AI CERTs™

AI+ Security™ Level 2

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 in their careers.

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

Acknowledgements

We sincerely thank all the Subject Matter Experts (SMEs), industry professionals, and teams who generously contributed their time, expertise, and insights to the development of the AI CERTs™ Certification Scheme. The collaboration of individuals from various fields—cybersecurity, artificial intelligence, education, and professional training—has been instrumental in ensuring the program's relevance, rigor, and alignment with industry standards

Contributors

Among those who have contributed to the AI+ Security Level 2 certification program are:

- **Subject Matter Experts (SMEs):** SMEs related to broad collection of experts in cybersecurity and artificial intelligence who contributed their in-depth knowledge to keep the certification material up to date, thorough, and compliant with industry standards.

- **Academic Practitioners:** Contributions from eminent academic institutions, whose theoretical frameworks and research helped form the basis of the certification program.

- **Industry Advisors**: partners from prestigious companies that have contributed significant knowledge about market trends and developing technologies. They make sure the certification considers the difficulties that AI and cybersecurity experts currently face in the real world.

- **Internal Development Teams:** Committed instructional designers, content producers, and technical personnel worked to transform domain expertise into a globally recognized certification that is organized, readable, and accessible.

AI CERTs AI+ Security Level 2 AIC-SEC-101

Exam Information

Our comprehensive course, AI+ Cybersecurity, offers professionals a thorough exploration of the integration of AI and Cybersecurity. Beginning with fundamental Python programming tailored for AI and Cybersecurity applications, participants delve into essential AI principles before applying machine learning techniques to detect and mitigate cyber threats, including email threats, malware, and network anomalies.

Advanced topics such as user authentication using AI algorithms and the application of Generative Adversarial Networks (GANs) for Cybersecurity purposes are also covered, ensuring participants are equipped with cutting-edge knowledge. Practical application is emphasized throughout, culminating in a Capstone Project where attendees synthesize their skills to address real-world cybersecurity challenges, leaving them adept in leveraging AI to safeguard digital assets effectively.

Exam Prerequisites

- **An Enthusiast:** Interest in learning about machine learning, deep learning, and natural language processing.
- **Fundamentals of Computing**: Basic knowledge computer science, no technical knowledge required
- Curiosity and openness to learning about new concepts and technologies
- **Legal Practitioners**: Willingness to explore ethical considerations and legal frameworks surrounding the use of AI and data privacy

Exam Specifications

Number of Questions: 50.

Passing Score: 70%

Duration: 90 Minutes

(**Note:** exam time includes 5 minutes for reading and signing the CandidateAgreement and 5 minutes for the proctoring tutorial).

Exam Options: Online, Remotely Proctored

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
    - 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.

Exam Description

Target Candidate:

The ideal candidates for this certification are:

- Cybersecurity Professionals
    - Information Security Professionals
    - Security Engineers
    - Incident Response Specialists

- AI and Machine Learning Enthusiasts
    - Understands AI Fundamentals
    - Proficient in Python
    - Application to Cybersecurity and Compliance
- Security Professionals
    - Threat Intelligence Specialists
    - Malware Specialists
    - Forensic Investigator
- Aspiring Cybersecurity Practitioners
    - Students and Recent Graduates pursuing degrees in cybersecurity or related fields
    - Career Changers looking to transition into cybersecurity.
- Educators and Instructors
    - University Professors teaching AI and cybersecurity courses
    - Corporate Trainers creating and delivering training programs

Exam Objective Statement:

- **Python Basics**: Gain a solid foundation in Python by learning its syntax, data structures, and functions, enabling effective coding practices for various applications in AI and cybersecurity.

- **Libraries for AI & Cybersecurity:** Acquire knowledge of essential Python libraries like NumPy, Pandas, Scikit-learn, and TensorFlow, which are critical for implementing machine learning models and enhancing cybersecurity measures.

- **Scripting for Security Tasks:** Develop skills in writing Python scripts to perform essential security tasks, including log analysis, automating security monitoring, and preprocessing data for better insights.

- **Key AI Concepts:** Understand the fundamental principles of AI, including supervised, unsupervised, and reinforcement learning, which are crucial for designing effective AI-driven solutions.

- **AI Algorithms**: Familiarize yourself with popular machine learning algorithms such as Decision Trees, Support Vector Machines (SVMs), Neural Networks, and K-Means clustering to apply these techniques in real-world scenarios.

- **AI Model Evaluation**: Learn about critical evaluation metrics like accuracy, precision, recall, F1 score, and confusion matrix, which help assess the performance of AI models and ensure their reliability in practical applications.

