

CompTIA SecAI+

Length: 5 days

Format: Classroom

Time: Day



About This Course

This course equips cybersecurity professionals with the practical skills needed to develop practical, job-ready skills for recognizing and responding to AI-driven threats, such as prompt injection, model abuse, data leakage, and adversarial attacks. They will be able to apply secure-by-design principles to AI use cases, policies, and workflows. SecAI+ also provides a verifiable way to demonstrate your skills to employers, helping you stand out in a competitive market. They signal a commitment to ongoing professional development and can support career advancement, role expansion, or salary growth over time.

This course covers the core domains tested on the SecAI+ exam: Basic AI Concepts Related to Cybersecurity, Securing AI Systems, AI-assisted Security and AI Governance, Risk, and Compliance. Participants will develop the knowledge and hands-on skills required to Understand important AI concepts, Secure AI systems using various technical controls, Leverage AI to enhance corporate security posture while automating security tasks, and Understand how governance, risk, and compliance (GRC) impacts AI technologies on a global scale.

By the end of the course, learners will be prepared to contribute to risk management, governance, and incident response activities involving AI.

[Click here to find your place on the CompTIA pathway.](#)

Required Exams

To earn the CompTIA SecAI+ certification, students must pass exam CY0—001.

Audience Profile

This course is ideal for those who currently hold a CompTIA cybersecurity certification (such as Security+, CySA+, PenTest+, etc.) or equivalent experience, and are looking to expand their skill set for evolving job roles in the context of AI technologies.

Course Objectives

After completing this course, students will be able to:

- * 1. Apply foundational and advanced AI concepts to strengthen organizational cybersecurity.
- * 2. Implement robust security controls and best practices for protecting AI systems and data.
- * 3. Leverage AI-driven tools to enhance threat detection, response, and automation of security operations.
- * 4. Navigate global governance, risk, and compliance.

Outline

- * Module 1: AI and Data Concepts for Cybersecurity
- * Module 2: Implementing Threat Modeling and Securing AI Systems
- * Module 3: Installing Access Controls for AI
- * Module 4: Distinguishing AI- Related Threats and Compensating Controls
- * Module 5: Leveraging AI in Security and Understanding Its Misuse
- * Module 6: Understanding AI Governance, Risk, and Compliance