INFOSECTRAIN
Educate. Excel. Empower.

AI Powered Course

CompTIA®

SecAI+

Certification Training

INFOSECTRAIN

Course Highlights

- **40-Hour** Instructor-Led Training
- Aligned with Official **CompTIA SecAI+** (v1) Exam Objectives
- Focus on Real-world AI Threats, Attacks, and Defenses
- Exam-Oriented Training with Scenario-Based Discussions
- Highly Interactive, Case-Driven Sessions
- Telegram Support Group for Exam Preparation
- Learn from Experienced AI & Security Practitioners
- Extended Post Training Support
- Access to Recorded Sessions

About Course

The CompTIA SecAI+ (v1) Certification Course from InfosecTrain equips cybersecurity professionals with the knowledge required to secure AI-enabled systems and defend against AI-driven threats. The course begins with basic AI concepts related to cybersecurity (17%), ensuring learners understand machine learning, deep learning, natural language processing, and automation, strictly from a security and risk perspective, not model development.

The core of the program focuses on securing AI systems (40%), including protection of AI models, training data, inference pipelines, and deployment environments across cloud, on-premises, and hybrid infrastructures. Learners explore defenses against adversarial machine learning, data poisoning, and model exploitation attacks. The training then covers AI-assisted security (24%), demonstrating how AI can enhance threat detection, automate security workflows, improve incident response, and support continuous monitoring within SOC and security operations.

Finally, the course addresses AI governance, risk, and compliance (19%), enabling professionals to understand global regulatory expectations, integrate GRC practices into AI initiatives, and ensure responsible and ethical use of AI, aligned with frameworks such as GDPR and NIST AI Risk Management Framework (AI RMF).

Course Objectives

Upon successful completion of the training, participants will be able to:

- Explain core AI concepts and terminology relevant to cybersecurity
- Identify AI applications used in threat detection and security operations
- Recognize AI-driven threats, including adversarial and generative AI misuse
- Implement security controls to protect AI systems, data, and models
- Secure AI deployment environments across cloud, on-prem, and hybrid platforms
- Mitigate adversarial risks targeting AI pipelines and inference layers
- Apply AI-assisted techniques to improve detection, response, and monitoring
- Automate security workflows using AI-enabled tools
- Integrate governance, risk, and compliance into AI initiatives
- Ensure responsible, ethical, and compliant use of AI technologies
- Prepare confidently for the CompTIA SecAI+ (v1) certification exam

