SecAI+ Training and Certification

Note: SecAI+ is a newly announced certification from CompTIA. The official exam (CY0-001) is scheduled to launch on February 17, 2026.

Course Description & Overview

SecureNinja’s CompTIA Security+ AI (SecAI+) certification training provides a comprehensive introduction to the intersection of artificial intelligence and cybersecurity. Designed to equip learners with both foundational and advanced knowledge, this course explores how AI and machine learning models are applied in security operations, threat analysis, and defensive strategies. As organizations rapidly adopt AI-driven technologies, SecAI+ ensures learners are prepared to understand and mitigate associated risks in real-world environments.

This vendor-neutral training covers secure AI implementation, data governance, model evaluation, risk management, and emerging compliance requirements. Students will learn how to assess AI system integrity, understand attack vectors targeting AI models, and apply principles of responsible AI use. SecureNinja's expert instructors break down this emerging field into manageable, engaging segments with practical context, making complex AI security concepts accessible to those with security or IT backgrounds.

Why Choose CompTIA SecAI+

- Emerging Credential: One of the first certifications focused specifically on secure AI practices in cybersecurity.
- High Relevance: Aligns with real-world needs in threat detection, data protection, and AI risk analysis.
- Career-Boosting: Enhances credentials for SOC analysts, compliance specialists, data security professionals, and aspiring AI security experts.
- Vendor-Neutral: Covers AI security concepts that apply across different tools, vendors, and ecosystems.

Topics Covered

- AI & ML Foundations: Core concepts in artificial intelligence and machine learning relevant to security operations.
- AI in Cybersecurity: Use of AI for threat detection, response, and automation in SOC environments.
- Model Governance & Risk: Secure design, model evaluation, and attack mitigation strategies.
- Compliance & Ethics: Responsible AI use, fairness, bias mitigation, and global regulatory trends.
- Security of AI Systems: Threats targeting machine learning pipelines and defenses against adversarial inputs.

Who is it for

- Cybersecurity Analysts: Professionals looking to upskill in AI-related security

practices.
- IT Practitioners: Individuals with networking, systems, or cloud experience expanding into AI-integrated environments.
- Data Analysts: Those seeking to understand the security implications of AI use and deployment.
- Compliance and Risk Specialists: Personnel managing AI risk, bias, governance, or regulatory concerns.

Who Would Benefit

- Security Engineers: Needing a framework to evaluate AI tools and integrate them into secure environments.
- SOC Teams: Analysts seeking a deeper understanding of how AI affects security monitoring and response.
- Technology Decision-Makers: CISOs, security architects, and team leads evaluating AI capabilities and vulnerabilities.

Prerequisites

There are no formal prerequisites, but it is recommended that learners have foundational knowledge in cybersecurity such as CompTIA Security+, and a basic understanding of IT concepts and terminology.

Course Outline

1. Domain 1: AI Fundamentals

   - Understanding AI and machine learning types, processes, and terminology.
   - Use cases and application of AI in cybersecurity.

2. Domain 2: Secure AI Systems

   - Designing AI systems with security in mind.
   - Recognizing risks and attack surfaces specific to ML models.

3. Domain 3: Threats and Vulnerabilities

   - Exploring adversarial attacks, poisoning, and data manipulation.
   - Understanding common vulnerabilities in AI workflows.

4. Domain 4: AI Security Operations

   - AI-enhanced threat detection and threat intelligence integration.
   - Automated security responses and SOC integration.

5. Domain 5: Governance, Risk, and Compliance

   - Establishing AI policy, governance frameworks, and ethical guidelines.
   - Addressing AI compliance standards and documentation.

Course Length

- 5 Days
- 40 Hours

Exam Details

- Exam Code: CY0-001
- Number of Questions: Maximum of 90
- Question Types: Multiple-choice and performance-based
- Duration: 90 minutes
- Passing Score: 700 (on a scale of 100 to 900)

The CompTIA SecAI+ certification is ideal for learners looking to stay ahead in the fast-moving world of AI-driven security. With real-world use cases and instruction from seasoned security experts, SecureNinja’s course ensures you’re prepared to meet the future of AI-driven cybersecurity head-on.