To ensure that exam candidates demonstrate the necessary skills, the **AI+ Security Level 2 Exam (Exam Code: AIC-SEC-201)** will assess their knowledge across the following domains, along with their respective weightings:

Modules	% of Examination
Introduction to Artificial Intelligence (AI) and Cyber Security	**8%**
Python Programming for AI and Cyber Security Professionals	**10%**

Application of Machine Learning in Cyber Security	**10%**
Detection of Email Threats with Artificial Intelligence (AI)	**11%**
Artificial Intelligence (AI) Algorithm for Malware Threat Detection	**11%**
Network Anomaly Detection using Artificial Intelligence (AI) Techniques	**11%**
User Authentication Security with Artificial Intelligence (AI)	**11%**
Generative Adversarial Network (GAN) for Cyber Security	**11%**
Penetration Testing with Artificial Intelligence	**11%**
Capstone Project	**6%**
Total	**100%**

Objectives

The following information is intended to help you get ready for your AI CERTs certification exam. Although this information is useful, it does not cover all the concepts and skills that could be assessed on your exam. The exam domains, as previously listed in the objectives, are the main subject areas included in the exam. Every goal in those categories represents the duties linked to the job role(s) under evaluation. More details outside

of the domains and objectives demonstrate examples of concepts, tools, skills, and abilities that are important for the related domains and objectives. This information relies on expert analysis from the industry concerning certification job role(s) and might not align perfectly with all aspects of the training program or exam content. We highly recommend that you undertake self-study to become familiar with any concepts mentioned here that were not specifically covered in your training program or materials

Module 1: Introduction to Artificial Intelligence (AI) and Cyber Security (8%)

1.1 Understanding the Cyber Security Artificial Intelligence (CSAI)

1.2 An Introduction to AI and its Applications in Cybersecurity

1.3 Overview of Cybersecurity Fundamentals

1.4 Identifying and Mitigating Risks in Real-Life

1.5 Building a Resilient and Adaptive Security Infrastructure

1.6 Enhancing Digital Defenses using CSAI

Module 2: Python Programming for AI and Cybersecurity Professionals (10%)

2.1 Python Programming Language and its Relevance in Cybersecurity

2.2 Python Programming Language and Cybersecurity Applications

2.3 AI Scripting for Automation in Cybersecurity Tasks

2.4 Data Analysis and Manipulation Using Python

2.5 Developing Security Tools with Python

Module 3: Application of Machine Learning in Cybersecurity (10%)

3.1 Understanding the Application of Machine Learning in Cybersecurity

3.2 Anomaly Detection to Behavior Analysis

3.3 Dynamic and Proactive Defense using Machine Learning

3.4 Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats

Module 4: Detection of Email Threats with AI (11%)

4.1 Utilizing Machine Learning for Email Threat Detection

4.2 Analyzing Patterns and Flagging Malicious Content

4.3 Enhancing Phishing Detection with AI

4.4 Autonomous Identification and Thwarting of Email Threats

4.5 Tools and Technology for Implementing AI in Email Security

Module 5: AI Algorithm for Malware Threat Detection (11%)

5.1 Introduction to AI Algorithm for Malware Threat Detection

5.2 Employing Advanced Algorithms and AI in Malware Threat Detection

5.3 Identifying, Analyzing, and Mitigating Malicious Software

5.4 Safeguarding Systems, Networks, and Data in Real-time

5.5 Bolstering Cybersecurity Measures Against Malware Threats

5.6 Tools and Technology: Python, Malware Analysis Tools

Module 6: Network Anomaly Detection using AI (11%)

6.1 Utilizing Machine Learning to Identify Unusual Patterns in Network Traffic

6.2 Enhancing Cybersecurity and Fortifying Network Defenses with AI Techniques

6.3 Implementing Network Anomaly Detection Techniques

Module 7: User Authentication Security with AI (11%)

7.1 Introduction

7.2 Enhancing User Authentication with AI Techniques

7.3 Introducing Biometric Recognition, Anomaly Detection, and Behavioral Analysis

7.4 Providing a Robust Defense Against Unauthorized Access

7.5 Ensuring a Seamless Yet Secure User Experience

7.6 Tools and Technology: AI-based Authentication

7.7 Conclusion

Module 8: Generative Adversarial Network (GAN) for Cyber Security (11%)

8.1 Introduction to Generative Adversarial Networks (GANs) in Cybersecurity

8.2 Creating Realistic Mock Threats to Fortify Systems

8.3 Detecting Vulnerabilities and Refining Security Measures Using GANs

8.4 Tools and Technology: Python and GAN Frameworks

Module 9: Penetration Testing with Artificial Intelligence (11%)

9.1 Enhancing Efficiency in Identifying Vulnerabilities Using AI

9.2 Automating Threat Detection and Adapting to Evolving Attack Patterns

9.3 Strengthening Organizations Against Cyber Threats Using AI-driven Penetration Testing

9.4 Tools and Technology: Penetration Testing Tools, AI based Vulnerability Scanners

Module 10: Capstone Project (6%)

10.1 Introduction

10.2 Use Cases: AI in Cybersecurity

10.3 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

GANs-Generative Adversarial Networks

AI - Artificial Intelligence

GANs - Generative Adversarial Networks

SMEs - Subject Matter Experts

CSAI - Cyber Security Artificial Intelligence

SVMs - Support Vector Machines

AIC - AI CERTs (e.g., AIC-SEC-101, AI CERTs Security certification code)

BDMs - Business Development Managers

SDRs - Sales Development Representatives

ATP - Authorized Training Providers

AI CERTs™

www.aicerts.io

Contact

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