# PECB Certified Artificial Intelligence Security Professional

**Master the skills to secure the future of AI and gain practical, hands-on expertise to identify AI-specific threats, defend AI systems, and build secure, resilient, and trustworthy AI environments.**

## Why should you attend?

Artificial intelligence systems introduce security risks that extend well beyond traditional cybersecurity controls. Unlike conventional software, AI systems can be manipulated through their inputs, corrupted through their training data, compromised through their supply chains, and exploited through the tools and permissions they are granted often in ways that leave no trace in standard security logs. Security professionals who work with or around AI systems need a fundamentally different set of competencies from those that protect traditional IT environments, and this course is designed to build exactly those competencies.

In this course, participants will develop a thorough understanding of how AI systems are attacked, how they are defended, and how they are governed, moving from foundational AI security concepts through to hands-on practical application.

The training course includes lab exercises that give participants direct experience with real-world AI security tools and techniques, including prompt injection testing, AI red teaming, threat intelligence workflows, and malware analysis using AI-assisted reverse engineering tools. These labs are designed to reinforce the technical content of each section and ensure that participants leave the course with skills they can apply immediately in their professional roles.

By the end of the course, participants will be equipped to assess the security posture of AI systems, implement appropriate controls, respond to AI security incidents, and support their organization's AI governance and compliance obligations.

## Who should attend?

This training course is intended for:

- AI and machine learning engineers responsible for developing, deploying, or maintaining AI systems
- Cybersecurity and information security professionals looking to extend their expertise to AI-specific threats and defenses
- SOC analysts and threat intelligence professionals working in AI-enabled security environments
- IT security architects and consultants designing or reviewing AI system architectures
- Risk management and compliance professionals working with AI governance frameworks and regulatory requirements
- Data scientists and AI developers seeking to apply security practices throughout the AI development life cycle
- Technology managers and technical leads responsible for AI security strategy and program management

## Course agenda

Duration: 5 days

### Day 1 | AI, ML, and deep learning fundamentals

- Training course objective and structure
- Introduction to AI security
- Modern AI systems
- Machine learning
- Deep learning

### Day 2 | LLM architecture, training workflows, and attack tactics

- Large language models (LLMs)
- Training and augmenting LLMs
- Attack tactics and techniques
- OWASP top 10 for LLM applications

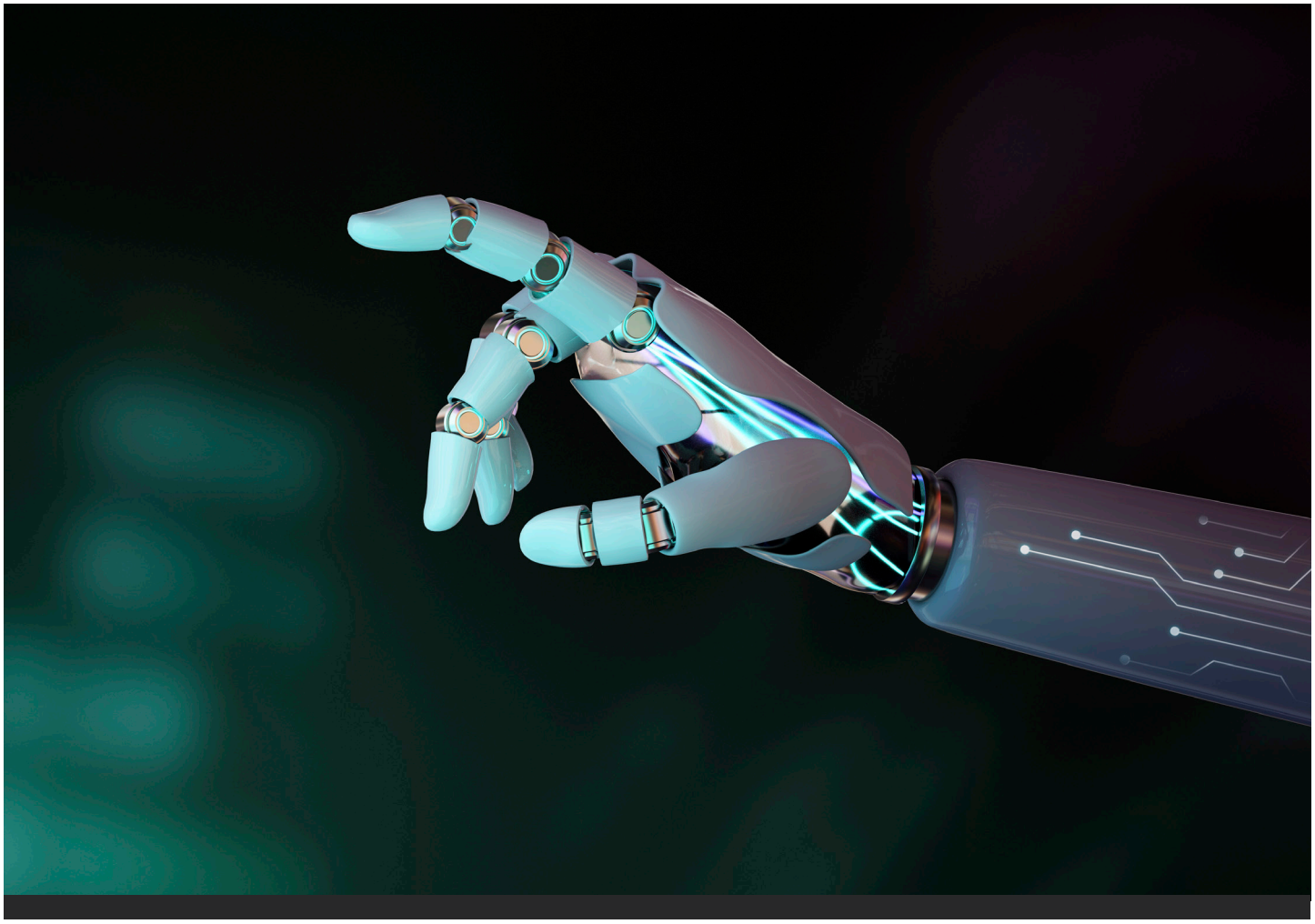
### Day 3 | AI security controls and mitigation strategies

