

**AI CERTS™**

# AI + Security Level 1™

Certification



# Executive Summary

Our comprehensive course, AI+ Security Level 1 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.

# Prerequisites

- **Basic Python Programming:** Familiarity with loops, functions, and variables.
- **Basic Cybersecurity Knowledge:** Understanding of CIA triad and common threats (e.g., malware, phishing).
- **Basic Machine Learning Concepts:** Awareness of fundamental machine learning concepts, not mandatory.
- **Basic Networking:** Understanding of IP addressing and TCP/IP protocols.
- **Linux/Command Line Skills:** Ability to navigate and use the CLI effectively.

# Exam Blueprint

Number  
of Questions

**50**

Passing  
Score

**35/50 or 70%**

Duration

**90 Minutes**

Format

**Online via AI  
Proctoring platform**

Question Type

**Multiple Choice/Multiple  
Response**

# Exam Overview

<b>Module</b>	<b>Weight</b>
<b>Introduction to Cybersecurity</b>	<b>6%</b>
<b>Operating System Fundamentals</b>	<b>7%</b>
<b>Networking Fundamentals</b>	<b>7%</b>
<b>Threats, Vulnerabilities, and Exploits</b>	<b>10%</b>
<b>Understanding of AI and ML</b>	<b>10%</b>
<b>Python Programming Fundamentals</b>	<b>10%</b>
<b>Applications of AI in Cybersecurity</b>	<b>10%</b>
<b>Incident Response and Disaster Recovery</b>	<b>10%</b>
<b>Open Source Security Tools</b>	<b>10%</b>
<b>Securing the Future</b>	<b>10%</b>
<b>Capstone Project</b>	<b>10%</b>
	<b>100%</b>

**AI CERTs™**

**AI<sup>+</sup>**

Security Level 1™

# Certification Modules

## Module 1

### **Introduction to Cybersecurity**

---

1.1 Definition and Scope of Cybersecurity

---

1.2 Key Cybersecurity Concepts

---

1.3 CIA Triad (Confidentiality, Integrity, Availability)

---

**1.4 Cybersecurity Frameworks and Standards (NIST, ISO/IEC 27001)**

---

**1.5 Cyber Security Laws and Regulations (e.g., GDPR, HIPAA)**

---

**1.6 Importance of Cybersecurity in Modern Enterprises**

---

**1.7 Careers in Cyber Security**

---

## Module 2

# Operating System Fundamentals

---

**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

# Networking Fundamentals

---

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

# Threats, Vulnerabilities, and Exploits

---

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 Introduction to Vulnerabilities**

---

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

---

**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**

# **Understanding of AI and ML**

---

**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

# Python Programming Fundamentals

---

6.1 Introduction to Python Programming

---

6.2 Understanding of Python Libraries

---

6.3 Python Programming Language for Cybersecurity Applications

---

6.4 AI Scripting for Automation in Cybersecurity Tasks

---

6.5 Data Analysis and Manipulation Using Python

---

6.6 Developing Security Tools with Python

---

## Module 7

# Applications of AI in Cybersecurity

---

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

# Incident Response and Disaster Recovery

---

## 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 Assessments

---

## 8.10 Legal and Regulatory Considerations of Security Incidents

---

# Module 9

## Open Source Security Tools

---

### 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 Tools**

---

## **Module 10**

# **Securing the Future**

---

**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**

**Capstone Project**

---

**11.1 Introduction**

---

**11.2 Use Cases: AI in Cybersecurity**

---

**11.3 Outcome Presentation**

---

# Certification Outcome

Upon successful completion of the AI+ Security level 1 course, participants will be awarded a certificate attesting to their proficiency in Python programming for AI and Cybersecurity applications, mastery in applying machine learning techniques to identify and mitigate cyber threats, including email threats, malware, and network anomalies, familiarity with advanced AI techniques such as Generative Adversarial Networks (GANs) for cybersecurity enhancement, practical skills in conducting penetration testing using AI methodologies, and the ability to synthesize acquired knowledge through a Capstone Project addressing real-world cybersecurity challenges. This certificate validates the participant's competence in leveraging Artificial Intelligence to fortify cybersecurity measures and their preparedness to confront the dynamic complexities of modern digital security landscapes.



## Market Insight

AI and Cybersecurity integration is booming as organizations adapt to evolving cyber threats. The global AI in cybersecurity market is set to expand significantly, driving demand for skilled professionals. Initiatives like "Introduction to AI and Cyber Security" are pivotal in preparing professionals to harness AI for robust cyber defense.



