AI SECURITY (AISEC) PRACTITIONER

Certification Overview

The AISEC Practitioner Certification provides the knowledge to sift through information, separating facts from the noise and understanding what's behind the excitement of AI. It gives you an understanding of what hype is and what isn't and, more importantly, where AI is going.

It explains the problems that can occur when AI isn't properly managed and the approaches adversaries take to attack AI. It also lets you understand and set up the guardrails to ensure your business can use AI safely and responsibly. The course provides real hands-on experience for applying AI security.

Learning Outcomes

On completing the AISECP Certification Course exam, you will gain competence in managing AI systems securely, safely, and responsibly. This includes understanding the underlying technology on which Generative-AI models and proactively identifying risk and security requirements for AI model deployments.

AI Security Knowledge

You will know the underlying technologies used to build AI models and understand the AI development lifecycle. You will know about the threats affecting AI and the controls you need to mitigate the risks.

AI Security Skills

You will be skilled in applying controls to AI systems and assessing the effectiveness of controls built into AI systems. You will be able to assess the risk and test and audit an AI system.

Our Trainers Make the Difference

Dr Malcolm Shore

Malcolm Shore is recognised as a global security leader and renowned keynote speaker.

Malcolm is the Chief Technology Officer at Outpace and an adjunct PhD supervisor at Deakin University. He is also a renowned LinkedIn instructor with a portfolio of over 30 cybersecurity courses. Malcolm held the role of Director of Infosec at GCSB, the national security agency in New Zealand, for a decade and has subsequently held various CISO and Technical Director positions across Australasia.

Malcolm represented NZ and Australia on the ASEAN Cyber Security Strategy Committee, CSCAP, and subsequently attended the Global Cyberspace Conferences as part of the Australian delegation. As part of his role in capacity building for cybersecurity in Australia, he initiated and developed Certificate IV in Cybersecurity for TAFE institutes. He actively contributes to GFCE (Global Forum for Cyber Expertise).

Who Should Attend

The AISECP Certification Course is suitable for anyone with an IT background who wants to understand the secure, safe, and responsible use of AI. It would particularly suit risk and security leaders and professionals who want to extend their skills into the AI field.

Typical roles would include:

- Those involved or interested in learning AI security
- SecOps, CloudOps, NetOps, MLOps and DevOps Engineers
- IT Professionals, Security Practitioners, and Domain Architects
- IT Support Staff and Managed Service Providers
- Product Managers, Software Engineers and Testers
- Data Governance Leaders, Data Architects & Operations
- SOC Analysts, Penetration Testers and Security Engineers

Course Contents

Domain 1: AI Introduction

- Understand AI ethics - ethics plays a big part in AI.
- Understand the principles of AI.

Domain 2: AI Technology

- Understand the history and basic concepts of AI.
- Be familiar with the structure of AI models.
- Learn how to run tokenisation and embedding for an AI model.
- Understand how data is used to train and enhance AI models.
- Learn how to run AI models locally, from the marketplace repository, and via online services.
- Learn how to run AI models programmatically.

Domain 3: AI Risk Management

- Understand the threats to AI.
- Learn how to use various prompt injection techniques to extract sensitive data from a model.
- Learn how to inject a backdoor into an AI Model and “pop a shell”.
- Learn how to manipulate an image to defeat image classification.
- Apply AI risk management based on the NIST AI Risk Management Framework.

Domain 4: AI Governance

- Understand AI governance. This covers the overall approach to the governance of AI
- Understand the conceptual AI architecture and how to develop an AI information architecture
- Understand and review an AI policy document.

Domain 5: AI Controls

- Introduce AI controls. This introduces the set of key controls used to protect AI systems.
- Learn how to apply Guardrails. This section describes typical design patterns.
- Red Teaming for AI. This describes using scanners to test AI models
- Learn how to use a variety of AI model scanners
- Logging and Monitoring for AI.

Domain 6: AI Agents

- Understand the principles of agentic AI
- Understand Agentic AI mesh
- Use the smolagent framework to develop an AI agent
- Assess the security implications of AI agents

Domain 6: AI Labs

- Understand the principles of agentic AI
- Hands-on with AI technology
- Hands-on with Prompt and thought injections
- Hands-on with Guardrails and scanners
- Hands-on with Agentic AI

Fees

AI Security (AISEC) Practitioner Course (3 Days)

Face-to-Face Training: $3,450 (ex GST)
Live Virtual Training: $2,950 (ex GST)

Course fee includes:

- Course presentation
- Course workbook
- Supplementary materials
- Certification exam

Face-to-Face Training—AISEC certification participants will receive a paper-based exam completed in the same venue during the course. The trainer and supporting staff invigilate the exams.

Live Virtual Training—AISEC certification participants will take the exam online during the course. The trainer and supporting staff invigilate the exams live.

Prerequisites

The AISEC Practitioner Course is designed for IT professionals. A working knowledge of AI systems and an understanding of basic Python will be an advantage.

Exam Format

The AISECP exam is a two-part online exam.

This includes a multiple-choice theory exam covering the required topics, plus four hands-on assessments designed to simulate the process of designing secure AI and assessing threats.

The multiple-choice exam consists of:

- 30 questions
- Multiple choice and single answer
- 1 hour (15 additional mins for EASL)
- Pass mark 75%

Examination Resit Options

Candidates who fail the multiple-choice exam or the assessments are entitled to one free resit. However, as the course material will be updated to account for developments in AI, resits should be taken as quickly as practicable.

Certification Levels

Candidates passing the multiple-choice exam will be awarded the **AI Security Level 1** Practitioner Certificate (AISECP—Level 1). Candidates who pass the multiple-choice exam and at least three of the four assessments will be awarded the **AI Security Level 2** Practitioner Certificate (AISECP—Level 2).