Updated on 02/04/2026

Register

CompTIA SecAI+? Training: Certification (CY0-001)

ALL-IN-ONE: EXAM INCLUDED IN THE PRICE

5 days (35 hours)

Overview

Our CompTIA SecAI+ training will validate your expertise at the critical convergence of cybersecurity and artificial intelligence. This certification attests to your ability to secure AI systems while leveraging these technologies to strengthen your organization's defenses.

During this training, you will benefit from a comprehensive program to prepare you for this exam. We will begin this training with the essential concepts of AI (LLM, Machine Learning) and their life cycle, in order to understand what we need to protect.

You will also learn how to master threat modeling (OWASP Top 10 LLM, MITRE ATLAS) and implement security barriers (Guardrails) for models and data. By the end of the training, you will know how to use AI as a defense tool (analysis, automation) while detecting specific attacks such as Prompt Injection or Poisoning.

Like all our training courses, this one will introduce you to the latest version of the exam objectives (CY0-001) and focuses on a practical approach through labs.

Objectives

- Understand and distinguish between different types of AI (GenAI, LLM, Deep Learning).
- Secure AI systems through threat modeling and access controls.
- Detect and counter specific attacks (injection, hallucinations).
- Use AI to automate incident response.
- Apply governance and compliance (EU AI Act, NIST AI RMF).

Target audience

- Cybersecurity analysts / SOC
- AI security engineers
- Data scientists & security architects
- Cloud & DevSecOps Engineers

Prerequisites

- 3 to 4 years in the IT field, including more than 2 years of practical experience in cybersecurity
- Security+, CySA+, PenTest+, or equivalent certifications recommended
- Proficiency in technical English

Note: Ambient IT does not own Comptia Certifications©. This certification belongs to Comptia, Inc.

Our CompTIA SecAI+ (CY0-001) Training Program

[Day 1 - Morning]

Fundamentals of AI and Learning Techniques

- Types of AI: Generative AI, Machine Learning, Deep Learning
- Architectures: Transformers, LLM vs. SLM, GANs
- Training Techniques: Supervised vs. Unsupervised Learning, Reinforcement Learning
- Key Concepts: Fine-tuning, Epoch, Pruning, Quantization
- Prompt Engineering: Zero-shot, Multi-shot, System Roles, and Templates
- Hands-on workshop: Prompt manipulation and model comparison (LLM vs. SLM).

[Day 1 - Afternoon]

Data Security and AI Lifecycle

- Data processing: Data cleansing, data lineage, and provenance
- Technologies: RAG (Retrieval-Augmented Generation), vector storage, and embeddings
- Lifecycle security: From collection to deployment
- Validation and monitoring: Human-in-the-loop, supervision, and feedback
- Design principles: Trustworthiness and authenticity
- Hands-on workshop: Data lifecycle analysis and risk identification.

[Day 2 - Morning]

Threat modeling for AI

- Reference frameworks: OWASP Top 10 LLM and ML Security Top 10
- Frameworks: MITRE ATLAS and MIT AI Risk Repository
- Vulnerability management: CVE AI Working Group
- Analysis of risks specific to AI systems
- Hands-on workshop: Threat modeling on a use case with MITRE ATLAS.

[Day 2 - Afternoon]

Security Controls and Access Management

- Model controls: Model guardrails, prompt templates
- Gateway controls: Prompt firewalls, rate limits, token limits
- Access management: Models, data, agents, and APIs
- Testing and validation of security barriers (guardrails)
- Hands-on workshop: Configuring filtering rules and access limits.

[Day 3 - Morning]

Data Security and Encryption

- Encryption requirements: In transit, At rest, In use
- Data protection: Anonymization, Masking, Redaction
- Data classification and minimization
- Label management (data classification labels)
- Hands-on workshop: Implementing anonymization techniques on a dataset.

[Day 3 - Afternoon]

Monitoring and Auditing AI Systems

- Monitoring: Prompts (Query/Response) and Logs
- Log protection: Log sanitization
- Cost monitoring: Tokens, Storage, Processing
- Quality Auditing: Detection of Hallucinations, Bias, and Fairness
- Hands-on workshop: Log analysis and cost anomaly detection.

[Day 4 - Morning]

Analysis of Attacks and Countermeasures

- Input attacks: Prompt injection, jailbreaking
- Model attacks: Poisoning, model inversion, model theft
- Output attacks: Insecure output handling, Hallucinations

- Countermeasures: Least privilege, Input validation, Encryption
- Hands-on workshop: Simulation of a prompt injection attack and mitigation.

[Day 4 - Afternoon]

AI in Defense (Blue Team)

- Tools: Security chatbots, IDE plugins, personal assistants
- Use cases: Vulnerability analysis, Pattern recognition, Threat modeling
- Automation: Scripting (low-code/no-code), document synthesis
- CI/CD integration: Code scanning, automated unit testing
- Hands-on workshop: Using an AI assistant for secure code analysis.

[Day 5 - Morning]

AI as an attack vector and governance

- AI-assisted attacks: Deepfakes, advanced social engineering
- Offensive automation: Malware generation, Polymorphism
- Governance structures: AI Center of Excellence
- Key roles: AI architect, data scientist, AI risk analyst
- Hands-on workshop: Identifying AI-generated content (deepfakes/phishing).

[Day 5 - Afternoon]

Risks, Compliance, and Regulations

- AI risks: Bias, Data leaks, Shadow AI
- Principles: Fairness, Transparency, Explainability
- Regulations: EU AI Act, OECD Standards, ISO
- Frameworks: NIST AI RMF (Risk Management Framework)
- Compliance: Data sovereignty and corporate policies
- Hands-on workshop: Assessing AI project compliance according to the NIST AI RMF.

FAQ – QUESTIONS/ANSWERS

In what language is the CompTIA SecAI+ training course taught?

The training is in French.

Is the exam included in the price of the training?

Yes, the certification fee is included in the course price ($330 as a guide). You can take the exam at the end of the session.

How is the Comptia SecAI+ certification exam conducted?

The exam consists of a performance-based multiple-choice test with a maximum of **90**

questions. It is taken online at a Pearson Vue-approved exam center.

The exam lasts **90 minutes** and is available in English

To pass this exam, you must score at least 750 points on a scale of 100 to 900 points.

Target companies

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

Positioning at the start of training

The placement test at the start of the training course complies with Qualiopi quality criteria. Once they have finalized their registration, learners receive a self-assessment questionnaire that allows us to gauge their estimated level of proficiency in different types of technologies, as well as their expectations and personal goals for the upcoming training course, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

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