

Certified AI Security Professional™ Interactive Live Training

2.5 Days

DURATION

19

MODULES

76

TOPICS

COURSE OVERVIEW

Certified AI Security Professional Interactive Live Training is a hands-on, instructor-led program designed to help professionals secure modern AI systems across the full lifecycle. This AI Security ILT course equips you with practical skills to identify and mitigate risks in machine learning models, data pipelines, MLOps workflows, cloud environments, and generative AI applications. Through live expert sessions, real-world case studies, and guided exercises, you will learn how to defend against adversarial attacks, prompt injection threats, model vulnerabilities, and data privacy risks. Gain expertise in AI governance, compliance, secure deployment, runtime monitoring, and incident response, ensuring your AI systems are resilient, trustworthy, and enterprise-ready. Delivered across 2 interactive live days totaling 6 hours of instructor-led training plus 12 hours of self-paced content, this program combines real-time expert guidance with flexible independent learning. Enrol now in the Certified AI Security Professional ILT and become a leader in AI security, AI risk management, and secure AI implementation.

WHO THIS COURSE IS FOR

- Working Professionals — Who prefer structured, instructor-led learning with real-time Q&A and accountability.
- Career Changers — Looking for guided, hands-on training with expert mentorship to break into a new field.
- Team Leads & Managers — Who need deep understanding to lead technology initiatives and make informed decisions.
- Entrepreneurs & Founders — Planning to build products or services and want expert guidance on implementation.

TOOLS AND REQUIREMENTS

- Basic understanding of technology concepts
- A computer with stable internet connection for live sessions
- Webcam and microphone recommended for interactive participation
- No prior specialized experience necessary - the program starts from foundations

- Students & Fresh Graduates — Seeking a competitive edge with a globally recognized, hands-on certification.
- Consultants & Advisors — Who need to quickly build expertise with structured, expert-guided training.

LEARNING OBJECTIVES

What You Will Learn

- Foundations of AI and AI Security
- AI Architecture
- MLOps
- and Data Security
- Privacy
- Governance
- Real-time problem solving with live instructor guidance
- Hands-on labs and collaborative exercises
- Industry best practices and real-world applications
- Exam preparation strategies and tips

COURSE SYLLABUS

19 Modules, 76 Topics

MODULE 1

01

Foundations of AI and AI Security

TOPICS

- Introduction to Foundations of AI and AI Security
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 2

02

AI Architecture

TOPICS

- Introduction to AI Architecture
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 3

03

MLOps

TOPICS

- Introduction to MLOps
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 4

04

and Data Security

TOPICS

- Introduction to and Data Security
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 5

05

Privacy

TOPICS

- Introduction to Privacy
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 6

06

Governance

TOPICS

- Introduction to Governance
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 7

07

and Responsible AI

TOPICS

- Introduction to and Responsible AI
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

08

Threat Modeling and Adversarial ML

TOPICS

- Introduction to Threat Modeling and Adversarial ML
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

09

Secure AI Development and Operations

TOPICS

- Introduction to Secure AI Development and Operations
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

10

Generative AI

TOPICS

- Introduction to Generative AI
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 11

11

LLM

TOPICS

- Introduction to LLM
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 12

12

and Prompt Security

TOPICS

- Introduction to and Prompt Security
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 13

13

AI Infrastructure and Cloud Security

TOPICS

- Introduction to AI Infrastructure and Cloud Security
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 14

14

AI Security Operations

TOPICS

- Introduction to AI Security Operations
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 15

15

Detection

TOPICS

- Introduction to Detection
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 16

16

and Testing

TOPICS

- Introduction to and Testing
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 17

17

Use Cases

TOPICS

- Introduction to Use Cases
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 18

18

Trust

TOPICS

- Introduction to Trust
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

MODULE 19

19

and the Future of AI Security

TOPICS

- Introduction to and the Future of AI Security
- Core concepts and principles
- Practical exercises and demonstrations
- Best practices and industry standards

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com