CompTIA SecAI+ Course Outline

EXAM NUMBER: CY0-001

Course Overview

- Develop practical skills for securing, governing, and responsibly integrating artificial intelligence into cybersecurity operations.
- Learn how AI supports threat detection, workflow automation, incident response, and enterprise security strategy.
- Prepare for AI security risks such as prompt injection, adversarial attacks, data poisoning, automated malware, and malicious use of generative AI.
- Build a foundation for evaluating AI-enabled tools, securing AI system components, and applying risk management throughout the AI lifecycle.

Exam Details

- Exam version: V1.
- Number of questions: Maximum of 60, including multiple-choice and performance-based questions.
- Duration: 60 minutes.
- Passing score: 600 on a scale of 100-900.
- Recommended experience: 3-4 years in IT, including 2+ years of hands-on cybersecurity experience.

Students Will Learn To

- Explain basic AI concepts and how they apply to modern cybersecurity environments.
- Secure AI systems, models, data, prompts, APIs, integrations, and supporting infrastructure.
- Use AI-assisted security tools to improve monitoring, detection, triage, and incident response.
- Apply governance, risk, compliance, and responsible AI practices in enterprise environments.

Basic AI Concepts Related to Cybersecurity (17%)

- Explain core AI principles and terminology, including machine learning, deep learning, natural language processing, and automation.
- Identify cybersecurity use cases for AI in threat detection, defense, and security operations.
- Recognize AI-driven threats such as automated phishing, polymorphic malware, adversarial machine learning, and malicious use of generative AI.

Securing AI Systems (40%)

- Implement security controls to protect AI systems, data, models, and infrastructure.
- Secure AI deployment environments across on-premises, cloud, and hybrid infrastructures.
- Protect model inputs, outputs, prompts, APIs, pipelines, training data, and inference layers.
- Mitigate adversarial risks that target AI models, data pipelines, and deployment environments.

AI-assisted Security (24%)

- Use AI-driven tools to identify anomalies, detect threats, and support incident remediation.
- Automate security workflows such as event triage, alert correlation, and response orchestration.
- Apply AI techniques in threat modeling, behavior analysis, continuous monitoring, and security operations.

AI Governance, Risk, and Compliance (19%)

- Identify global governance requirements and compliance considerations for AI adoption.
- Integrate governance, risk management, and compliance practices throughout the AI lifecycle.
- Apply responsible AI practices, ethical guidelines, legal standards, and frameworks such as GDPR and NIST AI RMF.