Training: CompTIA
CompTIA SecAI+ Prep Course

TRAINING GOALS:

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.

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.

Job roles that benefit from SecAI+ skills

- Security Analyst – Turn AI into an ally for threat detection and incident response, using it to surface patterns, model attacker behavior and act on threats more quickly.
- Cloud Engineer – Confidently design and maintain cloud environments that host AI workloads and data, with controls that support both security and compliance.
- SOC Analyst – Strengthen day-to-day operations in the SOC by using AI to flag anomalies, reduce alert fatigue and streamline how security events are handled.
- Penetration Tester / Security Consultant – Add AI systems to your testing playbook, evaluating models and data pipelines for unique vulnerabilities and providing clearer risk guidance to stakeholders.
- Senior Systems Administrator – Support AI projects running on the infrastructure you manage by understanding their governance, risk and compliance needs.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Data Scientist / ML Engineer – Build and deploy models with stronger protections around training data, pipelines and outputs, while collaborating more smoothly with security teams.
- DevSecOps / CI/CD Engineer – Extend existing DevOps practices with AI-aware security checks and automated tests that run before code or models reach production.
- Risk & Compliance Officer – Apply frameworks like GDPR and NIST AI RMF to real AI use cases, helping your organization meet legal and regulatory expectations.
- Military Cyber Operations Specialist – Defend mission-critical AI and ML systems and better understand how adversaries might use AI in contested environments.

Each participant in an authorized training CompTIA SecAI+ Prep Course held in Compendium CE will receive a free CY0-001 CompTIA SecAI+ Certification Exam vouchers.

CONSPECT:

- Summarizing AI and Data Concepts for Cybersecurity
  - Explain AI Concepts for Cybersecurity
    - Core AI Types
    - Types of AI
    - Generative AI
    - Machine Learning and Statistical Learning
    - Detect Suspicious Activity using ML
    - Activity: Comparing AI Types
    - Transformers
    - Deep Learning
    - Natural Language Processing
    - Live Lab: Explore the SecAI+ Lab Environment
  - Understand AI Model Training and Prompt Engineering
    - AI Model Training
    - Supervised Learning
    - Unsupervised Learning
    - Reinforcement Learning
    - Federated Learning
    - Model Training Techniques
    - Introduction to Prompt Engineering
    - Activity: Prompt Engineering

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Live Lab: Perform Prompt Engineering and Bias Detection
- System Roles and System Prompts
- User Prompts
- Zero-Shot, One-Shot, Multi-Shot, and Templates
- Securing the Model
- Live Lab: Prompt Design and Optimization

- Secure AI Data
  - Data Security Related to AI
  - Data Security Considerations for AI
  - AI Data Types
  - Live Lab: Examine RAG Solutions
  - Data Handling Techniques
  - Activity: Processing Data
  - Live Lab: Verify Data Integrity

- Implementing Threat Modeling and Securing AI Systems
  - Use AI Threat Modeling
    - Introduction to AI Threat Modeling
    - AI Threat Modeling
    - Utilizing AI Threat Resources
    - Live Lab: Analyze Threats using Public Resources
    - Prerequisites for Performing AI Threat Modeling
    - Process of AI Threat Modeling
    - Activity: Threat Model Analysis
    - AI Threat Modeling Frameworks
    - Live Lab: Apply a Threat Modeling Framework to AI
    - Live Lab: Create and Deploy an Azure OpenAI LLM
  - Implement Security Controls for AI Systems
    - Overview of AI Security Controls
    - Model Specific Controls
    - Model Guardrails
    - Prompt Template
    - Gateway and Interface Controls
    - Gateway Controls and Guardrails
    - Usage and Quota Limitations
    - Testing Security Controls
    - Activity: Defensive Policy Builder

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Live Lab: Apply Structured Prompt Templates
- Live Lab: Secure an Azure OpenAI LLM

