AICERTs™

AI+ Security™ Level 3

Certification

Executive Summary

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.

AI CERTs™

AI+ Security Level 3 Exam Blueprint

Date Issued: 20/3/2024
Version: 1.1

Prerequisites

- Completion of AI+ Security Level 1 and 2
- **Intermediate / Advanced Python Programming:** Proficiency or expert in Python, including deep learning frameworks (TensorFlow, PyTorch).
- **Intermediate Machine Learning Knowledge:** Proficiency in understanding of deep learning, adversarial AI, and model training.
- **Advanced Cybersecurity Knowledge:** Proficiency in threat detection, incident response, and network/endpoint security.
- **AI in Security Engineering:** Knowledge of AI's role in identity and access management (IAM), IoT security, and physical security.
- **Cloud and Container Expertise:** Understanding of cloud security, containerization, and blockchain technologies.
- **Linux/CLI Mastery:** Advanced command-line skills and experience with security tools in Linux environments.

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

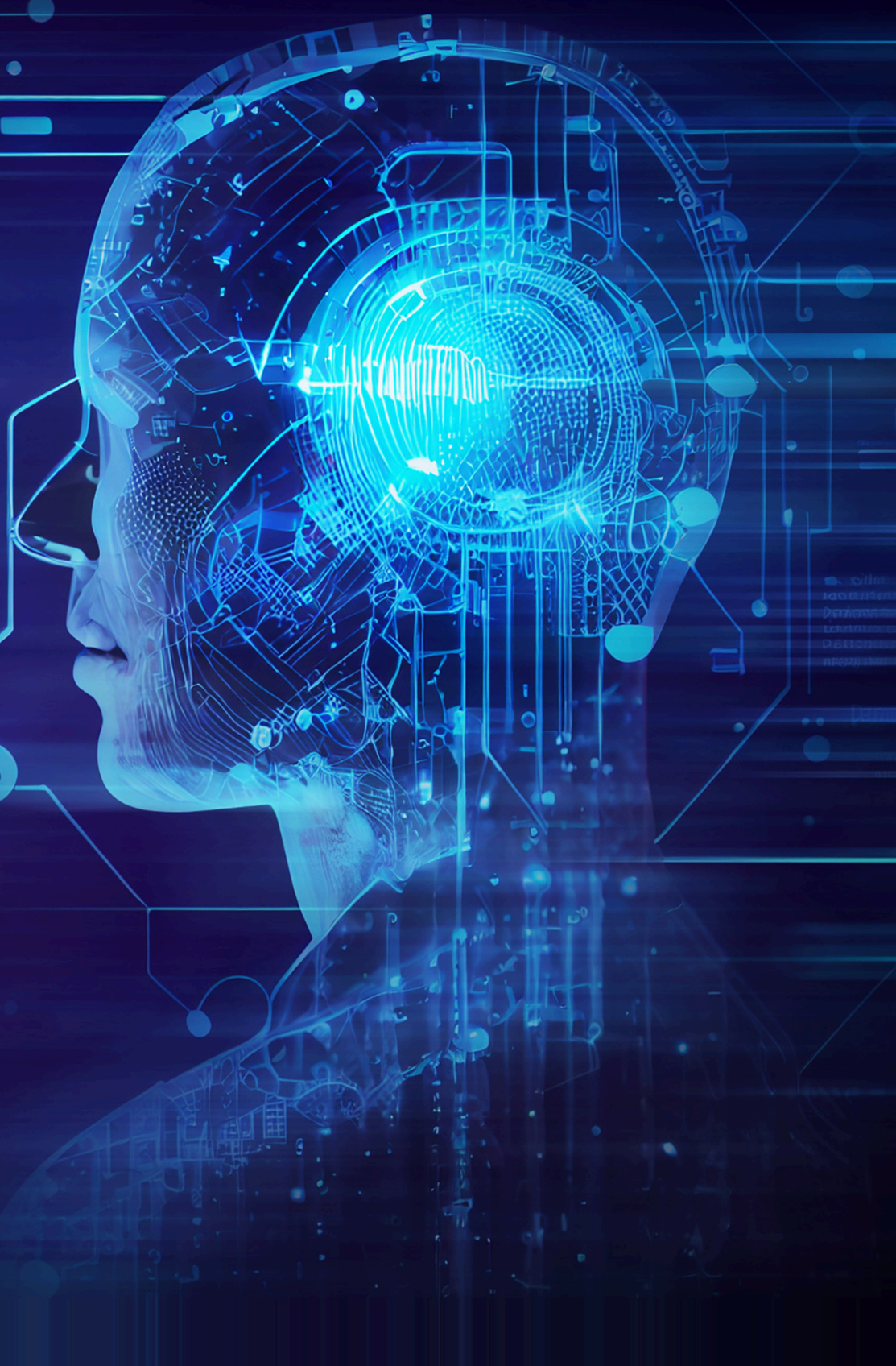
Exam Overview

Module	Weight
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%
	100%

AI CERTs™

AI+

Security Level 3™



Certification Modules

Module 1

Foundations of AI and Machine Learning for Security Engineering

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

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

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

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

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

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

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

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

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)

10.1 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

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

12.1 Defining the Capstone Project Problem

