

**AI CERTs™**

# AI+ Security™ Level 2

Certification



## Introduction to AI CERTs

AI CERTs™ is at the forefront of AI and blockchain certification, delivering top-tier programs that equip individuals to excel in these fast-evolving fields. Our certifications ensure candidates 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, 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:

- The successful creation and validation of the certification scheme involved several key stakeholders and teams:
  - **Subject Matter Experts (SMEs):** A diverse group of AI and cybersecurity professionals provided their expertise to ensure the certification content is comprehensive and in line with current industry standards
  - **Academic Partners:** We appreciate the contributions from distinguished academic institutions, whose research and frameworks have shaped the theoretical underpinnings of the certification.
  - **Industry Advisors:** We extend our special thanks to our partners from leading organizations for sharing insights on the latest market trends and emerging technologies, ensuring the certification effectively addresses the real-world challenges faced by today’s AI professionals.

- **Internal Development Teams:** Our content creators, and technical staff worked diligently to convert expert knowledge into a structured and accessible certification scheme for professionals worldwide.
- **Compliance and Accreditation Teams:** Their careful work in aligning the certification with ISO/IEC 17024:2012 standards have ensured that the scheme meets the highest levels of international accreditation.

# AI CERTs AI+ Security Level 2 (AIC-SEC-201)

---

## Exam Information

Our certification, AI+ Cybersecurity, offers professionals a thorough exploration of the integration of AI and Cybersecurity.

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. The certification also includes capstone-based assessment items designed to evaluate a candidate's ability to apply concepts in integrated cybersecurity scenarios. These capstone items are delivered as scenario-based multiple-choice questions within the examination and do not require submission of a separate project or practical implementation.

## Exam Specifications

**Number of Questions:** 50.

**Passing Score:** 70%

**Duration:** 90 Minutes

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

**Item Formats:** Multiple Choice

**Exam Options:** Online, Remotely Proctored

**Item Format Details:**

- The exam will primarily consist of multiple-choice questions with single-response options.

The exam will be administered using **Proctor 365**, AI CERTs' proprietary remote proctoring solution, ensuring a secure and reliable testing environment for all candidates.

## Exam Description

**Target Candidate:** This certification is designed for intermediate-level professionals with foundational knowledge in cybersecurity and an interest in applying AI techniques to security challenges. This may include:

- Cybersecurity professionals with basic experience
- IT professionals with security exposure
- Individuals with foundational knowledge of Python and AI concepts
- Students or professionals transitioning into AI-driven cybersecurity roles

**Note:** This certification validates intermediate-level knowledge and application skills. It is not intended to assess advanced or expert-level cybersecurity competencies.

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%

<b>Detection of Email Threats with Artificial Intelligence (AI)</b>	<b>11%</b>
<b>Artificial Intelligence (AI) Algorithm for Malware Threat Detection</b>	<b>11%</b>
<b>Network Anomaly Detection using Artificial Intelligence (AI) Techniques</b>	<b>11%</b>
<b>User Authentication Security with Artificial Intelligence (AI)</b>	<b>11%</b>
<b>Generative Adversarial Network (GAN) for Cyber Security</b>	<b>11%</b>
<b>Penetration Testing with Artificial Intelligence</b>	<b>11%</b>
<b>Capstone Project</b>	<b>6%</b>
<b>Total</b>	<b>100%</b>

## 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).

## **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

### **Certification Scheme Development:**

- Certification activities are independent of training. Training providers, including ATPs, do not participate in certification decisions, exam development, or exam review.

### **Certification Information Accuracy and Approval Control**

All certification-related information published by AI CERTs, including website content, candidate handbooks etc, is subject to formal review and approval by the Certification Body prior to publication. The Certification Body ensures that all information is accurate, consistent, and not misleading. No content may be published or modified without formal approval. Records of review and approval are maintained for audit purposes.

### **Initial Certification and Recertification Criteria**

#### **1.1 Eligibility and Prerequisites**

**Mandatory Prerequisites:** There are no mandatory prerequisites for this certification. Any candidate may apply for and attempt the AI+ Security Level 2 certification examination.

