# CompTIA SecAI+ Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

## Overview

**CompTIA SecAI+** is a comprehensive three-day instructor-led course designed for IT and**Cyber Security Professionals** who want to develop expertise in **Artificial Intelligence Security (AI Security)**. As a vendor-neutral certification, it helps organizations address emerging security challenges associated with AI adoption while maximizing the benefits of AI technologies.

Participants gain practical knowledge of **Machine Learning**, **Deep Learning**, **Generative AI**, and modern security methodologies. The course focuses on protecting **AI Models**, data pipelines, and deployment environments while leveraging AI-driven technologies to improve **Threat Detection**, **Incident Response**, and overall **Security Operations**.

## Prerequisites

- 3-4 years of IT experience
- Approximately 2 years of hands-on **Cyber Security** experience
- **CompTIA Security+** or equivalent knowledge recommended

## Who Should Attend

This course is ideal for:

- **Cyber Security Analysts**
- **Security Engineers**
- **Security Operations Center (SOC) Professionals**
- **Threat Intelligence Analysts**
- **DevSecOps Engineers**
- Software Developers
- **Security Architects**
- IT professionals working with **AI Systems**

## What You Will Learn

After completing this course, participants will be able to:

- Apply **Artificial Intelligence** concepts within cyber security environments.
- Implement effective **AI Security Controls**.
- Identify and mitigate **AI Threats** and vulnerabilities.
- Use AI-powered solutions for **Threat Detection** and response.
- Securely integrate AI into **DevSecOps** and enterprise architectures.
- Apply **Risk Management**, **Compliance**, and **AI Governance** frameworks.

# CompTIA SecAI+ Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

## Outline

### Module 1: AI and Data Foundations for Cyber Security

- **Machine Learning** and **Deep Learning** concepts
- **Generative AI** technologies
- Transformer architectures and **Natural Language Processing (NLP)**
- AI model training methodologies
- **Prompt Engineering** techniques
- Data integrity and protection controls
- **Retrieval-Augmented Generation (RAG)** fundamentals

### Module 2: Threat Modelling and Securing AI Systems

- **Threat Modelling** frameworks
- AI attack surfaces and vulnerabilities
- Implementation of **AI Security Controls**
- Secure configuration and guardrails
- Validation and testing of security measures

### Module 3: Access Control for AI Systems

- **Access Control** models
- API and network security
- **Data Protection** and encryption strategies
- Monitoring and logging practices
- Compliance and auditing procedures

### Module 4: AI Threats and Defensive Controls

- **Adversarial AI** attacks
- **Model Poisoning** techniques
- Model theft and inversion threats
- Ethical AI development principles
- Mitigation and compensating controls
- Post-incident investigation and analysis

### Module 5: Leveraging AI in Security Operations

- AI-powered **Threat Detection**
- Security analytics and assessment
- AI-driven vulnerability management
- Security automation workflows
- **Incident Response** optimization
- **DevSecOps** integration practices

### Module 6: AI Governance, Risk Management and Compliance

- **AI Governance** frameworks
- Organizational roles and responsibilities
- Responsible AI principles
- **Risk Management** methodologies

# CompTIA SecAI+ Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

- Regulatory and **Compliance** requirements
- Policy development and reporting mechanisms