

uCertify

Course Outline

CompTIA SecAI+



16 May 2026

1. Pre-Assessment
2. Exercises, Quizzes, Flashcards & Glossary
 - Number of Questions
3. Expert Instructor-Led Training
4. ADA Compliant & JAWS Compatible Platform
5. State of the Art Educator Tools
6. Award Winning Learning Platform (LMS)
7. Chapter & Lessons
 - Syllabus
 - Chapter 1: Preface
 - Chapter 2: The Convergence of Artificial Intelligence and Cybersecurity
 - Chapter 3: Data Science and Feature Engineering for Security
 - Chapter 4: Threat Modeling and Vulnerability Frameworks for AI
 - Chapter 5: Attack Vectors and Adversarial Engineering
 - Chapter 6: Security Engineering for AI Systems
 - Chapter 7: Governance, Risk, and Compliance for AI
 - Chapter 8: AI Application Security and Agent Architectures
 - Chapter 9: Synthetic Media, Deepfakes, and Multimedia Security
 - Chapter 10: Future Trends and Emerging AI Threats
 - Chapter 11: End-to-End Secure AI Implementation
 - Chapter 12: AI Security Operations and Incident Response
 - Chapter 13: Enterprise AI Strategy and Leadership
- Videos and How To
8. Practice Test
 - Here's what you get
 - Features
9. Live labs
 - Lab Tasks

Here's what you get

10. Post-Assessment

1. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

2. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

311
EXERCISES

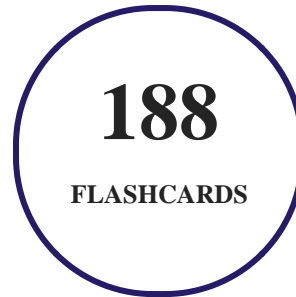
3. Quiz

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

184
QUIZ

4. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.



5. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.



6. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

7. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

8. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

9. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
 1. Best Postsecondary Learning Solution
- **2015**
 1. Best Education Solution

2. Best Virtual Learning Solution
3. Best Student Assessment Solution
4. Best Postsecondary Learning Solution
5. Best Career and Workforce Readiness Solution
6. Best Instructional Solution in Other Curriculum Areas
7. Best Corporate Learning/Workforce Development Solution

- **2016**

1. Best Virtual Learning Solution
2. Best Education Cloud-based Solution
3. Best College and Career Readiness Solution
4. Best Corporate / Workforce Learning Solution
5. Best Postsecondary Learning Content Solution
6. Best Postsecondary LMS or Learning Platform
7. Best Learning Relationship Management Solution

- **2017**

1. Best Overall Education Solution
2. Best Student Assessment Solution
3. Best Corporate/Workforce Learning Solution
4. Best Higher Education LMS or Learning Platform

- **2018**

1. Best Higher Education LMS or Learning Platform
2. Best Instructional Solution in Other Curriculum Areas
3. Best Learning Relationship Management Solution

- **2019**

1. Best Virtual Learning Solution
2. Best Content Authoring Development or Curation Solution
3. Best Higher Education Learning Management Solution (LMS)

- **2020**

1. Best College and Career Readiness Solution
2. Best Cross-Curricular Solution
3. Best Virtual Learning Solution

10. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Preface

- How to Use This Course
- Prerequisites and Expectations
- A Note on the Industry

Chapter 2: The Convergence of Artificial Intelligence and Cybersecurity

- Core Concepts of Artificial Intelligence
- The Dual Reality of AI in Security
- AI Paradigms for Security Professionals

- Modern AI Architectures and Security Implications
- The AI Development Lifecycle (Model Development Lifecycle – MDLC)
- Hands-On Practice: Establishing the AI Security Lab
- Summary and Exam Essentials

Chapter 3: Data Science and Feature Engineering for Security

- Data Security Foundations and the AI Lifecycle
- Deep Learning Architectures and Component Analysis
- Data as the New Attack Surface
- Secure Retrieval-Augmented Generation (RAG) Architectures
- Building a Secure Data Pipeline
- Summary and Exam Essentials

Chapter 4: Threat Modeling and Vulnerability Frameworks for AI

- The Necessity of Structured Risk Assessment
- Thinking Like an AI Adversary
- The OWASP Top 10 for Large Language Models
- The MITRE ATLAS Framework

- Applying STRIDE to AI Workflows
- Conducting an AI Threat Modeling Workshop
- Summary and Exam Essentials

Chapter 5: Attack Vectors and Adversarial Engineering

- Introduction to Adversarial Machine Learning
- Gradient-Based Evasion Attacks
- Black-Box Attacks and Oracle Abuse
- Data Poisoning and Backdoor Attacks
- Privacy Attacks
- Generative AI Attacks
- Advanced Threats: Manipulation, Theft, and Overreliance
- Adversarial Networks and AI-Enhanced Attacks
- Summary and Exam Essentials

Chapter 6: Security Engineering for AI Systems

- Adversarial Training and Model Hardening
- Input Guardrails and Sanitization
- Access Control for AI Systems

- Secure MLOps
- Privacy-Preserving Machine Learning (PPML)
- Watermarking and Detection
- Continuous Monitoring and AI Observability
- Prompt Monitoring and Log Protection
- Summary and Exam Essentials

