AI CERTs™

# AI+ Security™ Level 1

Certification

# Introduction to AI CERTs

AI CERTs™ leads the way in AI and blockchain certification, delivering top-tier programs that equip individuals to excel in these fast-evolving fields. Our certifications are tailored to bridge the gap between theory and real-world practice, ensuring learners are prepared to make an immediate impact on their careers.

AI CERTs™ was founded to offer high-quality, accessible certifications that empower individuals to thrive in the digital age. We aim to develop a new generation of tech leaders who are not just participants but innovators in the industry.

# Acknowledgements

We would like to extend our sincere gratitude to all the Subject Matter Experts (SMEs), industry professionals, and teams who contributed their valuable 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 played a crucial role in ensuring the relevance, rigor, and industry alignment of this certification program.

# Contributors

- **Subject Matter Experts (SMEs):** A diverse group of AI and cybersecurity professionals contributed their domain knowledge to ensure that the certification content is comprehensive and current with current industry standards.

- **Academic Partners:** We are grateful for the contributions from esteemed academic institutions, whose research and academic frameworks helped shape the theoretical foundations of the certification.

- **Industry Advisors:** Special thanks to our partners from leading organizations who provided insights into the latest market trends and emerging technologies, ensuring that the certification addresses real-world challenges faced by AI professionals today.

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

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

# Exam Information

- AI+ Security Level 1 offers professionals an in-depth exploration of the integration of Artificial Intelligence (AI) and Cybersecurity. Starting with foundational Python programming tailored for AI and cybersecurity applications, participants will gain a solid understanding of core AI principles. They will then apply machine learning techniques to detect and mitigate various cyber threats, including email-based attacks, malware, and network anomalies.

- The course also covers advanced topics such as AI-driven user authentication algorithms and the use of Generative Adversarial Networks (GANs) for cybersecurity purposes. Throughout the program, practical application is emphasized, culminating in a Capstone Project where participants will synthesize their acquired knowledge to address real-world cybersecurity challenges. Upon completion, participants will be well-equipped to leverage AI for safeguarding digital assets and enhancing overall cybersecurity strategies.

# Exam Prerequisites

While this course is designed to be accessible to a broad range of professionals, the following knowledge and skills are recommended to maximize your learning experience:

- **Basic Cybersecurity Knowledge:** An understanding of core cybersecurity concepts such as threat detection, malware, and network security is advantageous for contextualizing the application of AI in cybersecurity.
- **Programming Skills:** Familiarity with Python programming will be beneficial, as Python is used extensively throughout the course for implementing AI models and cybersecurity solutions.
- **Foundational Knowledge of Machine Learning:** Prior exposure to basic machine learning concepts, such as supervised learning and classification, is recommended to facilitate a deeper understanding of AI-driven cybersecurity techniques.
- **Technical Background:** A background in IT, computer science, or a related field will be helpful in quickly grasping the more advanced topics covered in the course.

# 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 | |
|---|---|
| CYBERSECURITY PROFESSIONALS | • Information Security Analysts<br>• Security Engineers<br>• Incident Response Teams |
| IT PERSONNEL | • System Administrators<br>• Network Administrators<br>• DevOps Engineers |
| SECURITY ANALYSTS | • Threat Intelligence Analysts<br>• Malware Analysts<br>• Forensic Analysts |
| ASPIRING CYBERSECURITY PRACTITIONERS | • Students and Recent Graduates pursuing degrees in cybersecurity or related fields<br>• Career Changers looking to transition into cybersecurity |
| COMPLIANCE AND RISK MANAGEMENT PROFESSIONALS | • Risk Analysts assessing potential risks<br>• Compliance Officers ensuring adherence to regulations |
| DATA SCIENTISTS AND ANALYSTS | • Machine Learning Engineers developing algorithms for cybersecurity applications<br>• Data Analysts utilizing AI for anomaly detection and behavior analysis |

| | |
|---|---|
| EDUCATORS AND TRAINERS | • University Professors teaching courses on AI and cybersecurity<br>• Corporate Trainers developing and delivering training programs |
| GOVERNMENT AND LAW ENFORCEMENT OFFICIALS | • Cybersecurity Policy Makers developing security policies<br>• Law Enforcement Cyber Units investigating cybercrimes |
| CONSULTANTS AND ADVISORS | • Cybersecurity Consultants providing insights and recommendations<br>• IT Strategy Advisors aligning cybersecurity initiatives with business goals |
| GENERAL PUBLIC WITH INTEREST IN CYBERSECURITY | • Individuals seeking to understand the basics of cybersecurity and AI applications |

# Exam Objective Statement

**Understand AI and Machine Learning Fundamentals:**

- Comprehend the basic concepts of artificial intelligence (AI) and machine learning (ML) and their relevance to cybersecurity.

