

CompTIA SecAI+ (CY0-001)

Course Overview

CompTIA SecAI+ is the first certification in CompTIA expansion series, designed to help you secure, govern and responsibly integrate artificial intelligence into your cybersecurity operations. You'll build the skills to defend AI systems, meet global compliance expectations and use AI to enhance threat detection, automation and innovation—so you can strengthen your expertise and help keep your organization's systems and data secure

Upon course completion, you will be able to:

- Understand fundamental cybersecurity concepts and best practices.
- Explain the role and application of artificial intelligence in security environments.
- Identify and mitigate common threats and vulnerabilities.
- Apply risk management techniques to real-world scenarios.
- Utilize security tools and technologies for threat detection and response.
- Interpret and analyze security data to inform decision-making.
- Communicate technical information clearly to both technical and non-technical audiences.

Skills you'll learn

- 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.

Course Prerequisites

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

Associated Certifications

SecAI+

Table of Contents

- 1.0 Summarizing AI and Data Concepts for Cybersecurity
 - 1.1 Explain AI Concepts for Cybersecurity
 - 1.2 Understand AI Model Training and Prompt Engineering
 - 1.3 Secure AI Data

- 2.0 Implementing Threat Modeling and Securing AI Systems
 - 2.1 Use AI Threat Modeling
 - 2.2 Implement Security Controls for AI Systems

- 3.0 Installing Access Controls for AI
 - 3.1 Deploy Access Controls for AI
 - 3.2 Apply Data Security Controls for AI Security
 - 3.3 Perform Monitoring and Auditing for AI Systems

- 4.0 Distinguishing AI-Related Threats and Compensating Controls
 - 4.1 Demonstrate the Importance of Security in the AI Life Cycle
 - 4.2 Analyze AI System Attacks and Utilize Compensating Controls

- 5.0 Leveraging AI in Security and Understanding Its Misuse
 - 5.1 Use AI-Enabled Tools for Security Tasks
 - 5.2 Summarize AI-Enabled and AI-Enhanced Attack Vectors
 - 5.3 Use AI to Automate Security Tasks

- 6.0 Understanding AI Governance, Risk, and Compliance
 - 6.1 Classify Organizational Governance Structures for AI
 - 6.2 Define the Risks Associated with AI
 - 6.3 Explain the Impact of Compliance on Business Use and Development of AI