

1-Day Training: AI Security Professional Certificate Training (choose in-person or remote)

1 Day

DURATION

1

MODULES

5

TOPICS

COURSE OVERVIEW

Proven training. Brand-new certification. A world first. Be among the first professionals worldwide to earn the new EXIN AI Security Professional certification! After breaking attendance records at OWASP events, this proven AI security training makes its US debut. And for the first time anywhere in the world, participants can combine the training with the opportunity to obtain the new EXIN AI Security Professional (AISP) certification. Delivered personally by the lead author of the courseware and founder of the OWASP AI Exchange, this is a unique opportunity to learn from the source and become part of the world's first certified cohort. The training fee includes an exam voucher, allowing participants to take the official accredited certification exam after the course. Learn more at aisp.exin.com . The one-day training is based on the OWASP AI Exchange , the leading open framework for AI security that contributes to international AI security standards. It combines foundational knowledge, the latest developments in AI security, and practical exercises to help you understand and address the rapidly evolving AI threat landscape. Your training fee includes an exam voucher that allows you to take the exam for the officially accredited EXIN AI Security Professional certification after completing the course. The certification is now available worldwide, providing security and AI professionals with formal recognition of their AI security knowledge. Learn more about the certification at aisp.exin.com . Built on the OWASP AI Exchange The course is based on the flagship OWASP AI Exchange (owaspai.org) project: an international, community-driven framework bringing together AI security threats, vulnerabilities, and controls. The framework provides foundational input for the international AI security standard ISO/IEC 27090 and the draft European AI security standard supporting the EU AI Act. This connection to international standardization ensures that the training goes beyond individual technologies and addresses the fundamental principles of AI security. This intensive, one-day training provides a structured and practical dive into AI security, covering both established threats and the latest developments in generative, agentic, and all AI. Starting with a pragmatic introduction to AI, the course explores the distinctive vulnerabilities and attack surfaces of AI systems, the methods attackers use to exploit them, and the security measures available to reduce these risks. Through practical exercises, you will gain hands-on experience with attacking AI systems, applying security controls, performing AI threat modelling, and conducting targeted vulnerability assessments. The primary focus is protecting AI systems against security threats, but the training also addresses related topics at a foundational level, including AI

governance, responsible AI, AI-supported software development, AI red teaming, and the use of AI in offensive security. The material reflects current developments in AI security research, practical experience, and international standardization.

WHO THIS COURSE IS FOR

- AI introduces new security challenges and responsibilities across many professional disciplines. Whether you are a security professional, software developer, AI engineer, red teamer, architect, or auditor, you need to understand the new attack surfaces and threats introduced by AI.
- What are your responsibilities when developing, deploying, or assessing AI systems? What vulnerabilities and attack techniques should you be aware of? And which security measures are effective against these emerging threats?
- This training provides the knowledge and practical insights needed to answer these questions.
- The training requires no advanced knowledge of AI or cybersecurity, although some experience in either field is helpful. Don't mistake accessibility for simplicity: the course covers cutting-edge developments in AI security, with insights and practical exercises that will challenge even experienced professionals.

LEARNING OBJECTIVES

What You Will Learn

- Understand the fundamental security challenges associated with AI, including generative and agentic AI.
- Recognize AI-specific vulnerabilities, attack techniques, and emerging threats.
- Understand how to select and apply appropriate security measures.
- Gain practical experience in AI threat modelling, security testing, and defensive techniques.
- Be better equipped to implement, evaluate, or review AI security measures in your organization.
- You will also receive a free exam voucher for the accredited EXIN AI Security Professional certification , allowing you to demonstrate your knowledge through an internationally available professional certification.

1 Module, 5 Topics

01

TOPICS

- AI security fundamentals : Understanding AI technology, its attack surfaces, security challenges, and associated responsibilities.
- AI-specific threats: Prompt injection, data poisoning, model theft, evasion, and other attacks targeting AI systems.
- Generative and agentic AI security : Understanding the additional threats introduced by large language models, autonomous agents, and their interactions with tools and external systems.
- Security controls: Selecting and applying measures to prevent, detect, and mitigate AI security threats.
- Threat modelling and security testing : Identifying potential attack scenarios and assessing vulnerabilities in AI applications.

DELIVERY NOTE

How It Is Delivered

- Duration: One full day.
- Level: Suitable for participants with varying levels of experience. Some knowledge of AI or cybersecurity is helpful, but no advanced expertise is required.
- Materials :Participants receive essential course handouts.
- Equipment :No laptop or other device is required for the exercises, although having a device available may be useful for looking up additional information.
- Certification : The training fee includes a voucher for the EXIN AI Security Professional certification exam, which participants can take after the training.

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