**Implement AI for Security Applications:**

- Apply AI techniques for intrusion detection, anomaly detection, and malware analysis to enhance security protocols.

**Utilize AI Algorithms for Threat Detection:**

- Employ AI algorithms for real-time threat detection and automated response mechanisms to minimize security risks.

**Leverage Machine Learning Models:**

- Use machine learning models for behavior analysis, phishing detection, and email security to safeguard digital environments.

**Develop Proactive Defense Strategies:**

- Create proactive cybersecurity strategies that predict and prevent attacks using AI models, ensuring a robust defense mechanism.

**Engage in Incident Response:**

- Understand and apply incident response processes, including detection, containment, and recovery, leveraging AI tools for efficiency.

**Work with Open Source Security Tools:**

- Familiarize with various open-source security tools and their applications in identifying and mitigating security threats.

**Capstone Project Synthesis:**

- Synthesize knowledge and skills acquired throughout the course in a capstone project, addressing real-world cybersecurity challenges.

To ensure that exam candidates demonstrate the necessary skills, the AI+ Security Level 1 exam (Exam Code: AIC-SEC-301) will assess their knowledge across the following domains, along with their respective weightings:

| Module | % of Examination |
|---|---|
| Introduction to Cyber 100 | 6% |
| Operating System Fundamentals | 7% |
| Networking Fundamentals | 7% |
| Threats, Vulnerabilities, and Exploits | 10% |
| Understanding of AI and ML | 10% |
| Python Programming Fundamentals | 10% |
| Applications of AI in Cybersecurity | 10% |
| Incident Response and Disaster Recovery | 10% |
| Open Source Security Tools | 10% |
| Security Securing the Future | 10% |
| Capstone Project | 10% |
| Total | 100% |

