

CompTIA SecAI+ (CY0-001) Exam Prep

CompTIA SecAI+ CY0-001. AI security, risk management, and scenario-based exam practice.

[IT Certifications](#) Instructor: Brian Taylor • 5 sections • 45 lessons • 14.50h total

[View this course online](#) [Browse all courses](#)

About this course

Preparing for the CompTIA SecurityAI+ (CY0-001) exam can feel overwhelming given the mix of AI concepts and security protocols. This course connects studying theory to passing the test by focusing on the practical application of the exam objectives. We will walk through the key domains, breaking down complex topics into manageable lessons.

You will learn how to tackle the toughest exam sections with a focus on real scenarios. We provide guidance on interpreting questions, applying risk management frameworks, and understanding AI security nuances. The course includes timed practice tests and a detailed question bank.

Course curriculum

Foundations and Exam Strategy

- **Understanding the CY0-001 Exam Blueprint (12m)**
We'll break down the official exam domains, weightings, and question formats to build your study roadmap.
- **Setting Up Your Study Environment (8m)**
Learn how to organize your resources and set up a distraction-free workspace for effective study sessions.
- **Key Terminology: AI vs. Machine Learning in Security (18m)**
A clear breakdown of the essential vocabulary you must know to decode exam questions correctly.
- **How to Read and Deconstruct Exam Questions (15m)**
A practical guide to spotting keywords, eliminating distractors, and identifying the 'best' answer in scenario-based questions.
- **Time Management Strategies for the Test (11m)**
Techniques for pacing yourself during the exam to ensure you have time for every question.
- **Downloadable: SecAI+ Study Checklist (7m)**
Get a step-by-step checklist to track your progress through the official exam objectives.
- **Common Pitfalls and Myths About SecAI+ (14m)**
We debunk common misconceptions and highlight topics that students often underestimate.

Core Concepts: Governance, Risk, and Compliance

- **Applying AI Risk Management Frameworks (22m)**
Walk through how to apply NIST AI RMF and other frameworks in real-world scenarios.
- **Data Governance for AI Systems (19m)**
Learn the critical data privacy and integrity concepts required for the exam.
- **Compliance Standards in an AI-Driven World (25m)**
A deep dive into GDPR, HIPAA, and other regulations as they apply to AI security.
- **Identifying and Mitigating AI Supply Chain Risks (16m)**
A problem-solving session on securing third-party AI models and datasets.
- **The Shared Responsibility Model for AI (12m)**
Clarifying who is responsible for security in cloud-based AI services.
- **Case Study: Regulatory Failure in a FinTech App (28m)**
Analyze a real-world case where poor AI governance led to compliance violations.
- **Quiz: Governance and Risk Scenarios (13m)**
Test your knowledge with 15 scenario-based questions focused on this domain.
- **Mapping Policies to Security Controls (17m)**
How to translate high-level security policies into actionable technical controls for AI.
- **Ethical Considerations and Security Bias (21m)**
Understanding how bias in AI models creates security vulnerabilities.

Deep Dive: AI System Security and Threats

- **Anatomy of an Adversarial AI Attack (24m)**
We'll dissect how attackers manipulate AI inputs (data poisoning, evasion) and how to spot them.
- **Securing Large Language Models (LLMs) (26m)**
A focused lesson on prompt injection, data leakage, and securing generative AI.
- **Traditional Security vs. AI Security: Key Differences (15m)**
Highlighting where standard cybersecurity practices fail and AI-specific defenses are needed.
- **Threat Modeling for AI Applications (23m)**
A step-by-step guide to mapping threats specific to machine learning pipelines.
- **Zero Trust Principles Applied to AI (19m)**
How to implement 'never trust, always verify' for AI model access and data feeds.
- **Hardening AI Infrastructure (20m)**
Practical steps for securing the compute and storage environments running your AI.
- **Real Case Study: The Model Inversion Breach (31m)**
Analyzing a historical attack where sensitive training data was extracted from a model.
- **Practice Drill: Identifying Attack Vectors (12m)**
An interactive drill to test your ability to identify weaknesses in a given AI architecture.

Advanced Application: Monitoring and Incident Response

- **Implementing MLOps Security Monitoring (22m)**
How to set up logging and alerting specifically for machine learning operations.
- **Detecting Model Drift and Performance Degradation (18m)**
Learn to distinguish between natural model drift and malicious manipulation.
- **The Incident Response Playbook for AI Attacks (27m)**
A detailed walkthrough of the steps to take when an AI model is compromised.
- **Forensics for AI Systems (25m)**
Techniques for investigating an AI security incident and determining the root cause.
- **Automating Security Response with AI (20m)**
Using AI to defend AI, use cases for automated threat containment.
- **Setting Up Canary Deployments for Models (16m)**
A practical guide to safely rolling out model updates to detect issues early.
- **Handling False Positives in AI Security Alerts (14m)**
Strategies for tuning your monitoring systems to reduce alert fatigue.
- **Quiz: Operations and Response (15m)**
A set of questions focused on incident handling and monitoring scenarios.
- **Building a Robust AI Incident Response Team (19m)**
Defining roles and responsibilities for handling AI-specific security events.
- **Downloadable: AI Incident Response Template (9m)**
A fill-in-the-blanks template for documenting and responding to AI threats.

Full Practice Exams and Final Review

- **Timed Practice Test 1: Domains 1 & 2 (35m)**
A full-length, timed simulation covering Governance and Risk, with immediate feedback.
- **Deep Dive Review: Practice Test 1 Missed Questions (28m)**
We go through every missed question from Test 1, explaining the logic behind the correct answers.
- **Timed Practice Test 2: Domains 3 & 4 (32m)**
A focused exam on Security Engineering and Monitoring, designed to test your technical knowledge.
- **Deep Dive Review: Practice Test 2 Missed Questions (26m)**
A detailed breakdown of the technical concepts tested in Practice Test 2.
- **Timed Practice Test 3: Full Exam Simulation (40m)**
A comprehensive mock exam that replicates the pressure and format of the real CY0-001 test.
- **Final Review: Full Exam Score Analysis (32m)**
A personalized guide on how to interpret your score and which areas to focus on in your final 48 hours.
- **The Ultimate 48-Hour Cram Strategy (15m)**
A highly focused study plan for the two days leading up to your exam.
- **Last-Minute Checklist: Before You Click 'Start' (8m)**
A quick review of technical requirements, ID checks, and mental prep for exam day.
- **Question Bank Walkthrough: Hard Questions (29m)**
We tackle the 10 hardest practice questions and explain the 'trick' in each one.
- **What to Expect After the Exam (10m)**
Understanding the scoring process, getting your results, and next steps for certification maintenance.
- **Congratulations and Next Steps (6m)**
A wrap-up message and advice on leveraging your new SecAI+ certification in your career.

Discover our blog

Learn more with free articles written by our professors and guest experts.

Latest article: **Flight Attendant Preparation: What to Study Before You Apply**

[Visit the blog](#) [All courses](#) [This course](#)