**Recommended Prior Knowledge (Non-Mandatory):**

While not required, candidates may benefit from:

- Basic understanding of computer systems and operating systems
- Familiarity with networking and operating systems
- Introductory knowledge of Python programming
- Basic understanding of AI/ML concepts

Note: Recommended knowledge is provided only for guidance and does not affect eligibility.

**Required Documentation**

1. Completed application form
  2. Agreement to the Certification Body’s policies, including the Code of Conduct, Confidentiality Policy, and Impartiality Declaration.
- Pay all applicable fees associated with the certification process.

**1.1.1 Public Availability of Certification Requirements**

- All certification requirements, including eligibility, examination structure, certification decision process, validity, recertification, and disciplinary policies, are publicly available without request through the official AI CERTs website (<https://www.ai-certs.org>).

1.2 Assessment Requirements

To obtain certification, the applicant shall:

- Complete the required examination(s) or assessment(s) aligned with the competence requirements of the scheme.
- Demonstrate the required level of competence according to the passing score and evaluation methods established by the Certification Body.

**1.3 Issuance of Certificate**

- Upon meeting all requirements, the Certification Body will issue an electronic certificate to the applicant.

- The certificate will clearly display the certificant's name, certification scheme, certificate ID, date of issuance, and expiration date.
- Validity Period: All certificates are valid for **1 year from the date of issuance**.
- Certificants must maintain compliance with the Code of Conduct and certification requirements throughout the validity period.
- The Certification Body reserves the right to suspend or withdraw the certificate in cases of misconduct, non-compliance, or falsification of information.

## Recertification Requirements

AI CERTs certifications are valid for one (1) year from the date of issuance. Candidates are responsible for monitoring their certification expiration date and completing all recertification requirements **prior to** the expiration date.

### 1. Recertification Criteria / Eligibility

To qualify for recertification, candidates must meet the following criteria:

- The only method for recertification is through **re-examination**. This involves a secure, proctored, multiple-choice assessment that must be completed before the certificate expires.
- **Certification Status:** Candidates with a valid certificate, or certificates nearing expiry.
- Ensure compliance with all Certification Body policies, including the most recent versions of the Code of Conduct.
- Pay the applicable recertification fees through the AI CERTs portal.

### 2. Recertification Process

Recertification must be completed before the certification expiration date. Candidates can initiate the recertification process as follows:

- **Step 1:** Pay the recertification fee via the AI CERTs portal.
- **Step 2:** Submit recertification request through candidate dashboard after payment.
- **Step 3:** Complete and pass the required assessment for recertification as defined by the certification scheme.
- **Step 4:** Upon passing the exam, the certification will be renewed and valid for another year.

### 3. Grace Period

- If candidates are unable to complete recertification before the expiration date, they may request a **grace period**.

- The grace period can be requested up to **1 day before** the recertification eligibility window closes.
- To request a grace period, candidates must contact the **Certification Body** at [support@aicerts.ai](mailto:support@aicerts.ai) within the eligibility window (before the certification expiration date).
- If a grace period is granted, candidates will have 30 to 90 additional days to complete the recertification process.
- **Note:** If recertification is not completed within the grace period, the certification status will change to **Suspended – Non-Recertified**, and candidates may need to reapply as new applicants.

#### 4. Issuance of Renewed Certificate

- Upon successful completion of the recertification requirements, a new certificate will be issued. The **issuance date** and **expiration date** will reflect the recertification completion date.

#### 5. Failure to Recertify

- If recertification is not completed before the certification expiration date and no grace period is requested, the certification status will be **Suspended – Non-Recertified**.
- Individuals whose certificates have expired without a grace period **cannot** recertify and must undergo the **full certification process** again to regain certification.

#### Contact Us for Recertification Inquiries

For any questions or to initiate the recertification process, please contact the **AI CERTs support team** at [support@aicerts.ai](mailto:support@aicerts.ai)

### Suspension and Withdrawal

#### Suspension or withdrawal may occur due to:

- Violation of the Code of Conduct
- Misuse or misrepresentation of certification
- Failure to comply with examination or recertification rules
- Non-payment of required fees
- Falsification of information
- Failure to recertify within the defined timelines

## **1.1 Certification Suspension**

When certification is suspended, the certified person or organization must cease all use of the certification. This includes removing references to the certification on websites, and in any other public materials. Suspension is a temporary measure that allows time for the certified person to resolve outstanding issues, but certification rights are revoked during this period.

