AICERTs™

AI+ Security™ Level 3

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 want to thank all the Subject Matter Experts (SMEs), industry professionals, and teams who generously dedicated their time, knowledge, and perspectives to help in creating the AI CERTs™ Certification Scheme. The certification program's significance, thoroughness, and alignment with industry standards have been guaranteed by the teamwork of people from various backgrounds like cybersecurity, artificial intelligence, education, and professional training.

Contributors

- **Subject Matter Experts (SMEs):** Professionals with extensive knowledge in AI, machine learning, and cybersecurity who can provide insights on advanced topics and applications.
- **Academics and Researchers:** University professors and researchers specializing in AI, cybersecurity, and related fields who can contribute theoretical frameworks and cutting-edge research findings.
- **Industry Practitioners**: Security engineers, threat intelligence analysts, and incident responders who have hands-on experience and can share practical insights into real-world security challenges.
- **Corporate Trainers**: Trainers from organizations that specialize in AI and cybersecurity, capable of developing course materials that are engaging and effective for learners.

- **Compliance and Regulatory Experts**: Professionals knowledgeable about security standards and regulations who can ensure that course content aligns with industry compliance requirements.

- **Technical Writers:** Skilled writers who can articulate complex concepts clearly and concisely, creating accessible and engaging learning materials.

- **Data Scientists and AI Engineers**: Experts with experience in applying AI and machine learning in security contexts, contributing to the technical aspects of the certification.

- **Cybersecurity Analysts:** Professionals who understand the current threat landscape and can provide real-world examples and case studies relevant to the certification.

AI CERTs AI+ Security Level 3 AIC-SEC-301

Exam Information

The AI+ Security Level 3 course provides a comprehensive exploration of the intersection between AI and cybersecurity, focusing on advanced topics critical to modern security engineering. It covers foundational concepts in AI and machine learning for security, delving into areas like threat detection, response mechanisms, and the use of deep learning for security applications.

The course addresses the challenges of adversarial AI, network and endpoint security, and secure AI system engineering, along with emerging topics such as AI for cloud, container security, and blockchain integration. Key subjects also include AI in identity and access management (IAM), IoT security, and physical security systems, culminating in a hands-on capstone project that tasks learners with designing and engineering AI-driven security solutions.

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:

- **Foundational Cybersecurity Knowledge**: Basic knowledge of cybersecurity principles and familiarity with common security threats and defense mechanisms.
- **Machine Learning Fundamentals:** Understanding of machine learning concepts, including supervised and unsupervised learning, model training, and evaluation techniques.
- **Programming Proficiency:** Proficiency in programming languages such as Python, with experience in AI/ML libraries like TensorFlow or PyTorch.
- **Cloud and Networking Technologies:** Familiarity with cloud and networking technologies as well as containerization tools like Docker and Kubernetes.

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 testing system tutorial.)

Exam Options: Online, Remotely Proctored

Item Formats: 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.

Exam Description

Target Candidate:

The ideal candidates for this certification are:

- Experts in Cybersecurity
    - Engineers specializing in security
- Information Technology Experts
    - IT professionals who manage and maintain computer systems
    - IT professionals who manage networks
    - Engineers specializing in DevOps
- Analysts specializing in security
    - Security experts specializing in analyzing threats and gathering intelligence.
    - Analysts who specialize in studying malware
    - Investigators who specialize in analyzing evidence and information related to crimes
- Future professionals in the field of cybersecurity
    - Students and Recent Graduates who are studying for degrees in cybersecurity or a related field
    - Individuals seeking to switch careers and move into the field of cybersecurity

- Professionals in Compliance and Risk Management
    - Risk analysts are evaluating possible risks.
    - Compliance Officers are responsible for making sure that regulations are being followed.
- Professionals in the field of data analysis and science
    - Machine Learning Engineers are creating algorithms for cybersecurity purposes.
    - Data Analysts are using AI to spot irregularities and analyze behavior.
- Leaders in the business world and corporate executives
    - Top information security officers (CISOs)
    - IT managers are making strategic security-related decisions.
- Teachers and instructors
    - University instructors are offering classes on artificial intelligence and cybersecurity.
    - Corporate Trainers are creating and providing training programs.
- Officials from the government and law enforcement
    - Cybersecurity policymakers are creating security policies.
    - Law enforcement cyber units are looking into cybercrimes.