Chapter 7: Governance, Risk, and Compliance for AI

- Introduction to AI Governance and Regulation
- Explainability and Interpretability
- Fairness, Bias, and Ethics in AI
- AI Auditing and Documentation Standards
- The Role of the Human in the Loop (HITL)
- AI Incident Response and Forensics
- Summary and Exam Essentials

Chapter 8: AI Application Security and Agent Architectures

- Introduction to Agents and RAG Workflows

- Secure Prompt Engineering and System Prompts
- Sandboxing and Isolation for AI Agents
- Identity Management and Authorization for AI Agents
- Red Teaming and Adversarial Testing for Agents
- AI Tooling Interfaces Used by Security Teams
- Secure Deployment Strategies for AI Systems
- Summary and Exam Essentials

Chapter 9: Synthetic Media, Deepfakes, and Multimedia Security

- Foundations of Generative AI: GANs and Diffusion Models
- Audio Synthesis and Voice Cloning
- Multimedia Content Provenance and Watermarking
- Adversarial Attacks on Multimedia Systems
- Deepfake Detection Technologies and Forensics
- Ethical and Legal Implications of Synthetic Media
- Summary and Exam Essentials

Chapter 10: Future Trends and Emerging AI Threats

- Introduction to Quantum Computing and AI

- Quantum Machine Learning and Adversarial Intelligence
- Autonomous Agents and Swarm Intelligence Security
- Neuromorphic Computing and Spiking Neural Networks
- AI Governance and the Future of Work
- AI in Defense and Kinetic Operations
- Summary and Exam Essentials

Chapter 11: End-to-End Secure AI Implementation

- Project Scope and Architecture Design
- Data Pipeline and Vector Database Implementation
- Model Hardening and Guardrail Integration
- Red Teaming and Adversarial Simulation
- Deployment, Monitoring, and Incident Response
- Personal Assistants in Security Operations
- System Cards, Documentation, and Executive Reporting
- Summary and Exam Essentials

Chapter 12: AI Security Operations and Incident Response

- Designing the AI Security Operations Center (AISOC)
- AI Incident Response and Forensics
- AI Vulnerability Management and Model Remediation
- Adversarial Machine Learning Defense Strategies
- AI Supply Chain Security and SBOMs
- Continuous Security Monitoring and Compliance
- AI-Related Roles and Accountability in Security Programs
- Responsible AI as a Security Discipline
- Summary and Exam Essentials

Chapter 13: Enterprise AI Strategy and Leadership

- Developing an AI Security Strategy
- Regulatory Compliance and Legal Frameworks
- Ethics, Bias Mitigation, and Fairness Engineering
- AI Workforce Security and Culture
- Future-Proofing
- Third-Party Risk Management (TPRM) and AI Procurement
- Summary and Exam Essentials

Videos and How To

uCertify course includes videos to help understand concepts. It also includes How Tos that help learners in accomplishing certain tasks.

49

VIDEOS

05:43

HOURS

11. Practice Test

Here's what you get

60

PRE-ASSESSMENTS
QUESTIONS

2

FULL LENGTH TESTS

60

POST-ASSESSMENTS
QUESTIONS

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

12. Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

Lab Tasks

The Convergence of Artificial Intelligence and Cybersecurity

- Interacting with a Pre-Trained ML Model
- Running Local Inference with Ollama

Data Science and Feature Engineering for Security

- Implementing Cryptographic Data Provenance
- Architecting and Inspecting a Convolutional Neural Network (CNN)
- Transforming Logs into Numeric Features

- Performing a Dataset Poisoning Attack
- Configuring a Secure RAG Vector Store
- Implementing LBAC Metadata Tagging in a Secure RAG Pipeline

Attack Vectors and Adversarial Engineering

- Executing an FGSM Attack
- Executing a Black-Box Attack Using the HopSkipJump Method
- Injecting a Backdoor into an ML Model
- Simulating a Membership Inference Attack
- Experimenting with a Prompt Injection Attack

Security Engineering for AI Systems

- Building a Semantic Guardrail
- Training a Neural Network with DP
- Implementing a Text Watermark
- Building a Drift Detector
- Implementing Adversarial Training

Governance, Risk, and Compliance for AI

- Explaining a Model with SHAP
- Mitigating Bias Using Fairlearn
- Simulating an Active Learning Loop
- Analyzing a Data Poisoning Incident

AI Application Security and Agent Architectures

- Implementing a Secure RAG Retrieval Process
- Exploring Zero-Shot, One-Shot, and Few-Shot Prompting
- Simulating Token-Based Tool Access

Synthetic Media, Deepfakes, and Multimedia Security

- Visualizing the Forward Diffusion Process

Future Trends and Emerging AI Threats

- Building a Quantum-Inspired Classifier

End-to-End Secure AI Implementation

- Chunking Strategies for AI Systems
- Mitigating Model Poisoning Attacks on Vector Embeddings
- Executing a Red Team Campaign

AI Security Operations and Incident Response

- Building a Low-Code SOAR Automation Playbook
- Capturing Forensic Snapshots of AI Incidents
- Building a Security Regression Pipeline

Enterprise AI Strategy and Leadership

- Developing an Acceptable Use Policy (AUP)

Here's what you get

34

LIVE LABS

33

VIDEO TUTORIALS

01:19

HOURS

13. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

You can't stay away! Get



3187 Independence Drive
Livermore, CA 94551,
United States



+1-415-763-6300



support@ucertify.com



www.ucertify.com