CompTIA SecAI+

Course Duration: 5 Days
Exam Reference: CYO-001

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.

Prerequisites

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

Course Objectives

- Apply AI concepts to strengthen your organization's cybersecurity posture.
- Secure AI systems using advanced controls and protections to safeguard data, models, and infrastructure.
- Leverage AI technologies to automate workflows, accelerate incident response, and scale security operations.
- Navigate global GRC frameworks to ensure ethical and compliant AI adoption across industries.
- Defend against AI-driven threats like adversarial attacks, automated malware, and malicious use of generative AI.
- Integrate AI securely into DevSecOps pipelines and enterprise security strategies.

APPLIED TECHNOLOGY ACADEMY

Contact Us

☎ 800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

CompTIA SecAI+

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.