Exam Objective Statement

The AI + Security Level 3 certification is designed to equip professionals with the knowledge and skills to integrate artificial intelligence (AI) with cybersecurity compliance frameworks. The exam objectives include:

- **AI Threats & Vulnerabilities**: Types of attacks: Adversarial attacks on AI models (e.g., data poisoning, evasion attacks).
- **AI in Cybersecurity AI-driven security solutions**: Machine learning (ML) and deep learning models used for threat detection (e.g., malware analysis, intrusion detection).
- **Security Automation**: Leveraging AI for automated incident response, vulnerability management, and monitoring.
- **Anomaly Detection:** Techniques for identifying unusual behavior using AI and ML models.
- **Ethics and Governance in AI Security**
- **Ethical AI Development**: Ensuring AI is used responsibly, avoiding harm, privacy breaches, and discrimination.

To ensure that exam candidates demonstrate the necessary skills, the **AI+ Security Level 3** exam (Exam Code: **AIC-SEC-301**) will assess their knowledge across the following domains, along with their respective weightings:

Modules	% of Examination
Foundations of AI and Machine Learning for Security Engineering	**6%**
Machine Learning for Threat Detection and Response	**7%**
Deep Learning for Security Applications	**7%**
Adversarial AI in Security	**10%**
AI in Network Security	**10%**
AI in Endpoint Security	**10%**
Secure AI System Engineering	**10%**
AI for Cloud and Container Security	**10%**
AI and Blockchain for Security	**10%**

AI in Identity and Access Management (IAM)	**10%**
AI for Physical and IoT Security	**10%**
Capstone Project - Engineering AI Security Systems	**10%**
Total	**100%**

Objectives

Module 1: Foundations of AI and Machine (6%)

1.1 Core AI and ML Concepts for 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: Machine Learning for Threat Detection and Response (7%)

2.1 Engineering Feature Extraction for Cybersecurity Datasets

2.2 Supervised Learning for Threat Classification

2.3 Unsupervised Learning for Anomaly Detection

2.4 Engineering Real-Time Threat Detection Systems

Module 3: Deep Learning for Security Applications (7%)

3.1 Convolutional Neural Networks (CNNs) for Threat Detection

3.2 Recurrent Neural Networks (RNNs) and LSTMs for Security

3.3 Autoencoders for Anomaly Detection

3.4 Adversarial Deep Learning in Security

Module 4: Adversarial AI in Security (10%)

4.1 Introduction to Adversarial AI Attacks

4.2 Defense Mechanisms Against Adversarial Attacks

4.3 Adversarial Testing and Red Teaming for AI Systems

4.4 Engineering Robust AI Systems Against Adversarial AI

Module 5: AI in Network Security (10%)

5.1 AI-Powered Intrusion Detection Systems

5.2 AI for Distributed Denial of Service (DDoS) Detection

5.3 AI-Based Network Anomaly Detection

5.4 Engineering Secure Network Architectures with AI

Module 6: AI in Endpoint Security (10%)

6.1 AI for Malware Detection and Classification

6.2 AI for Endpoint Detection and Response (EDR)

6.3 AI-Driven Threat Hunting

6.4 AI for Securing Mobile and IoT Devices

Module 7: Secure AI System Engineering (10%)

7.1 Designing Secure AI Architectures

7.2 Cryptography in AI for Security

7.3 Ensuring Model Explainability and Transparency in Security

7.4 Performance Optimization of AI Security Systems

Module 8: AI for Cloud and Container Security (10%)

8.1 AI for Securing Cloud Environments

8.2 AI-Driven Container Security

8.3 AI for Securing Serverless Architectures

8.4 AI and DevSecOps

Module 9: AI and Blockchain for Security (10%)

9.1 Fundamentals of Blockchain and AI Integration

9.2 AI for Fraud Detection in Blockchain

9.3 Smart Contracts and AI Security

9.4 AI-Enhanced Consensus Algorithms

Module 10: AI in Identity and Access Management (IAM) (10%)

10.1 AI for User Behavior Analytics in IAM

10.2 AI for Multi-Factor Authentication (MFA)

10.3 AI for Zero-Trust Architecture

10.4 AI for Role-Based Access Control (RBAC)

Module 11: AI for Physical and IoT Security (10%)

11.1 AI for Securing Smart Cities

11.2 AI for Industrial IoT Security

11.3 AI for Autonomous Vehicle Security

11.4 AI for Securing Smart Homes and Consumer IoT

Module 12: Capstone Project - Engineering AI Security Systems (10%)

12.1 Defining the Capstone Project Problem

12.2 Engineering the AI Solution

12.3 Deploying and Monitoring the AI System

12.4 Final Capstone Presentation and Evaluation

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

DDoS-Distributed Denial of Service

EDR-Endpoint Detection and Response

MFA-Multi-Factor Authentication

IoT-Internet of Things

RBAC-Role-Based Access Control

AI CERTs™

www.aicerts.io

Contact

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