CompTIA SecAI+ Training Course

CompTIA SecAI+ is the first certification in our expansion series, designed to help you secure, govern and responsibly integrate artificial intelligence into your cybersecurity operations.

SEC-20F

Course Objectives

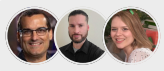
Professional, practical, & hands-on live instructor-led training

Start as a beginner and graduate as a certified professional, with the skills, experience, and job-search know how to get your career started.

Start Today

Potential Career Tracks

- AI Security Specialist
- SOC Analyst (AI-Enabled)
- AI Governance & Compliance Lead
- Machine Learning Security Engineer



Taught by Industry Veterans & Qualified Instructors

Introduction to CompTIA SecAI+

Course Overview

Intellectual Point's comprehensive CompTIA SecAI+ training program is designed to bridge the gap between cybersecurity and artificial intelligence. As the industry's first certification dedicated to securing AI systems and using AI for defense, this course prepares you for the challenges of the modern threat landscape.

Throughout the course, you'll explore critical topics such as Machine Learning (ML) security, protecting Large Language Models (LLMs), and implementing AI Governance, Risk, and Compliance (GRC). You will go beyond theory with hands-on labs that teach you to detect AI-specific threats (like prompt injection and model poisoning) and utilize AI tools to automate incident response. This training ensures you are not only prepared for the SecAI+ certification exam but also ready to secure the next generation of enterprise technology.

Obtainable Skills

- Securing AI/ML Systems
- Defending LLMs & Generative AI
- AI Governance & Compliance
- AI-Assisted Threat Detection
- Adversarial ML Defense
- Responsible AI Implementation

Course Insights

Audience Profile

This course is designed for cybersecurity professionals, security analysts, and engineers who are looking to specialize in the security of Artificial Intelligence. It is ideal for those who already hold foundational security knowledge (such as CompTIA Security+ or CySA+) and want to validate their ability to secure AI workloads and use AI tools for defense.

Whether you are a SOC analyst integrating AI tools, or a security architect designing defenses for ML models, this course provides the specialized skills required for the AI era.

Course Objectives

By the end of this course, participants should:

1. Implement controls to protect AI models, data pipelines, and infrastructure.
2. Identify and mitigate adversarial attacks like data poisoning and prompt injection.
3. Use AI-driven tools to enhance threat detection and automate security operations.
4. Apply frameworks (NIST AI RMF, EU AI Act) to ensure compliant and ethical AI use.
5. Fully prepare to take the CompTIA SecAI+ certification exam with confidence.

Module by Module Learning *Outline*

6 Modules

Module 1: AI Concepts for Cybersecurity

Learning Objectives:

- Understand the fundamental principles of Machine Learning (ML) and Generative AI.
- Identify the unique security challenges posed by AI supply chains and lifecycles.

Topics Covered

AI Fundamentals:

- LLMs, Neural Networks, and Deep Learning basics.

The AI Lifecycle:

- Data acquisition, training, fine-tuning, and inference.

AI vs. Traditional Software:

- Understanding non-deterministic behavior and new attack surfaces.

Module 2: Securing AI Systems & Infrastructures

Learning Objectives:

- Implement security controls for AI environments, including cloud and on-premise.
- Secure the data pipelines that feed AI models to prevent corruption.

Topics Covered

Platform Security:

- Securing MLOps pipelines and AI development environments.

Data Security:

- Data sanitization, privacy-preserving ML, and preventing data leakage.

Model Security:

- Protecting model weights and intellectual property.

Module 3: Defending Against AI-Specific Threats

Learning Objectives:

- Analyze and mitigate adversarial attacks targeting AI models.
- Understand vulnerabilities unique to Generative AI and LLMs.

Topics Covered

Adversarial Machine Learning:

- Evasion, extraction, and inference attacks.

Generative AI Attacks:

- Prompt injection, jailbreaking, and hallucinations.

Poisoning Attacks:

- Training data poisoning and model manipulation.

Module 4: AI-Assisted Security Operations

Learning Objectives:

- Utilize AI and ML tools to enhance defensive cybersecurity operations.
- Automate repetitive security tasks using AI-driven agents.

Topics Covered

AI for Defense:

- Enhancing SIEM/SOAR with AI anomaly detection.

Threat Intelligence:

- Using AI to analyze vast amounts of threat data.

Automated Response:

- AI-driven incident triage and remediation workflows.

Module 5: AI Governance, Risk, and Compliance (GRC)

Learning Objectives:

- Navigate the complex regulatory landscape of Artificial Intelligence.
- Develop organizational policies for responsible and ethical AI use.

Topics Covered

Compliance Frameworks:

- NIST AI RMF, ISO 42001, and the EU AI Act.

Risk Management:

- Assessing bias, fairness, and safety in AI models.

Privacy & Ethics:

- Managing data privacy and ethical considerations in AI deployment.

Module 6: Hands-On Lab and Certification Preparation

Learning Objectives:

- Apply theoretical knowledge in simulated AI attack and defense scenarios.
- Prepare effectively for the CompTIA SecAI+ certification exam.

Topics Covered

Real-World Simulations:

- Hands-on labs for prompt injection defense and secure model deployment.

Exam Preparation:

- Review of key exam domains, practice questions, and test-taking strategies.

Final Assessment:

- Mock exam to gauge readiness.