Course Content

Course Description:

CompTIA SecAI+ is the IT industry's first comprehensive certification focused on securing artificial intelligence systems and applying AI responsibly within cybersecurity operations. It equips learners with the skills to understand, defend, and ethically deploy AI technologies across modern enterprises. The course covers AI concepts, threat modeling, secure AI system design, governance, risk, compliance, and the use of AI-enabled tools in security operations. Learners gain hands-on experience with prompt engineering, adversarial testing, model security controls, and AI-driven automation.

This course supports preparation for the CompTIA SecAI+ (CY0-001) certification exam.

Course Objectives:

- Apply foundational and advanced AI concepts to strengthen cybersecurity posture.
- Implement security controls for AI systems, including model guardrails, access controls, and data protections.
- Perform AI-specific threat modeling and analyze AI-related attack vectors.
- Use AI-enabled tools to enhance detection, analysis, automation, and incident response.
- Identify and mitigate risks associated with AI misuse, bias, adversarial attacks, and data leakage.
- Navigate AI governance, risk, and compliance frameworks to support responsible AI adoption.
- Evaluate AI system integrity and conduct monitoring, auditing, and post-incident analysis.
- Prepare for the SecAI+ certification exam through structured practice and applied labs.

Prerequisites:

- 3–4 years of IT experience, including approximately 2 years of hands-on cybersecurity experience (recommended).
- Familiarity with security fundamentals, networking, and basic AI/ML concepts is helpful.
- Ideal for learners who already hold certifications such as Security+, CySA+, or PenTest+.

CompTIA: SecAI+ Certification

Course ID #: 7000-1154-ZZ-Z

Hours: 35

Target Audience:
- Cybersecurity analysts and engineers
- SOC teams and incident responders
- IT practitioners expanding into AI-integrated environments
- Governance, risk, and compliance professionals
- Technology leaders evaluating AI capabilities and vulnerabilities
- Anyone responsible for securing, deploying, or managing AI systems

Topics:

Lesson 1: Summarizing AI and Data Concepts for Cybersecurity
- Explain AI concepts for cybersecurity
- Core AI types; Generative AI; ML and statistical learning; Transformers; NLP
- Detect suspicious activity using ML
- Live Lab: Explore the SecAI+ Lab Environment
- Understand AI model training and prompt engineering
- Supervised, unsupervised, reinforcement, and federated learning
- Prompt engineering fundamentals; system roles; zero-shot/one-shot/multi-shot prompting
- Live Lab: Prompt engineering, bias detection, design, and optimization
- Secure AI data
- AI data types; data security considerations; RAG solutions
- Data handling techniques; integrity verification
- Module Quiz

Lesson 2: Implementing Threat Modeling and Securing AI Systems
- Use AI threat modeling
- AI threat resources; prerequisites; modeling processes; frameworks
- Live Labs: Analyze threats; apply frameworks; deploy Azure OpenAI LLM
- Implement security controls for AI systems
- Model-specific controls; guardrails; prompt templates
- Gateway/interface controls; quota limitations; testing controls
- Live Labs: Structured prompt templates; secure Azure OpenAI LLM
- Module Quiz

Lesson 3: Installing Access Controls for AI
- Deploy access controls for AI
- Access control principles; AI access control models; model access; agent/data access
- Network/API access; threat landscape
- Apply data security controls
- Encryption; data safety measures; masking/anonymization
- Live Lab: Sanitize data for AI analysis
- Perform monitoring and auditing
- Prompt/log monitoring; performance/cost monitoring; compliance auditing
- Live Lab: Analyze logs with AI
- Module Quiz

Lesson 4: Distinguishing AI-Related Threats and Compensating Controls
- Demonstrate the importance of security in the AI lifecycle
- Lifecycle stages; data security; human factors; ethics
- Analyze AI system attacks and compensating controls
- Backdoor/Trojan attacks; poisoning; inversion; theft
- Compensating controls; post-incident analysis
- Live Lab: Test prompt injection attacks
- Module Quiz

Lesson 5: Leveraging AI in Security and Understanding Its Misuse
- Use AI-enabled tools for security tasks
- Vulnerability analysis; detection/analysis; pattern recognition; incident management
- Summarize AI-enabled and AI-enhanced attack vectors
- Deepfakes; reconnaissance; automated attacks; AI-assisted vector identification
- Use AI to automate security tasks
- Scripting; summarization; workflow automation; DevSecOps
- Live Labs: Accelerate scripting; transform documentation; automate workflows
- Module Quiz

Lesson 6: Understanding AI Governance, Risk, and Compliance
- Classify organizational governance structures
- Governance roles; structures; design activities
- Define risks associated with AI
- Responsible AI principles; unique AI risks; risk assessment
- Explain compliance impacts
- AI regulations; compliance frameworks; organizational policies; external impacts
- Module Quiz

Appendix A: SecAI+ (CY0-001) Practice Exams
- Why certification matters
- Exam details and preparation guidance
- Practice Exams:
- AI Concepts & Cybersecurity
- Securing AI Systems
- AI-Assisted Security
- AI Governance, Risk & Compliance
- Full Practice Test

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535

CompTIA: SecAI+ Certification

Course ID #: 7000-1154-ZZ-Z

Hours: 35

NASBA Information

Level: Intermediate

Attendance Requirement: To be awarded the full credit hours, you must sign in and attend the entire course.

Fields: Computer Software & Applications

CPEs: 39

Policies: Course Registration, Cancellation, Refund and Complaint Resolution

For more information regarding administrative policies such as complaint and refund, please contact our offices at 800-639-3535 or visit us at: **www.tcworkshop.com**

Official National Registry Statement:

The Computer Workshop is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

NOTE: Since our information is in multiple places on our web site or in PDF format that is sent to clients, we have provided our normal course content with the NASBA Information added along with links to our policy page on the web. We will add our name to the Official National Registry Statement after we are approved.