

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- **We do not teach the test.** Extended hours of immersive, hands-on work
- All reading material and study guides sent to you when you register
- Every course taught by working security practitioners

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- CompTIA Security+, CySA+ or PenTest+, or equivalent knowledge
- Comfortable with network and host security controls, logging and incident response
- No machine-learning background is assumed — the AI is taught from the security side
- CompTIA recommends three to four years in IT with two hands-on in security — a recommendation, not a bar to entry

TARGET AUDIENCE

- Security analysts and engineers whose organisation has started deploying AI systems
- SOC analysts using AI-assisted tooling who need to know when to trust it
- Security architects and risk staff answering questions about AI governance
- Service members, veterans and military spouses using AF COOL, Army CA, MyCAA or VET TEC 2.0

EXAM

CY0-001 — CompTIA SecAI+

60 questions, 60 minutes, pass 600 of 900.

CompTIA SecAI+ was released on **17 February 2026**. It is vendor-neutral, so what students learn applies whichever models and platforms their employer has adopted.

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **CompTIA SecAI+** certification. As with all our CompTIA training experiences, the exam is delivered in the classroom.

SecAI+ is for the security professional whose organisation has already deployed AI. It runs in both directions: securing AI systems against prompt injection, model abuse, data leakage and adversarial attack, and using AI properly as a security tool — including knowing when its output cannot be trusted.

The course maps to exam **CY0-001**, with objective coverage marked throughout. No machine-learning background is assumed; the AI is taught from the security side, for people who already know how to defend a network.

WHAT YOU WILL BE ABLE TO DO

- Threat-model an AI system and apply controls that fit how it actually fails
- Recognise and defend against prompt injection, model abuse and training-data attacks
- Use AI-assisted tooling in detection and response, and know when to override it
- Answer the governance, risk and compliance questions an AI deployment provokes

COURSE OBJECTIVES

Primary course objectives:

- Explain the AI and data concepts a security practitioner actually needs
- Threat-model AI systems and the pipelines that feed them
- Secure models, training data, inference endpoints and the supply chain around them
- Defend against prompt injection, jailbreaks, model extraction and data poisoning
- Use AI to accelerate detection, triage and response — and verify what it produces
- Recognise adversarial use of AI: automated phishing, deepfakes and accelerated tooling
- Apply AI governance frameworks, and evidence compliance to an auditor

EXCLUSIVE LEARNING PACKAGE

- AI security lab environment you keep after the camp
- Prompt-injection and model-abuse exercise set
- SecAI+ video course
- AI governance and risk templates
- SecAI+ reading plan and review guide
- SecAI+ certification practice exam

COURSE MODULES

- 01 Basic AI Concepts for Cybersecurity 17%**

 - Topic A: Models, training, inference and where the data comes from
 - Topic B: The AI attack surface, in security terms
 - Topic C: Vocabulary that matters in an incident
 - Topic D: Limits, hallucination and why output needs verifying
- 02 Securing AI Systems 40%**

 - Topic A: Threat modelling an AI deployment
 - Topic B: Prompt injection, jailbreaks and output handling
 - Topic C: Training-data poisoning and model integrity
 - Topic D: Model extraction, inversion and leakage of sensitive data
 - Topic E: Access control, isolation and secrets for AI workloads
 - Topic F: Supply chain: third-party models, plugins and agents
 - Topic G: Logging, monitoring and detection for AI systems
- 03 AI-Assisted Security 24%**

 - Topic A: AI in detection, triage and alert reduction
 - Topic B: Automating investigation and response safely
 - Topic C: Verifying AI output before acting on it
 - Topic D: Adversarial use: phishing, deepfakes and accelerated attack tooling
- 04 AI Governance, Risk and Compliance 19%**

 - Topic A: AI governance frameworks and acceptable-use policy
 - Topic B: Risk assessment for an AI deployment
 - Topic C: Privacy, data residency and regulatory exposure
 - Topic D: Audit evidence, documentation and model inventory

WHAT IT COSTS, WHAT IS INCLUDED

Training camp, five days	\$2,850
CompTIA SecAI+ exam voucher (CY0-001)	\$273
Exam sat in the classroom on the final day	included
Retakes of any part of the course for 24 months	included
Six months mentoring with our engineers	included

WAYS TO PAY

- **AF COOL** — Air Force and Space Force enlisted
- **Army Credentialing Assistance** — enlisted and warrant officers
- **MyCAA** — military spouses
- **VET TEC 2.0** — veterans and separating service members
- **thinQflex™** — name your own price, paid over twelve months

WHERE IT RUNS

- **Sterling, VA** — 21481 Ridgetop Cir
- **Atlanta, GA** — 431 Marietta St NW
- **Burbank, CA** — 3301 N San Fernando Blvd
- Five days, Monday to Friday. Also delivered live-online and on-site.

TERMS



© 2026 thinQtank® Global, Inc. All rights reserved. The product or learning service names referenced are trademarks of their respective owners. CompTIA and SecAI+ are trademarks of CompTIA, Inc.

thinQtank Global, Inc. warrants that it will perform these training services in a professional and workmanlike manner, by qualified personnel. Course content is subject to change to reflect vendor updates to the certification.