

SecAI+ is CompTIA's newest expansion certification—a first-to-market opportunity in the emerging AI security credential space with comprehensive learning products and instructor resources.

The aligned SecAI+ CertMaster learning products—CertMaster Perform, CertMaster Labs, and CertMaster Study—offer a rich blend of content, with a strong emphasis on practical, hands-on learning.

Course Modules

1. Summarizing AI and Data Concepts for Cybersecurity
2. Implementing Threat Modeling and Securing AI Systems
3. Installing Access Controls for AI
4. Distinguishing AI-Related Threats and Compensating Controls
5. Leveraging AI in Security and Understanding Its Misuse
6. Understanding AI Governance, Risk, and Compliance

Scope

- Duration: 5 days
- Format: Lecture and hands-on labs
- Exam: CY0-001

Prerequisites

3–4 years in IT, inclusive of 2+ years hands-on cybersecurity; Security+, CySA+, PenTest+, or equivalent recommended.

Objectives

- Apply AI concepts to strengthen your organization's cybersecurity posture.
- Secure AI systems using advanced controls and protections to safeguard data, models, and infrastructure.
- Leverage AI technologies to automate workflows, accelerate incident response, and scale security operations.
- Navigate global GRC frameworks to ensure ethical and compliant AI adoption across industries.
- Defend against AI-driven threats like adversarial attacks, automated malware, and malicious use of generative AI.
- Integrate AI securely into DevSecOps pipelines and enterprise security strategies.

Target Audience

Training providers, bootcamps, corporate training departments, and learning delivery organizations serving IT and cybersecurity professionals seeking AI security skills.