## Value Proposition

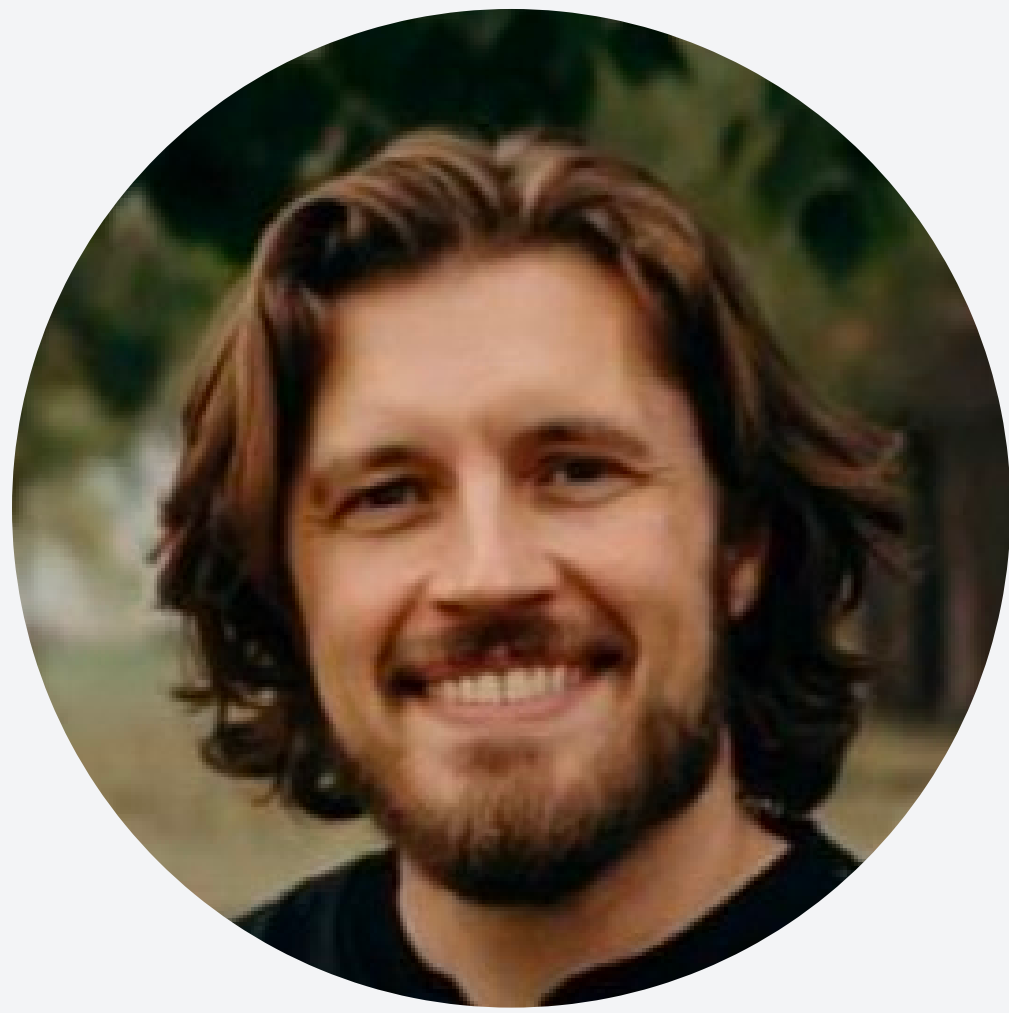
AI+ Cybersecurity empowers professionals with essential skills to protect against evolving cyber threats. By merging AI principles with cybersecurity practices, participants gain practical expertise in Python programming, machine learning, and advanced AI algorithms. Stay ahead in today's digital landscape with our hands-on training and drive innovation within your organization.



## Additional Features

Alongside comprehensive AI and cybersecurity training, AI+ Cybersecurity offers interactive labs, expert-led discussions, and career development resources for professional growth within the cybersecurity field. Ongoing support from instructors and access to the latest tools ensure participants stay updated and equipped to address evolving cyber threats while driving innovation.

# AI Experts



## Jason Kellington

AI Expert

As a consultant, trainer, and technical writer with more than 25 years of experience in IT, I specialize in the development and delivery of solutions focused on effective and efficient enterprise IT.



## Justin Frébault

AI Expert

I'm a boutique data consultant specializing in data mesh and lakehouse solutions. I've dedicated my career to helping organizations transform their approach to data, moving beyond mere knowledge.



## J Tom Kinser

AI Expert

I have over forty years of experience in software development, data engineering, management, and technical training. I am a Microsoft Certified Trainer and a software developer, holding multiple certifications.



## Terumi Laskowsky

AI Expert

Country Manager for Global Consulting Services in Japan, Specialties: Information Security (Compliance, Policy, Application, Host, Network)

# AI CERTS™

AI & BITCOIN CERTIFICATIONS!

[aicerts.io](https://aicerts.io)

## Contact

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

