training code: SecAI+ (+exam) / ENG DL 5d / EN

CompTIA SecAI+ Authorized training with CY0-001 exam

The CompTIA SecAI+ training is an authorized course focused on securing artificial intelligence systems and leveraging AI in modern cybersecurity operations.

The program is designed for IT and security professionals who want to understand both the technical foundations of AI and the real-world risks associated with large language models, machine learning, data pipelines, and the integration of AI into organizational infrastructure.

Participants gain the skills to:

- analyze and model threats in AI systems
- design and implement technical security controls
- monitor and audit AI models
- apply AI in SOC operations, DevSecOps, and threat hunting
- manage risk, compliance, and responsible AI usage.

The training prepares candidates for the SecAI+ (CY0-001) exam and validates specialist-level competencies in AI security

The growing adoption of AI in business, along with regulations such as the AI Act, NIS2, the NIST AI Risk Management Framework, and ISO/IEC 42001, means that organizations must not only deploy AI solutions but also secure and govern them effectively.

SecAI+ addresses this challenge by teaching how to combine technical controls, security processes, and governance into a unified, coherent model.

Training recipients

The CompTIA SecAI+ course is intended for technical professionals and individuals responsible for information security who want to deepen their understanding of threats, protective mechanisms, and regulatory requirements related to artificial intelligence systems. The program focuses on AI architecture analysis, risk modeling, standards interpretation, and understanding attacks specific to ML and LLM models.

The course is particularly valuable for professionals who need structured knowledge of AI security in an organizational and strategic context — including security teams, architects, risk analysts, and governance and compliance specialists.

In particular, the course is recommended for:

- SOC analysts and cybersecurity teams
- Security engineers and system architects
- DevSecOps and Cloud Security specialists
- Professionals holding Security+, CySA+, PenTest+, or equivalent experience
- Specialists responsible for AI governance and risk management
- Organizations implementing LLMs, RAG architectures, AI agents, or ML-based solutions

Recommended experience: 3–4 years of IT experience and approximately 2 years in cybersecurity.

Benefits

Completing the CompTIA SecAI+ course enables participants to understand how artificial intelligence systems are reshaping the cybersecurity landscape — both from a defensive and adversarial perspective. Participants not only learn the theoretical foundations but also gain the ability to identify real technical and operational risks related to language models, data pipelines, API integrations, and AI agents used within organizations.

The course develops competencies in designing and implementing security controls for AI systems. This includes controlling access to models and data, implementing guardrails, rate limiting, encryption mechanisms, and monitoring prompts and logs. Participants learn to identify critical risk points across the AI lifecycle and apply appropriate technical and procedural safeguards.

Participants also gain the ability to align AI systems with organizational security policies, regulatory requirements, and responsible AI principles. This enables effective collaboration not only with technical teams but also with compliance, audit, and risk management departments.

As a result, graduates are prepared to securely deploy and manage AI-based solutions, integrate them into existing security infrastructure, and successfully attempt the CompTIA SecAI+ (CY0-001) certification exam, which formally validates their competencies.

Training program

1. Basic AI Concepts in Cybersecurity
   - Types of AI used in security
   - Prompt engineering and prompt security
   - Model training processes and validation
   - AI data security
   - The importance of security throughout the AI lifecycle
2. Threat Modeling and Securing AI Systems
   - AI threat modeling (OWASP LLM Top 10, MITRE ATLAS)
   - Identifying vulnerabilities in AI models
   - Model controls and guardrails
   - Gateway controls (rate limiting, prompt firewalls)
   - Securing on-premises and vendor-delivered models
   - Security validation and testing
3. Access Control and Data Security in AI
   - RBAC and ABAC in the context of AI
   - Access control for models, data, agents, and APIs
   - Data encryption (in transit, at rest, in use)
   - Masking, anonymization, and data minimization
   - Prompt and log monitoring
   - AI cost monitoring and quality auditing
4. Attacks on AI Systems and Compensating Controls
   - Prompt injection and jailbreaking
   - Data poisoning and model poisoning
   - Model inversion and model theft
   - Supply chain attacks
   - Sensitive information disclosure
   - Designing compensating controls
   - Red teaming AI models
5. AI in Security Operations
   - AI in vulnerability analysis
   - AI in detection and response
   - Automation of incident response and DevSecOps
   - AI-assisted scripting
   - AI in threat modeling
   - AI-enhanced attack vectors (deepfakes, OSINT automation, reconnaissance)
6. Governance, Risk & Compliance in AI
   - Governance structures (AI Center of Excellence)
   - Organizational roles (AI Risk Analyst, AI Governance Engineer)

- Responsible AI (human-in-the-loop, oversight)
- Monitoring risk and model drift
- AI documentation and auditing

Expected preparation of the participant

The CompTIA SecAI+ course is designed for individuals who already have experience in IT and cybersecurity. Participants should be comfortable with system architecture concepts, log analysis, access control mechanisms, and foundational infrastructure protection techniques.
Practical familiarity with security environments such as SIEM platforms, EDR/XDR solutions, vulnerability assessment tools, and event monitoring systems is recommended. Participants do not need to be AI experts, but they should understand fundamental AI concepts.
Prior experience equivalent to Security+ certification or comparable hands-on information security practice is recommended.

Training Includes

- 5 days of instructor-led training
- Instructor supervision
- Community access
- Authorized courseware: CompTIA SecAI+
- Lab environment integrated with the course material
- Exam voucher: CY0-001

Language

- Training delivery: English
- Materials: English

Duration

5 days / 35 hours

Examination method

The exam can be taken at authorized Pearson VUE testing centers.
The exam voucher is not included in the course price.
Exam code: CY0-001
Number of questions: Maximum of 60 (multiple-choice and performance-based)
Scoring scale: 100–900
Passing score: 600
Format: Combination of multiple-choice and performance-based questions
Duration: 60 minutes