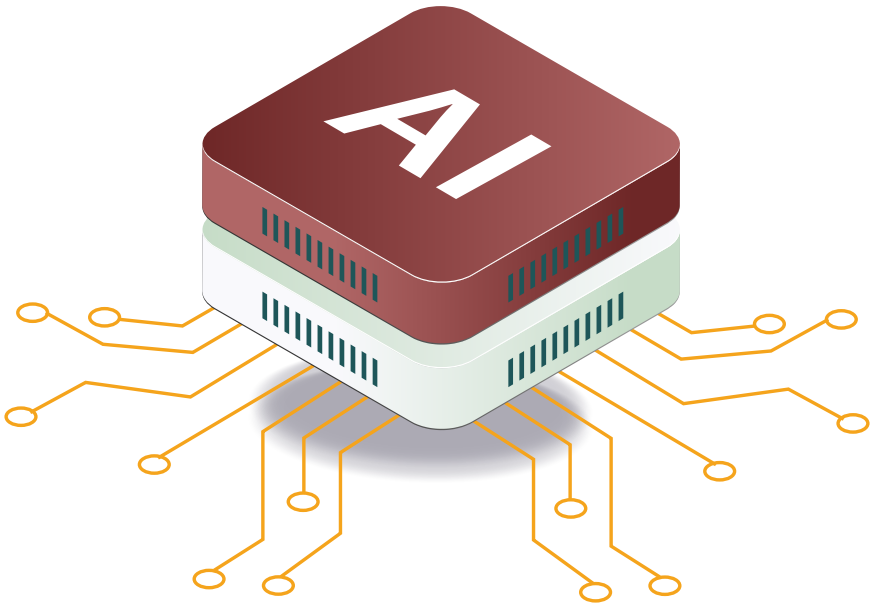
INFOSECTRAIN

Target Audience

- Cybersecurity Analysts & Engineers
- SOC Analysts & Incident Responders
- Security Architects & Consultants
- Risk, GRC, and Compliance Professionals
- Cloud Security Professionals
- Security Leaders responsible for AI adoption
- Professionals securing AI-enabled systems

Pre-Requisites

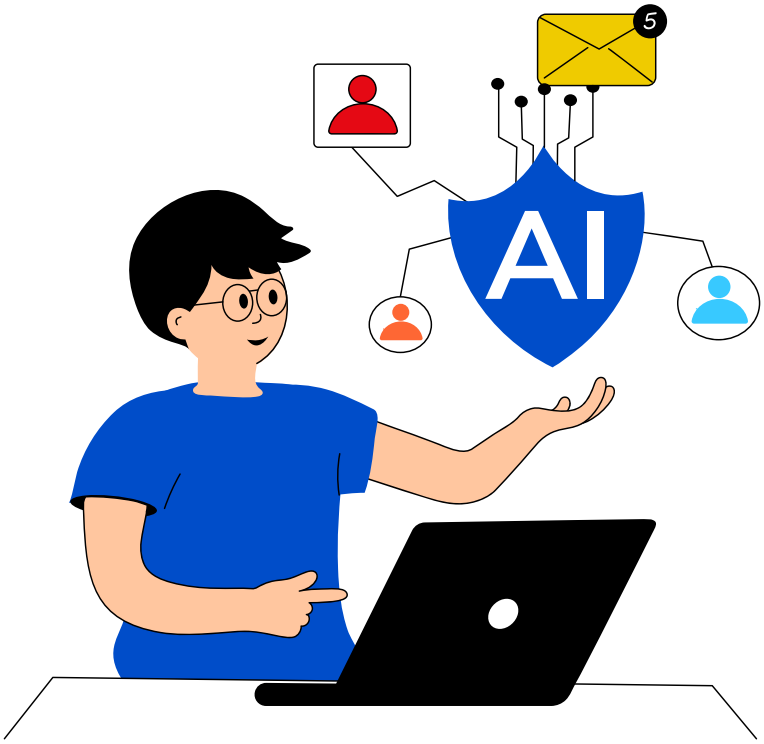
It is recommended to have 3–4 years experience in IT, inclusive of 2+ years hands-on cybersecurity; Security+, CySA+, PenTest+, or equivalent discipline.



INFOSECTRAIN

Exam Details

Exam Code	CY0-001
Launch Date	February 17, 2026
Number of Questions	60
Exam Pattern	Multiple-Choice and Performance-Based
Exam Duration	60 Minutes
Passing Score	600 (on a Scale of 100–900)
Exam language	English



INFOSECTRAIN

Course Content

Basic AI concepts related to cybersecurity (17%)

- Explain core AI principles and terminology: Machine learning, deep learning, natural language processing, and automation.
- Identify AI applications in security: Use cases for AI in threat detection, defense, and security operations.
- Recognize AI-driven threats: Automated phishing, polymorphic malware, adversarial machine learning, and malicious use of generative AI.