## **1.2 Certification Withdrawal**

Certification withdrawal occurs when issues remain unresolved or there is a significant breach of certification requirements. Once withdrawn, the certified person must immediately remove all references to the certification and return or destroy any certification documents or certificates issued by the certification body. Failure to comply with withdrawal requirements may result in legal action and public notification of the withdrawal.

### **Non-Resolution of Issues Leading to Withdrawal or Scope Reduction**

#### **2.1 Transition from Suspension to Withdrawal**

If issues remain unresolved during the suspension period, the certification body may proceed with the withdrawal of the certification or the reduction of the certification scope. This decision will be communicated in writing, and the certified person will be given a final opportunity to address the outstanding issues before the withdrawal or scope reduction is enforced.

#### **2.2 Scope Reduction**

If certain areas of certification are no longer valid due to unresolved issues, a scope reduction may be applied. This means the certified person will retain certification in some areas, but the reduced scope will be reflected in public records and on the issued certificate.

### **Monitoring and Compliance**

#### **3.1 Monitoring During Suspension or Withdrawal**

The certification body will actively monitor certified persons during suspension or withdrawal periods to ensure compliance with the requirements to cease certification promotion. Regular checks will be conducted on websites, and any other public-facing documents to verify compliance.

### **3.2 Consequences for Non-Compliance**

Non-compliance with the requirements of suspension or withdrawal may result in further legal action, public notifications of non-compliance, and permanent disqualification from future certification. Any violations will be documented and may be reported to legal authorities if necessary.

## **Reinstatement and Appeals**

### **4.1 Reinstatement of Certification**

Certified persons who resolve their issues during the suspension period may apply for reinstatement of their certification. The certification body will review the resolution of issues, and if all requirements are met, the suspension will be lifted, and certification rights will be reinstated.

### **4.2 Appeals Process for Withdrawal or Scope Reduction**

Certified persons have the right to appeal certification withdrawal or scope reduction decisions. Appeals must be submitted in writing, outlining the reasons for contesting the decision. The certification body will review the appeal and provide a decision within a specified time frame.

## **Legal and Public Notifications**

### **5.1 Public Notification of Certification Withdrawal**

AI CERTs will maintain and make publicly available an up-to-date registry of certified persons, including those whose certification is suspended, withdrawn, or reduced in scope. This information will be published on the AI CERTs website and also provided upon request. More Information regarding suspended, withdrawn, or scope-reduced certifications shall be made available to the upon request over the email.

### **5.2 Legal Action for Non-Compliance**

If a certified person continues to use or promote their certification after withdrawal or during suspension, legal action may be taken. The certification body will consult with legal authorities to determine the appropriate actions to address non-compliance.

## NO SCOPE / LEVEL CHANGE CRITERIA

The AI+ Security Level 2 (AIC-SEC-201) certification is a single-level credential.

There are currently no upper or lower certification levels associated with this scheme; therefore, no level upgrade or downgrade applies.

If additional levels or specializations are introduced in the future (e.g., AI Security Level 3), candidates must apply to those schemes independently and meet their respective certification criteria.

## Statement on Certification Scope and Claims

This certification validates intermediate-level knowledge and application of AI in cybersecurity. It does not imply advanced or expert-level competency unless explicitly stated.

## Duties and Rights of Certified Persons

### Duties

Certified individuals must:

- Uphold ethical conduct as outlined in the Code of Conduct
- Maintain confidentiality of examination content
- Use certification marks accurately and appropriately
- Notify the Certification Body of any changes in personal information
- Refrain from using the certification after expiry, suspension, or withdrawal
- Maintain ongoing competence in the certification domains
- Complete recertification within the required cycle

### Rights

Certified individuals have the right to:

---

- Fair, impartial, and confidential treatment
- Access certification requirements and policies
- Appeal adverse certification decisions
- Submit complaints regarding certification processes
- Receive updated certification and recertification requirements

## Code of Conduct

Code of conduct for review available on the AI CERTs official website at: <https://www.ai-certs.org/code-of-conduct-for-candidates-certificants/>

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.