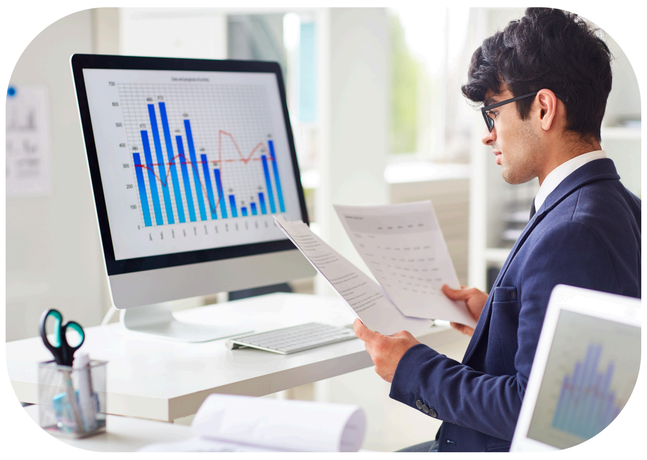
12.2 Engineering the AI Solution

12.3 Deploying and Monitoring the AI System

12.4 Final Capstone Presentation and Evaluation

Certification Outcome

Upon completing the AI+ Security Level 3 course, participants will gain advanced expertise in applying AI and machine learning to enhance cybersecurity measures. They will be proficient in leveraging AI-driven techniques for threat detection, response, and securing networks, endpoints, and cloud environments. Graduates will also be equipped to handle adversarial AI challenges, implement secure AI systems, and apply AI to areas like identity management, IoT, and blockchain-based security. The capstone project ensures practical experience in designing AI-powered security solutions, preparing participants for roles in AI-driven cybersecurity engineering and architecture.



Market Insight

The AI-driven cybersecurity market is expanding quickly, projected to exceed $60 billion by 2028, as businesses increasingly adopt AI to combat sophisticated cyber threats. Expertise in AI-powered security solutions is becoming highly valuable across industries, especially in finance, healthcare, and critical infrastructure.

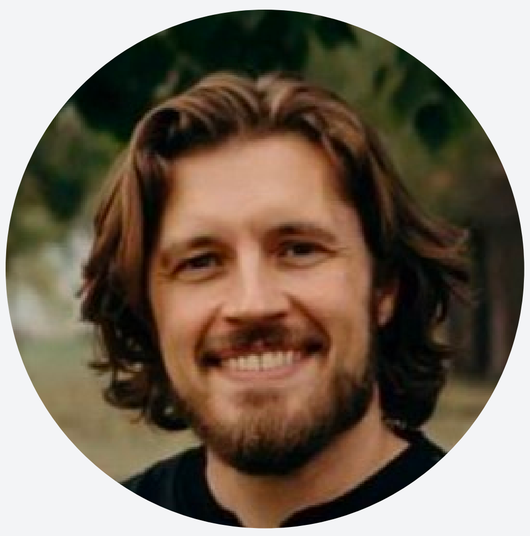
Value Proposition

The AI+ Security Level 3 course equips professionals with cutting-edge skills to leverage AI and machine learning for advanced cybersecurity. Participants will gain hands-on expertise in designing AI-driven security solutions, making them highly competitive in a rapidly evolving market where AI is essential for combating sophisticated cyber threats.

Additional Features

The AI+ Security Level 3 course offers hands-on experience through a capstone project, expert-led instruction, and training with cutting-edge AI tools like TensorFlow and PyTorch. It also includes industry-relevant case studies, providing practical insights into AI applications for modern cybersecurity challenges.

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