CompTIA SecAI+ (CY0-001)

Duration 5 Days

COURSE DESCRIPTION

CompTIA SecAI+ enables a safer digital future by empowering IT and cybersecurity talent worldwide to meet the emerging challenges and opportunities at the intersection of AI and security.

CompTIA SecAI+ is the global IT industry's first comprehensive "expansion" certification focused on the security of artificial intelligence systems and the secure application of AI in cybersecurity operations. This certification equips professionals with critical, vendor-neutral skills to understand, defend, and ethically deploy AI technologies within any organization.

COURSE OBJECTIVES

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

COURSE OUTLINE

Module 1 — AI and Data Concepts for Cybersecurity

- AI concepts and core AI types
- Generative AI and transformers
- Machine learning and deep learning
- Natural language processing
- AI model training approaches
- Prompt engineering fundamentals
- Model security considerations
- AI data types and data security techniques
- RAG (Retrieval Augmented Generation) concepts
- Data integrity and processing controls

Module 2 — Threat Modeling and Securing AI Systems

- AI threat modeling fundamentals
- Threat modeling processes and prerequisites
- AI threat modeling frameworks
- AI security control types
- Model guardrails and prompt templates
- Gateway and interface controls
- Usage quotas and limitation controls
- Security control testing

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

Module 3 — Access Controls for AI

- AI access control principles and models
- Model and agent access controls
- API and network access security
- AI data security controls
- Encryption and data safety measures
- Monitoring and logging AI systems
- Performance and cost monitoring
- AI auditing and compliance monitoring

Module 4 — AI Threats and Compensating Controls

- AI lifecycle security
- Ethical AI design considerations
- AI attack types and techniques
- Backdoor and trojan model attacks
- Model poisoning and inversion
- Model theft risks
- Compensating control strategies
- Post-incident AI analysis

Module 5 — Leveraging AI in Security Operations

- AI-enabled security tools
- AI use cases in detection and analysis
- AI for vulnerability assessment
- AI-enhanced attack vectors
- AI for social engineering and deception
- AI reconnaissance techniques
- AI-driven automation
- AI in DevSecOps workflows
- AI scripting and summarization

Module 6 — AI Governance, Risk, and Compliance

- AI governance structures
- AI organizational roles
- Responsible AI principles
- AI risk identification and assessment
- AI regulatory themes
- Compliance frameworks for AI
- Organizational AI policy design
- Compliance reporting

WHO SHOULD ATTEND

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.

PREREQUISITES

This is equivalent to 3–4 years of IT experience with approximately 2 years of hands-on cybersecurity experience.

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th