### Scope:

This Code of Conduct applies to all:

- Candidates seeking certification
- Certified individuals (certificants)
- Individuals renewing certification
- Any person representing themselves as part of AI CERTs certification programs

### 1. Professional Conduct:

Candidates and certificants shall:

- Act with honesty, integrity, and professionalism at all times.
- Demonstrate respect toward peers, exam staff, and AI CERTs personnel.
- Avoid any behavior that may harm the reputation of AI CERTs or its certification programs.

### 2. Compliance with Laws and Regulations:

Candidates and certificants shall:

- Adhere to all applicable local, national, and international laws.

- Comply with all AI CERTs policies, certification rules, and examination requirements.

### **3. Examination Ethics:**

Candidates shall not:

- Engage in cheating, copying, impersonation, or any form of misconduct.
- Share, reproduce, or solicit confidential exam content.
- Use unauthorized materials, devices, or assistance during examinations.
- Disrupt the examination environment.

Violations will result in disciplinary action, including cancellation of exam results or prohibition from future exams.

### **4. Confidentiality:**

Certificants and candidates shall:

- Maintain confidentiality of all exam materials, scenarios, test items, and secure content.
- Not disclose proprietary AI CERTs certification information to unauthorized individuals.

### **5. Conflict of Interest:**

Candidates and certificants must:

- Disclose any conflict of interest that may influence their participation, endorsement, or representation of AI CERTs certifications.
- Avoid situations that could compromise impartiality.

### **6. Ethical Use of Certification:**

Certificants shall:

- Present their certification status accurately, without false claims.
- Not misuse, misrepresent, or exaggerate their certification.
- Discontinue use of AI CERTs credentials if certification expires, is suspended, or revoked.

### **7. Misconduct and Disciplinary Actions:** Examples of misconduct include:

- Fraud, forgery, falsification of documents

- Cheating or attempting to gain unfair advantage
- Unethical professional practice
- Violating AI CERTs policies or exam rules

**AI CERTs may impose disciplinary actions such as:**

- • Written warning
- • Exam disqualification
- • Revocation or suspension of certification
- • Permanent ban from future certification activities

**8. Reporting Violations:**

- Candidates and certificants are required to:
- Report any observed misconduct or violations of this Code of Conduct.
- Cooperate fully in investigations conducted by AI CERTs.

Reports may be submitted confidentially to: [compliance@aicerts.ai](mailto:compliance@aicerts.ai)

**9. Agreement:**

By applying for, participating in, or maintaining certification, candidates and certificants acknowledge that:

- • They have read, understand, and agree to comply with the AI CERTs Code of Conduct.
- • Violations may result in disciplinary action.

**Enforcement & Consequences**

Failure to comply with this Code of Conduct, including obligations applicable during certification suspension or withdrawal, is enforceable under the Certification Suspension, Withdrawal, and Scope Reduction Policy.

Candidates and certificants are hereby notified that non-compliance may result in one or more enforcement actions, including but not limited to: continued suspension, formal withdrawal of certification, revocation of credentials, removal from public certification records, and prohibition from representing oneself as AI CERTs certified.

Enforcement actions are determined and applied in accordance with the Certification Suspension, Withdrawal, and Scope Reduction Policy. Compliance with this Code of Conduct is a mandatory condition for obtaining, maintaining, or renewing AI CERTs 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

<b>Version History</b>
------------------------

Version	Date	Description of Changes	Policy Title/Section Updated	Notes
V1.0	8 <sup>th</sup> Jan 2024	Initial Copy	AI+ Security Level 2 Certification Scheme	NA
V2.0	28 <sup>th</sup> Nov 2025	Updated Certificate Scheme Development, Initial Certification and Recertification Criteria and Code of Conduct	AI+ Security Level 2 Certification Scheme	NA
V3.0	18 <sup>th</sup> March 2026	Updated certification content, target candidate profile, eligibility and prerequisites, approval controls, public availability of requirements, application requirements, contact details, level change criteria, terminology, glossary entries, and document formatting/numbering. Removed references to learning materials or terms.	AI+ Security Level 2 Certification Scheme	NA



[www.aicerts.io](http://www.aicerts.io)

**Contact**

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