CompTIA SecAI+ Course Outline

ERIC REED

CYBERSECURITY TRAINING

PASS ON THE FIRST ATTEMPT!™

COMPANY OVERVIEW

For over 25 years, Eric Reed Cybersecurity Training has been a trusted leader in cybersecurity education, equipping more than 60,000 professionals with the skills needed to defend against emerging cyber threats. Our mission is to empower individuals and organizations with comprehensive, hands-on training that translates directly to real-world success. Recognized with multiple industry awards—including an unprecedented 10-time EC Council Instructor of the Year and 7-time Circle of Excellence honoree—we combine innovative delivery methods with a passion for excellence to ensure our students achieve certification success on the first attempt

COMPTIA SECAI+

CompTIA SecAI+ is the first certification in our new expansion series, designed to help you secure, govern, and responsibly integrate artificial intelligence into cybersecurity operations. Gain the skills to defend AI systems, meet global compliance standards, and use AI to enhance threat detection, automation, and innovation while strengthening organizational resilience. CompTIA SecAI+ is scheduled to launch on February 17, 2026, and is now available for pre-order.

COURSE 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.

SALARY RANGE

SecAI+ → $120,000

These figures are approximate and depend on location, experience, and job role. Higher salaries are usually seen in major tech hubs and with significant experience.

JOB ROLES

- Cybersecurity Analyst
- SOC (Security Operations Center) Analyst
- Security Engineer
- Security Architect
- Threat Intelligence Analyst
- Incident Responder
- Cloud Security Engineer
- DevSecOps Engineer
- AI/ML Engineer (working with secure AI systems)
- GRC (Governance, Risk, and Compliance) Analyst

WWW.LINKEDIN.COM/IN/ERICREEDLIVE/

ONLINE LIVE LEARNING

ON-DEMAND LIVE LEARNING

ONLINE LIVE & ON-DEMAND LIVE

All the benefits of live, instructor-led training with the convenience of on-demand.

- **Online Live:** Attend our scheduled sessions in real time (Monday–Friday). Get immediate interaction with the instructor and fellow students.
- **On-Demand Live:** Access recordings of the most recent live sessions on your own schedule, while still having direct instructor support.
- **Flexible Scheduling:** Choose a structured approach—one-week bootcamp (M–F), two nights a week for five weeks, or every Saturday for five weeks. Need more wiggle room? Adjust any schedule to fit your lifestyle!

Contact Us

(707) 722-7333

info@ericreedlive.com

1401 61st St S
Gulfport, FL 33707

CompTIA SecAI+ Course Outline

COMPTIA SECAI+ OVERVIEW

Module 1: Basic AI concepts related to cybersecurity

- Explain core AI principles and terminology: Machine learning, deep learning, natural language processing, and automation.
- Identify AI applications in security: Use cases for AI in threat detection, defense, and security operations.
- Recognize AI-driven threats: Automated phishing, polymorphic malware, adversarial machine learning, and malicious use of generative AI.

Module 2: Securing AI systems

- Implement security controls: Protect AI systems, data, and models using robust technical safeguards.
- Secure AI deployment environments: Apply best practices across on-premises, cloud, and hybrid infrastructures.
- Mitigate adversarial risks: Defend against attacks targeting AI models, data pipelines, and inference layers.

Module 3: AI-assisted security

- Enhance detection and response: Use AI-driven tools to identify anomalies, detect threats, and accelerate incident remediation.
- Automate security workflows: Integrate AI for event triage, alert correlation, and response orchestration.
- Apply AI techniques in operations: Incorporate AI into threat modeling, behavior analysis, and continuous monitoring.

Module 4: AI governance, risk, and compliance

- Understand regulatory frameworks: Identify global governance requirements and their implications for AI adoption.
- Integrate GRC into AI projects: Incorporate governance, risk management,and compliance practices throughout the AI lifecycle.
- Ensure responsible AI use: Apply ethical guidelines, legal standards, and industry frameworks such as GDPR and NIST AI RMF.

★★★★★

“It’s was a great class that covered all aspects of security. Most importantly, I appreciate the fact that you are giving up your own time to assist us and maintain a sharedrive with the latest security tools and informative papers even after the class is over. I was able to pass the test after one week of attending the training.”

-Shadi Ehalabi