- AI system security controls and operations
- AI-driven security monitoring and threat hunting
- AI-enhanced threat intelligence
- AI-assisted security analysis and reverse engineering

### Day 4 | Detection, response, and secure deployment

- AI-driven incident response
- Training and trusting AI models
- AI security governance and incident readiness
- Secure AI architecture
- Closing of the training course

### Day 5 | Certification exam



## Learning objectives

By the end of this training course, participants will be able to:

- Explain the architecture and operation of machine learning, deep learning, LLMs, and AI agents, and identify risks arising from their design, training, and deployment
- Analyze threats to AI and LLM systems using MITRE ATLAS and the OWASP LLM Top 10 across the AI attack life cycle
- Apply AI security controls, monitoring strategies, and threat intelligence workflows to detect, contain, and investigate adversarial activity
- Design and evaluate an AI security program covering incident response, supply chain governance, regulatory compliance, secure architecture, and red teaming

## Examination

Duration: 3 hours

The "PECB Certified Artificial Intelligence Security Professional" exam fully meets the PECB Examination and Certification Program (ECP) requirements. It covers the following competency domains:

**Domain 1** | Security foundations for AI and ML

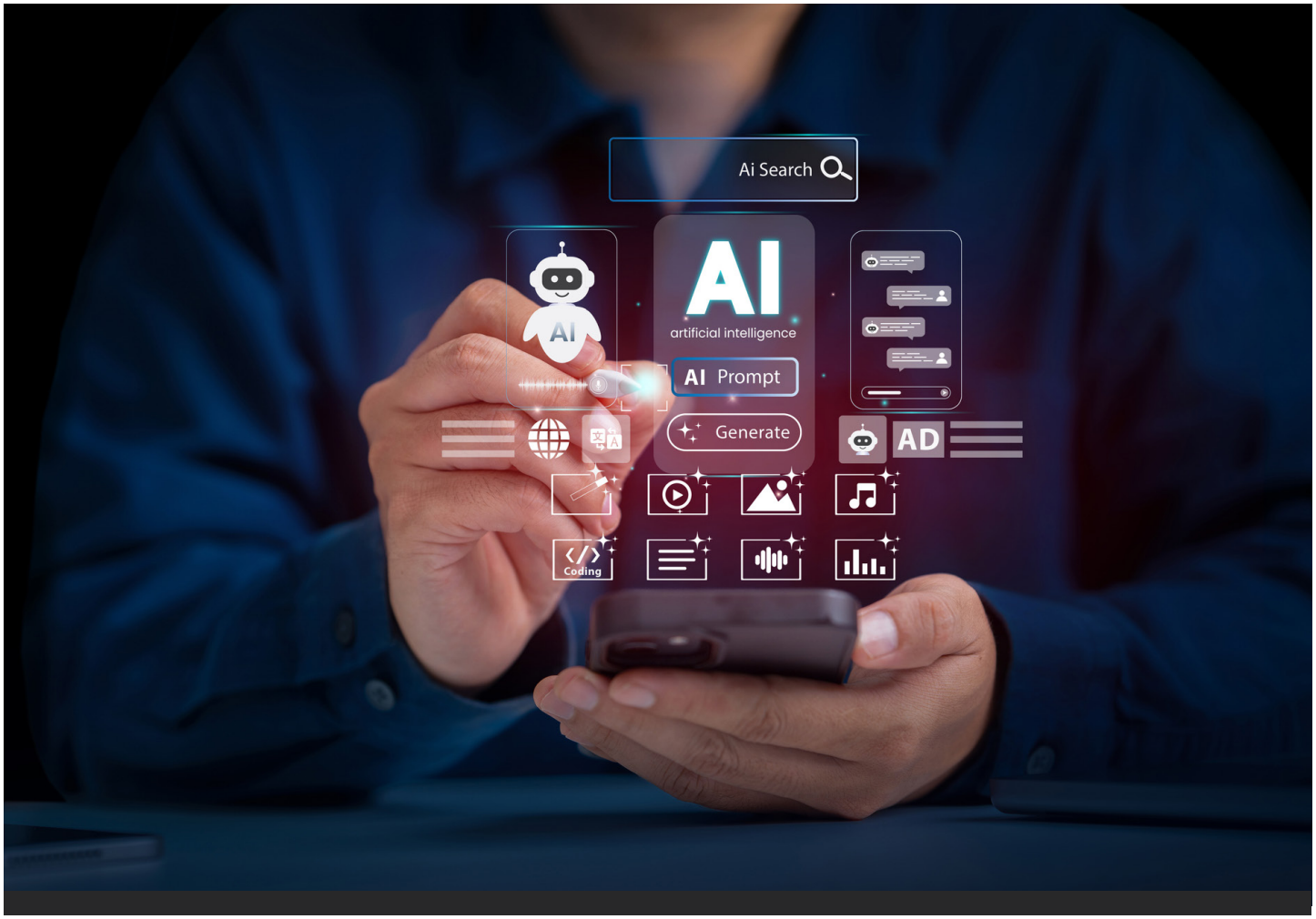
**Domain 2** | AI attack techniques and adversarial threats

**Domain 3** | AI security controls and defensive operations

**Domain 4** | AI enhanced security analysis and threat intelligence

**Domain 5** | AI governance, risk management, and secure architecture

For specific information about exam type, languages available, and other details, please visit the List of PECB Exams and the Exam Rules and Policies.




## Certification

After passing the exam, you can apply for the credential shown in the table below.
You will receive a certificate once you fulfill all the requirements of the selected credential.

The certificate requirements for Certified Artificial Intelligence Security Professional are:

| Professional credential | Exam | Professional experience | Project experience | Other requirements |
|---|---|---|---|---|
| **PECB Certified Provisional Artificial Intelligence Security Professional** | PECB Certified Artificial Intelligence Security Professional exam or equivalent | None | None | Signing the PECB Code of Ethics |
| **PECB Certified Artificial Intelligence Security Professional** | | 5 years (2 in information or cyber security | 300 hours | |

## General information

- For candidates who complete a training, eLearning, or self-study course delivered by a PECB Partner, the training fee includes the first exam attempt, one free retake, the certification application fee, and the first year of the Annual Maintenance Fee (AMF). This cycle must be completed within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats.
- Candidates will receive more than 320 pages of comprehensive training materials, including practical examples, exercises, and quizzes.
- An attestation of course completion worth 31 CPD (Continuing Professional Development) credits will be awarded to the candidate.
- If the initial exam is not passed, a free retake may be taken within 12 months of the course completion date. For self-study or eLearning courses, the 12-month period is calculated from the date of purchase.