APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

CompTIA SecAI+ Training

CompTIA Authorized Training · Applied Technology Academy

CompTIA SecAI+ is the first certification in the new Expansion Series, designed to equip cybersecurity professionals with the skills to secure, govern, and responsibly integrate Artificial Intelligence into cybersecurity operations. The course focuses on defending AI systems, leveraging AI for threat detection and automation, navigating global GRC frameworks, and defending against AI-driven threats like adversarial attacks and malicious use of generative AI.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Advanced	**5 Days**	**3-4 years IT, incl. 2 years cybersecurity**	**$129,180**	**Yes**

Course Overview

CompTIA SecAI+ will be the first certification in our new expansion series, designed to help you secure, govern, and responsibly integrate artificial intelligence into cybersecurity operations. Gain the skills to defend AI systems, meet global compliance standards, and use AI to enhance threat detection, automation, and innovation while strengthening organizational resilience.

Course Outline

- **Module 1: Basic AI concepts related to cybersecurity**
  - Explain core AI principles and terminology: Machine learning, deep learning, natural language processing, and automation.
  - Identify AI applications in security: Use cases for AI in threat detection, defense, and security operations.
  - Recognize AI-driven threats: Automated phishing, polymorphic malware, adversarial machine learning, and malicious use of generative AI.
- **Module 2: Securing AI systems**
  - Implement security controls: Protect AI systems, data, and models using robust technical safeguards.
  - Secure AI deployment environments: Apply best practices across on-premises, cloud, and hybrid infrastructures.
  - Mitigate adversarial risks: Defend against attacks targeting AI models, data pipelines, and inference layers.
- **Module 3: AI-assisted security**
  - Enhance detection and response: Use AI-driven tools to identify anomalies, detect threats, and accelerate incident remediation.

  - Automate security workflows: Integrate AI for event triage, alert correlation, and response orchestration.
  - Apply AI techniques in operations: Incorporate AI into threat modeling,behavior analysis, and continuous monitoring.
- **Module 4: AI governance, risk, and compliance**
  - Understand regulatory frameworks: Identify global governance requirements and their implications for AI adoption.
  - Integrate GRC into AI projects: Incorporate governance, risk management,and compliance practices throughout the AI lifecycle.
  - Ensure responsible AI use: Apply ethical guidelines, legal standards, and industry frameworks such as GDPR and NIST AI RMF.

Intended Audience

- Cybersecurity Analysts
- Cybersecurity Engineers
- Information Security Analyst

Prerequisites

3–4 years in IT, inclusive of 2+ years hands-on cybersecurity; Security+, CySA+, PenTest+, or equivalent recommended.

Follow-On Courses

- ISACA Advanced in AI Security Management (AAISM)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.