+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 11/13/2026

Sign Up

Certified Artificial Intelligence Security Professional Training and Certification

5 days (35 hours)

Overview

PECB's official Certified Artificial Intelligence Security Professional certification validates the skills needed to secure artificial intelligence systems. From machine learning to LLMs and autonomous AI agents, the course covers threats, protective controls, and governance throughout the entire lifecycle.

Our Certified Artificial Intelligence Security Professional Certification Training will help you prepare for the exam while developing an operational approach to AI security tailored to professional environments.

You will learn to explain architectures, identify risks related to data and models, and analyze attacks using MITRE ATLAS and the OWASP LLM Top 10 as reference frameworks. The exercises will train you to select and evaluate appropriate protective measures.

Upon completion of the training, you will be able to define a secure AI architecture, organize monitoring, conduct an investigation, and structure the response to incidents specific to generative models and applications.

This preparation combines hands-on workshops with practice exam questions. It also covers the supply chain, compliance, and red teaming of AI systems. Earning the professional certification is subject to PECB's experience and certification requirements.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Explain how machine learning and deep learning work, as well as the architectures of LLMs and AI agents
- Identify the risks associated with the design, training, and deployment of AI systems
- Analyze threats across the entire attack cycle using MITRE ATLAS and the OWASP LLM Top 10 as reference frameworks
- Apply security controls, monitoring strategies, and threat intelligence
- Design and evaluate an AI security program that integrates governance, compliance, incident response, and red teaming
- Prepare for the Certified Artificial Intelligence Security Professional exam through hands-on exercises and practice questions

Target Audience

- Cybersecurity Engineer
- Security architect
- SOC Analyst
- AI and machine learning engineer
- Governance Consultant

Requirements

- Knowledge of cybersecurity principles, access control, and data protection
- Familiarity with threat modeling, security monitoring, and incident response incident response
- Basic understanding of machine learning and the training and inference stages
- Ability to read technical logs and API exchanges in an application environment
- Understanding of technical English to consult resources and prepare for the exam

Technical Prerequisites

- A computer running Windows 11 or macOS that is compatible with the training tools; 16 GB of RAM is recommended
- An up-to-date Chrome or Firefox browser to access remote labs; no dedicated graphics card is required
- Stable internet connection with authorized access to the learning platforms and isolated workshop environments
- A personal myPECB account and the PECB Exams app to take the online exam, with prior compatibility check
- Webcam, microphone, and a quiet space for remote training and proctored exam monitoring

Curriculum for our Certified Artificial Intelligence Security Professional training

[Day 1 - Morning]

AI Fundamentals and Scope of Certification

- The five competency areas of the certification and exam preparation objectives
- Differences between artificial intelligence, machine learning, deep learning, and generative AI
- Principles of supervised, unsupervised, and reinforcement learning
- The AI system lifecycle, sensitive assets, and stakeholder responsibilities
- Hands-on workshop: mapping the components, data, and critical assets of an AI service based on a certification case study.

[Day 1 - Afternoon]

ML architectures and model risks

- How Neural Networks Work: Training, Validation, and Inference
- Data pipelines, quality, data splitting, and overfitting
- Design risks, bias, privacy, and limitations of explainability
- Poisoning attacks, escape attacks, model extraction, and membership inference
- Hands-on workshop: Compare a model’s results on normal and corrupted data, then justify the identified risks and selected safeguards.

[Day 2 - Morning]

LLMs, RAG, and AI Agents

- Transformer architecture, tokenization, embeddings, and attention mechanisms
- Pre-training, fine-tuning, alignment, and risks associated with training data
- RAG architecture, vector databases, and document confidence boundaries
- How AI agents work, memory, orchestration, tools, and permission delegation
- Hands-on workshop: Analyze a RAG application with an agent and identify confidence boundaries as well as access paths to sensitive data.

[Day 2 - Afternoon]

Attack analysis with ATLAS and OWASP

- MITRE ATLAS overview, tactics, techniques, and progression of the attack cycle
- Analysis of the OWASP LLM Top 10 and correlations with certification scenarios
- Direct and indirect prompt injection, jailbreaking, and disclosure of sensitive information
- Supply chain compromise, vector vulnerabilities, insecure outputs, and excessive autonomy
- System prompt leakage, misinformation, and unchecked resource consumption

- Hands-on workshop: Testing injections in an isolated training application and mapping the scenario in MITRE ATLAS and the OWASP LLM Top 10.

[Day 3 - Morning]

Protective controls and secure architecture

- Defense in depth, segmentation, and applying Zero Trust principles to AI components
- Identity management, least privilege, secrets, and agent tool authorizations
- Input validation, secure output handling, and the limitations of safeguards
- Data protection, context isolation, quotas, and human validation of sensitive actions
- Hands-on workshop: Strengthen controls for a vulnerable AI application and compare the results before and after protection.

[Day 3 - Afternoon]

Monitoring and detection of adversarial activities

- Collection of AI telemetry, call traces, model versions, and tool execution
- Logging interactions and minimizing sensitive data in traces
- Anomaly detection, data drift, and distinguishing between degradation and hostile activity
- SIEM and SOAR integration, event correlation, and alert prioritization
- Measuring control effectiveness, detection coverage, and managing false positives
- Hands-on workshop: Build a detection rule based on AI logs and analyze a suspicious sequence of calls and data access.

[Day 4 - Morning]

Threat intelligence and AI-assisted investigation

- Threat intelligence lifecycle: collection, analysis, dissemination, and operational feedback
- Leveraging IoCs, attack indicators, and adversarial tactics, techniques, and procedures
- AI-assisted correlation, enrichment, and synthesis with source validation
- Threat hunting, code analysis, and malware report analysis with AI assistance
- Managing hallucinations, confidentiality, and hostile content in analyzed sources
- Hands-on workshop: producing an intelligence report based on a fictional incident file and verifying the conclusions proposed by the AI assistant.

[Day 4 - Afternoon]

Incident response and controlled deployment

- Preparing AI playbooks, incident classification, and escalation criteria
- Service containment, revocation of access, and suspension of agent actions
- Preservation of evidence, data timeline and investigation, models, and configurations
- Restoration from trusted artifacts, security validation, and return to production
- Securing pipelines, ensuring model integrity, and post-incident lessons learned
- Hands-on workshop: Conducting an agent compromise response exercise, from containment to the decision to restore service.

[Day 5 - Morning]

Governance, compliance, and the supply chain

- Building an AI security program: roles, policies, risk register, and metrics
- Supplier assessment, data and model provenance, dependencies, and supply chain
- Analysis of applicable requirements, alignment with the AI Act, ISO/IEC 42001, and the NIST AI RMF
- Preparing for red teaming, authorized scope, success criteria, and tracking remediation
- Hands-on workshop: Design and evaluate an AI security program, including target architecture, compliance requirements, and an adversarial testing campaign.

[Day 5 - Afternoon]

Summary and exam preparation

- Comprehensive review of the five domains of the Certified Artificial Intelligence Security Professional certification
- Strategies for answering multiple-choice questions and scenario analysis
- Time management, organization of permitted resources, and identification of key considerations
- Procedures for scheduling the official exam during a dedicated session and the distinction between passing the exam and receiving the certification
- Hands-on workshop: Take a targeted, timed practice exam, analyze your answers, and develop your personalized study plan.

Target Companies

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technology or to acquire specific professional knowledge or modern methods.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also enables us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could

problematic for the monitoring and smooth running of the training session.

Teaching Methods

Hands-On Course: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical presentations by the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg