AICERTs™

AI+ Security Level 2™

Certification

Executive Summary

Our comprehensive course, AI+ Security Level 2 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.

AI CERTs™

AI+ Security Level 2 Exam Blueprint

Date Issued: 20/3/2024
Version: 1.1

Prerequisites

- Completion of AI+ Security Level 1, not mandatory
- **Basic Python Skills:** Familiarity with Python basics, including variables, loops, and functions
- **Basic Cybersecurity:** Basic understanding of cybersecurity principles, such as the CIA triad and common cyber threats
- **Basic Machine Learning Awareness:** General awareness about machine learning, no technical skills required
- **Basic Networking Knowledge:** Understanding of IP addresses and how the internet works.
- **Basic command line Skills:** Comfort using the command line like Linux or Windows terminal for basic tasks
- **Interest in AI for Security:** Willingness to explore how AI can be applied to detect and mitigate security threats.

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

Module	Weight
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%
	100%

AI CERTs™

AI+

Security Level 2™

Certification Modules

Module 1

Introduction to Artificial Intelligence (AI) and Cyber Security

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

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

3.1 Understanding the Application of Machine Learning in Cybersecurity

3.2 Anomaly Detection to Behaviour 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

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

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

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

7.1 Introduction

7.2 Enhancing User Authentication with AI Techniques

7.3 Introducing Biometric Recognition, Anomaly Detection, and Behavioural Analysis

7.4 Providing a Robust Defence Against Unauthorized Access

7.5 Ensuring a Seamless Yet Secure User Experience

7.6 Tools and Technology: AI-based Authentication Platforms

7.7 Conclusion

Module 8

Generative Adversarial Network (GAN) for Cyber Security

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

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

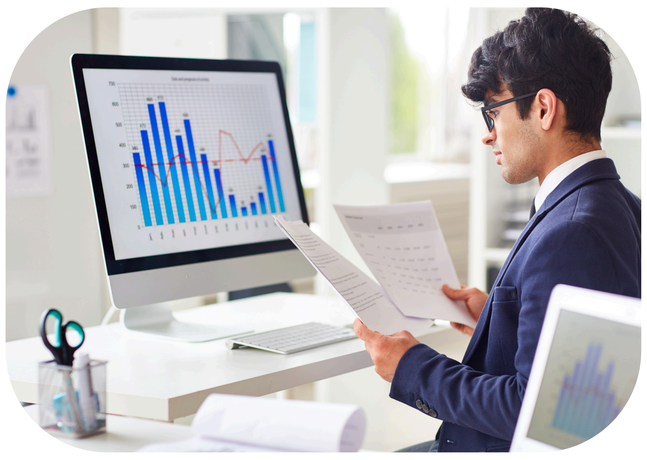
10.1 Introduction

10.2 Use Cases: AI in Cybersecurity

10.3 Outcome Presentation

Certification Outcome

Upon successful completion of the AI+ Security Level 2 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.

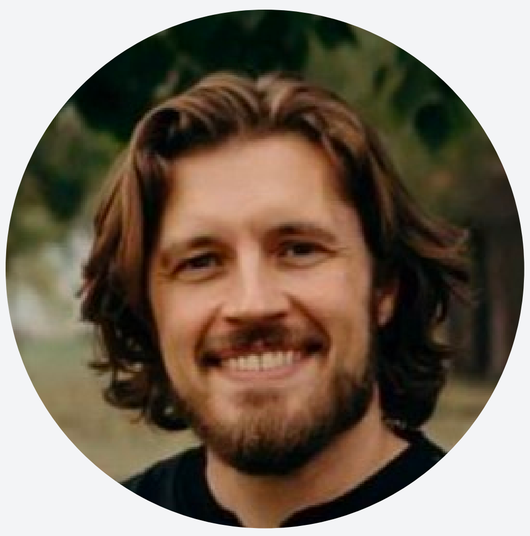
Value Proposition

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)

AICERTs™

AI & BITCOIN CERTIFICATIONS!

aicerts.io

Contact

252 West 37th St., Suite 1200W

New York, NY 10018