Driven Threat Hunting

7.9 Challenges and Considerations in Behavioral Analysis

Module 8

Module 8: AI Enabled Incident Response Systems (9%)

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

Module 9: AI for Identity and Access Management (IAM) (9%)

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

9.9 AI in Identity Governance and Administration (IGA)

Module 10

Module 10: Securing AI Systems (9%)

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

Module 11: Ethics in AI and Cybersecurity (9%)

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

Module 12: Capstone Project (5%)

12.1 Case Study 1: AI-Enhanced Threat Detection and Response

12.2 Case Study 2: Ethical Hacking with AI Integration

12.3 Case Study 3: AI in Identity and Access Management (IAM)

12.4 Case Study 4: Secure Deployment of AI Systems

Recertification Requirements

To maintain your certification status, AI CERTs require recertification every 1 year. Candidates will be notified 3 months before their recertification due date. Candidates need to apply for recertification following the guidelines provided in the candidate handbook.

Contact Us for Recertification Inquiries

For any questions or to initiate the recertification process, please reach out to our support team. We are here to assist you with your recertification needs. Email: support@aicerts.io

Code of Conduct

All AI CERTs-certified professionals must adhere to the AI CERTs Code of Conduct, which emphasizes integrity, confidentiality, continuous competence development, fairness, and compliance with applicable laws and regulations. Certified individuals are expected to avoid conflicts of interest, respect intellectual property rights, and uphold ethical behavior in all professional activities. Any violation of this code may result in suspension or revocation of certification. Certified professionals agree to these terms as a requirement for maintaining their certification.

Acronyms

Acronym Expanded Form

- OSINT-Open Source Intelligence
- DNS-Domain Name System
- DAST-Dynamic Application Security Testing
- UEBA-User and Entity Behavior Analytics
- IAM-Identity and Access Management
- PAM-Privileged Access Management
- IGA- Identity Governance and Administration

AI CERTs™

www.aicerts.io

Contact

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