AI CERTs™

AI+ Security Level 1™

# 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: Introduction to Cyber Security (6%)

1.1 Definition and Scope of CyberSecurity

1.2 Key Cybersecurity Concepts

1.3 CIA Triad (Confidentiality, Integrity, Availability)

1.4 Challenges in Applying AI to Security

1.2 AI Use Cases in Cybersecurity

1.3 Engineering AI Pipelines for Security

1.4 Challenges in Applying AI to Security

Module 2

## Module 2: Operating System Fundamentals (7%)

2.1 Core OS Functions (Memory Management, Process Management)

2.2 User Accounts and Privileges

2.3 Access Control Mechanisms (ACLs, DAC, MAC)

2.4 OS Security Features and Configurations

2.5 Hardening OS Security (Patching, Disabling Unnecessary Services)

2.6 Virtualization and Containerization Security Considerations

2.7 Secure Boot and Secure Remote Access

2.8 OS Vulnerabilities and Mitigations

Module 3

## Module 3: Networking Fundamentals (7%)

3.1 Network Topologies and Protocols (TCP/IP, OSI Model)

3.2 Network Devices and Their Roles (Routers, Switches, Firewalls)

3.3 Network Security Devices (Firewalls, IDS/IPS)

3.4 Network Segmentation and Zoning

3.5 Wireless Network Security (WPA2, Open WEP vulnerabilities)

3.6 VPN Technologies and Use Cases

3.7 Network Address Translation (NAT)

3.8 Basic Network Troubleshooting

Module 4

## Module 4: Threats, Vulnerabilities, and Exploits (10%)

4.1 Types of Threat Actors (Script Kiddies, Hacktivists, Nation-States)

4.2 Threat Hunting Methodologies using AI

4.3 AI Tools for Threat Hunting (SIEM, IDS/IPS)

4.4 Open-Source Intelligence (OSINT) Techniques

4.5 Software Development Life Cycle (SDLC) and Security Integration with AI

4.6 Introduction to Vulnerabilities

4.7 Zero-Day Attacks and Patch Management Strategies

4.8 Vulnerability Scanning Tools and Techniques using AI

4.9 Exploiting Vulnerabilities (Hands-on Labs)

Module 5

## Module 5: Understanding of AI and ML (10%)

5.1 An Introduction to AI

5.2 Types and Applications of AI

5.3 Identifying and Mitigating Risks in Real-Life

5.4 Building a Resilient and Adaptive Security Infrastructure with AI

5.5 Enhancing Digital Defenses using CSAI

5.6 Application of Machine Learning in Cybersecurity

5.7 Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats

5.8 Threat Intelligence and Threat Hunting Concepts

Module 6

## Module 6: Python Programming Fundamentals (10%)

6.1 Introduction to Python Programming

6.2 Understanding of Python Libraries

6.3 Python Programming Language for Cybersecurity Applications

6.4 AI for Securing Mobile and IoT Devices

6.5 Data Analysis and Manipulation Using Python

6.6 Developing Security Tools with Python

Module 7

## Module 7: Applications of AI in Cybersecurity (10%)

7.1 Understanding the Application of Machine Learning in Cybersecurity

7.2 Anomaly Detection to Behavior Analysis

7.3 Dynamic and Proactive Defense using Machine Learning

7.4 Utilizing Machine Learning for Email Threat Detection

7.5 Enhancing Phishing Detection with AI

7.6 Autonomous Identification and Thwarting of Email Threats

7.7 Employing Advanced Algorithms and AI in Malware Threat Detection

7.8 Identifying, Analyzing, and Mitigating Malicious Software

7.9 Enhancing User Authentication with AI Techniques

7.10 Penetration Testing with AI

Module 8

# Module 8: Incident Response and Disaster Recovery (10%)

8.1 Incident Response Process (Identification, Containment, Eradication, Recovery)

8.2 Incident Response Lifecycle

8.3 Preparing an Incident Response Plan

8.4 Detecting and Analyzing Incidents

8.5 Containment, Eradication, and Recovery

8.6 Post-Incident Activities

8.7 Digital Forensics and Evidence Collection

8.8 Disaster Recovery Planning (Backups, Business Continuity)

8.9 Penetration Testing and Vulnerability Assessment

8.10 Legal and Regulatory Considerations of Security Incidents

Module 9

# Module 9: Open Source Security Tools (10%)

9.1 Introduction to Open-Source Security Tools

9.2 Popular Open Source Security Tools

9.3 Benefits and Challenges of Using Open-Source Tools

9.4 Implementing Open Source Solutions in Organizations

9.5 Community Support and Resources

9.6 Network Security Scanning and Vulnerability Detection

9.7 Security Information and Event Management (SIEM) Tools (Open-Source options)

9.8 Open-Source Packet Filtering Firewalls

9.9 Password Hashing and Cracking Tools (Ethical Use)

9.10 Open-Source Forensics Tool

Module 10

# Module 10: Securing the Future (10%)

10.1 Emerging Cyber Threats and Trends

10.2 Artificial Intelligence and Machine Learning in Cybersecurity

10.3 Blockchain for Security

10.4 Internet of Things (IoT) Security

10.5 Cloud Security

10.6 Quantum Computing and its Impact on Security

10.7 Cybersecurity in Critical Infrastructure

10.8 Cryptography and Secure Hashing

10.9 Cyber Security Awareness and Training for Users

10.10 Continuous Security Monitoring and Improvement

Module 11

# Module 11: Capstone Project (10%)

11.1 Introduction

11.2 Use Cases: AI in Cybersecurity

11.3 Outcome Presentation

# 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

- CIA- Confidentiality, Integrity, Availability
- NIST- National Institute of Standards and Technology
- GDPR- General Data Protection Regulation
- HIPAA Health Insurance Portability and Accountability Act
- ACLs-Access Control List
- DAC Discretionary Access Control
- MAC - Message Authentication Code
- TCP/IP- Transmission Control Protocol/Internet Protocol.30 Jul 2019
- OSI Model Open Systems Interconnection Model)
- IDS/IPS Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- WPA2 Wi-Fi Protected Access 2
- WEP Wired Equivalent Privacy

- SIEM, Security Information and Event Management
- OSINT- Open Source Intelligence
- SDLC-Software Development Life Cycle
- CSAI- Computer Science and Artificial Intelligence
- SIEM Security Information and Event Management
- IOT- Internet of Things

AI CERTs™

www.aicerts.io

**Contact**

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