Securing AI systems (40%)

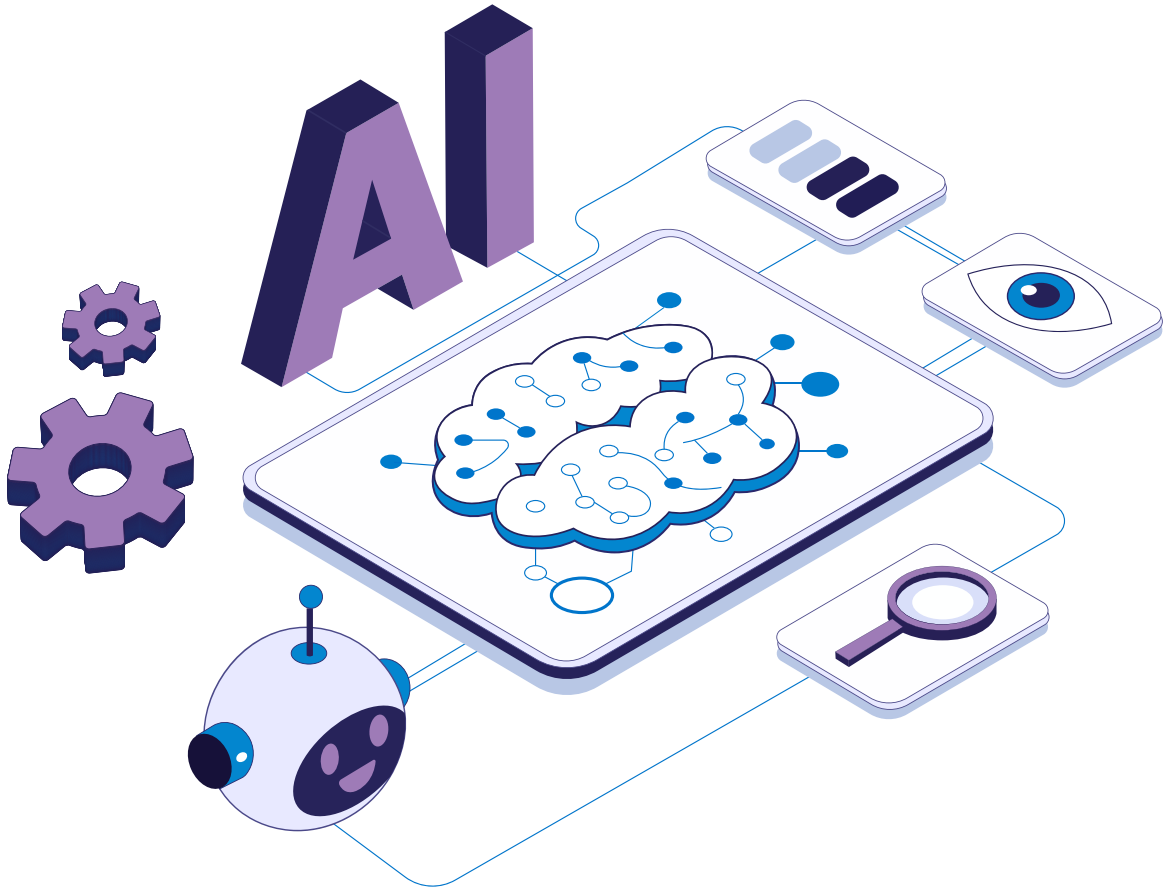
- Implement security controls: Protect AI systems, data, and models using robust technical safeguards.
- Secure AI deployment environments: Apply best practices across on-premises, cloud, and hybrid infrastructures.
- Mitigate adversarial risks: Defend against attacks targeting AI models, data pipelines, and inference layers.

AI-assisted security (24%)

- Enhance detection and response: Use AI-driven tools to identify anomalies, detect threats, and accelerate incident remediation.
- Automate security workflows: Integrate AI for event triage, alert correlation, and response orchestration.
- Apply AI techniques in operations: Incorporate AI into threat modeling, behavior analysis, and continuous monitoring.

AI governance, risk, and compliance (19%)

- Understand regulatory frameworks: Identify global governance requirements and their implications for AI adoption.
- Integrate GRC into AI projects: Incorporate governance, risk management, and compliance practices throughout the AI lifecycle.
- Ensure responsible AI use: Apply ethical guidelines, legal standards, and industry frameworks such as GDPR and NIST AI RMF.



INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on