

Where AI and Cybersecurity Converge: Introducing CompTIA SecAI+

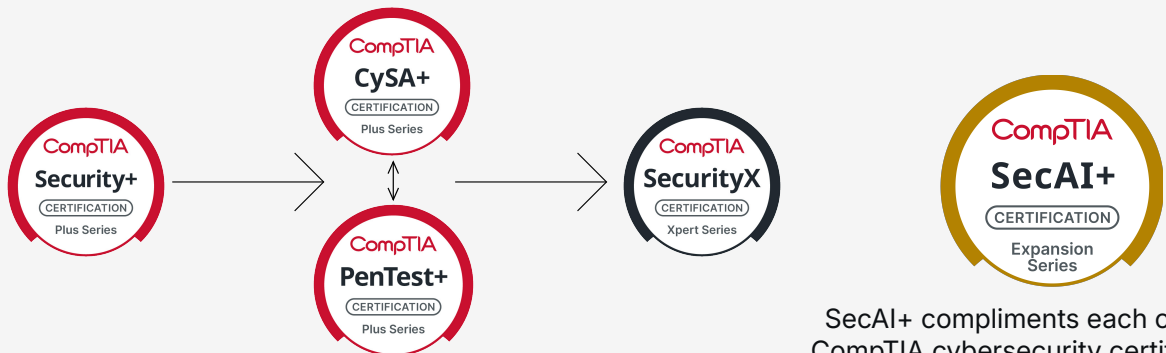
CompTIA's first Expansion Series certification addresses skills to defend against and leverage AI technologies in modern cybersecurity environments



AI security knowledge now is essential for cybersecurity professionals

CompTIA SecAI+ is designed to help you secure, govern and responsibly integrate artificial intelligence into your cybersecurity operations. You'll build the skills to defend AI systems, meet global compliance expectations and use AI to enhance threat detection, automation and innovation, so you can strengthen your expertise and help keep your organization's systems and data secure.

CompTIA Cyber Pathway



SecAI+ compliments each of these
CompTIA cybersecurity certifications

Skills You'll Learn

- 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.

Exam Objectives

- Basic AI concepts related to cybersecurity (17%)
- Securing AI systems (40%)
- AI-assisted security (24%)
- AI governance, risk, and compliance (19%)

Recommended Experience

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



Where AI and Cybersecurity Converge: Introducing CompTIA SecAI+

CompTIA's first Expansion Series certification addresses skills to defend against and leverage AI technologies in modern cybersecurity environments

SecAI+ is designed to complement, and elevate, professionals in roles such as:

Job Role	Job Task	Job Task
Security Analyst / SOC Analyst	Use AI-powered tools for threat hunting, anomaly detection and incident triage	Automate routine analysis so you can focus on higher-value investigations
Cybersecurity Engineer / Security Architect	Design and secure AI-integrated systems and architectures	Implement technical controls around AI models, APIs and data flows
Penetration Tester / Security Consultant	Assess AI systems and AI-enabled defenses for vulnerabilities	Model and test adversarial AI threats and AI-assisted attack techniques
Cloud Engineer / DevSecOps / CI/CD Engineer	Secure AI workloads in cloud and containerized environments	Integrate AI security checks into DevOps pipelines and automated testing
Risk, Compliance & Governance Professionals	Map AI systems to global regulations and frameworks (e.g., NIST AI RMF, GDPR)	Build and enforce AI governance and risk management policies

How SecAI+ Keeps You Competitive

Stay Ahead of AI-Driven Threats

Attackers are already using AI for automated phishing, polymorphic malware, deepfakes and more. SecAI+ helps you understand these threats and build proactive defenses.

Align with Where the Industry Is Going

Most organizations are already deploying AI for monitoring and defense. Cyber professionals who understand AI will be better positioned for promotions and strategic roles.

Use AI to Work Smarter, Not Just Harder

Learn how to safely use generative AI and AI-powered tools for tasks like log analysis, vulnerability triage, threat modeling and ticketing, boosting your productivity and impact.

Signal Commitment to Continuous Learning

Earning SecAI+ shows employers you're serious about staying current as the industry evolves, an important signal when promotions, raises and leadership roles are on the line.