- Installing Access Controls for AI
  - Deploy Access Controls for AI
    - Access Control Principles for AI
    - AI Access Control Models
    - Activity: Deploy an Access Request
    - Threat Landscape of AI Systems
    - Model Access
    - Access Control for AI Systems
    - Data and Agent Access
    - Network and API Access
  - Apply Data Security Controls for AI Security
    - Overview of AI Data Security Controls
    - Encryption of AI Data
    - Data Safety Measures
    - Activity: Data Masking/Anonymization
    - Live Lab: Sanitize Data for AI Analysis
  - Perform Monitoring and Auditing for AI Systems
    - Prompt and Log Monitoring
    - Performance and Cost Monitoring
    - AI Cost Monitoring
    - Quality and Compliance Auditing
    - Activity: Audit the AI
    - Live Lab: Analyze Logs with AI
- Distinguishing AI-Related Threats and Compensating Controls
  - Demonstrate the Importance of Security in the AI Life Cycle
    - Exploring the AI Life Cycle
    - Activity: Classify AI Life Cycle for a Use Case
    - Data Security Considerations
    - AI Life Cycle Security Considerations
    - The Human Role in AI Security
    - Ethical Considerations in AI Design
  - Analyze AI System Attacks and Utilize Compensating Controls
    - Analyzing AI Attacks
    - Backdoor and Trojan Attacks

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Model and Data Poisoning
- Model Inversion and Model Theft
- Activity: Model Inversion or Theft
- AI Attacks Analysis and Controls
- Applying Compensating Controls
- Activity: Conduct a Post-Incident Analysis
- Live Lab: Test Prompt Injection Attacks

- Leveraging AI in Security and Understanding Its Misuse
  - Use AI-Enabled Tools for Security Tasks
    - AI Tools in Security Operations
    - Activity: Perform AI-Assisted Vulnerability Analysis
    - AI Use Cases: Detection and Analysis
    - Activity: Use Case: Pattern Recognition
    - AI Security Use Cases
    - AI Use Cases: Testing and Management
    - AI and Incident Management
  - Summarize AI-Enabled and AI-Enhanced Attack Vectors
    - AI for Deception and Social Engineering
    - Activity: Identify a Deepfake
    - AI for Reconnaissance and Data Correlation
    - AI for Automated Attacks
    - AI Attack Vectors
    - Live Lab: Explore AI-Assisted Attack Vector Identification
  - Use AI to Automate Security Tasks
    - AI for Security Scripting and Content Summarization
    - Live Lab: Accelerate Scripting with AI
    - Live Lab: Transform Documentation into Insights with AI
    - AI in Security Workflows
    - Automate Security Tasks
    - Activity: AI Assisted Approval
    - AI in DevSecOps
    - Live Lab: Automate Workflows with AI
- Understanding AI Governance, Risk, and Compliance
  - Classify Organizational Governance Structures for AI
    - Establish AI Governance
    - Important Roles in AI

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- AI Governance
- Activity: Designing an AI Governance Structure

- Define the Risks Associated with AI
  - Principles of Responsible AI
  - Identifying Risks Unique to AI
  - Putting Principles into Practice
  - Common AI Risks
  - Discuss Risks with AI
  - Activity: Conduct a Risk Assessment
- Explain the Impact of Compliance on Business Use and Development of AI
  - Common Themes in AI Regulation
  - Important AI Compliance Frameworks
  - Organizational AI Policies
  - Activity: Create a Compliance Report
  - External Compliance Impacts
  - Activity: Analyze an Organization's AI Structure

REQUIREMENTS:

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

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the CompTIA SecAI+ certification exam, which is available through the Pearson VUE test centers.

Each participant in an authorized training CompTIA SecAI+ Prep Course held in Compendium CE will receive a free CY0-001 CompTIA SecAI+ Certification Exam vouchers.

TRAINER:

Authorized CompTIA Trainer

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007