

uCertify

Course Outline

Adversarial AI Attacks, Mitigations, and Defense Strategies



16 May 2026

1. Exercises, Quizzes, Flashcards & Glossary

Number of Questions

2. Expert Instructor-Led Training

3. ADA Compliant & JAWS Compatible Platform

4. State of the Art Educator Tools

5. Award Winning Learning Platform (LMS)

6. Chapter & Lessons

Syllabus

Chapter 1: Preface

Chapter 2: Getting Started with AI

Chapter 3: Building Our Adversarial Playground

Chapter 4: Security and Adversarial AI

Chapter 5: Poisoning Attacks

Chapter 6: Model Tampering with Trojan Horses and Model Reprogramming

Chapter 7: Supply Chain Attacks and Adversarial AI

Chapter 8: Evasion Attacks against Deployed AI

Chapter 9: Privacy Attacks – Stealing Models

Chapter 10: Privacy Attacks – Stealing Data

Chapter 11: Privacy-Preserving AI

Chapter 12: Generative AI – A New Frontier

Chapter 13: Weaponizing GANs for Deepfakes and Adversarial Attacks

Chapter 14: LLM Foundations for Adversarial AI

Chapter 15: Adversarial Attacks with Prompts

Chapter 16: Poisoning Attacks and LLMs

Chapter 17: Advanced Generative AI Scenarios

Chapter 18: Secure by Design and Trustworthy AI

Chapter 19: AI Security with MLSecOps

Chapter 20: Maturing AI Security

Videos and How To

7. Live labs

Lab Tasks

Here's what you get

1.  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.

60
EXERCISES

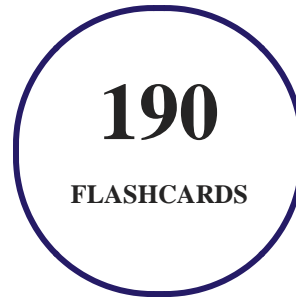
2.  Quiz

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.

200
QUIZ

3.  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.



4. 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.



5. 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.

6. 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.

7. 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.

8. 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

9. 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

- Who this course is for
- What this course covers
- To get the most out of this course

Chapter 2: Getting Started with AI

- Understanding AI and ML
- Types of ML and the ML life cycle
- Key algorithms in ML

- Neural networks and deep learning
- ML development tools
- Summary

Chapter 3: Building Our Adversarial Playground

- Technical requirements
- Setting up your development environment
- Hands-on basic baseline ML
- Developing our target AI service with CNNs
- ML development at scale
- Summary

Chapter 4: Security and Adversarial AI

- Technical requirements
- Security fundamentals
- Securing our adversarial playground
- Securing code and artifacts
- Bypassing security with adversarial AI

- Summary

Chapter 5: Poisoning Attacks

- Basics of poisoning attacks
- Staging a simple poisoning attack
- Backdoor poisoning attacks
- Hidden-trigger backdoor attacks
- Clean-label attacks
- Advanced poisoning attacks
- Mitigations and defenses
- Summary

Chapter 6: Model Tampering with Trojan Horses and Model Reprogramming

- Injecting backdoors using pickle serialization
- Injecting Trojan horses with Keras Lambda layers
- Trojan horses with custom layers
- Neural payload injection
- Attacking edge AI
- Model hijacking

- Summary

Chapter 7: Supply Chain Attacks and Adversarial AI

- Traditional supply chain risks and AI
- AI supply chain risks
- Data poisoning
- AI/ML SBOMs
- Summary

Chapter 8: Evasion Attacks against Deployed AI

- Fundamentals of evasion attacks
- Perturbations and image evasion attack techniques
- NLP evasion attacks with BERT using TextAttack
- Universal Adversarial Perturbations (UAPs)
- Black-box attacks with transferability
- Defending against evasion attacks
- Summary

Chapter 9: Privacy Attacks – Stealing Models

- Understanding privacy attacks
- Stealing models with model extraction attacks
- Defenses and mitigations
- Summary

Chapter 10: Privacy Attacks – Stealing Data

- Understanding model inversion attacks
- Types of model inversion attacks
- Example model inversion attack
- Understanding inference attacks
- Attribute inference attacks
- Example attribute inference attack
- Membership inference attacks
- Summary

Chapter 11: Privacy-Preserving AI

- Privacy-preserving ML and AI
- Simple data anonymization

- Advanced anonymization
- Differential privacy (DP)
- Federated learning (FL)
- Split learning
- Advanced encryption options for privacy-preserving ML
- Advanced ML encryption techniques in practice
- Applying privacy-preserving ML techniques
- Summary

Chapter 12: Generative AI – A New Frontier

- A brief introduction to generative AI
- Using GANs
- Using pre-trained GANs
- Summary

Chapter 13: Weaponizing GANs for Deepfakes and Adversarial Attacks

- Use of GANs for deepfakes and deepfake detection
- Using GANs in cyberattacks and offensive security
- Defenses and mitigations

- Summary

Chapter 14: LLM Foundations for Adversarial AI

- A brief introduction to LLMs
- Developing AI applications with LLMs
- Hello LLM with Python
- Hello LLM with LangChain
- Bringing your own data
- How LLMs change Adversarial AI
- Summary

Chapter 15: Adversarial Attacks with Prompts

- Adversarial inputs and prompt injection
- Direct prompt injection
- Automated gradient-based prompt injection
- Risks from bringing your own data
- Indirect prompt injection
- Data exfiltration with prompt injection

- Privilege escalation with prompt injection
- RCE with prompt injection
- Defenses and mitigations
- Summary

Chapter 16: Poisoning Attacks and LLMs

- Poisoning embeddings in RAG
- Poisoning attacks on fine-tuning LLMs
- Summary

Chapter 17: Advanced Generative AI Scenarios

- Supply-chain attacks in LLMs
- Privacy attacks and LLMs
- Model inversion and training data extraction attacks on LLMs
- Inference attacks on LLMs
- Model cloning with LLMs using a secondary model
- Defenses and mitigations for privacy attacks
- Summary

Chapter 18: Secure by Design and Trustworthy AI

- Secure by design AI
- Building our threat library
- Industry AI threat taxonomies
- AI threat taxonomy mapping
- Threat modeling for AI
- Threat modelling in action
- Enhanced FoodieAI threat model
- Risk assessment and prioritization
- Security design and implementation
- Testing and verification
- Shifting left – embedding security into the AI life cycle
- Live operations
- Beyond security – Trustworthy AI
- Summary

Chapter 19: AI Security with MLSecOps

- The MLSecOps imperative

- Toward an MLSecOps 2.0 framework
- Building a primary MLSecOps platform
- MLSecOps in action
- Integrating MLSecOps with LLMOps
- Advanced MLSecOps with SBOMs
- Summary

Chapter 20: Maturing AI Security

- Enterprise security AI challenges
- Foundations of enterprise AI security
- Protecting AI with enterprise security
- Operational AI security
- Iterative enterprise security
- Summary

Videos and How To

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

4

VIDEOS

05

MINUTES

10. 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

Building Our Adversarial Playground

- Building Baseline ML and CNN Models

Security and Adversarial AI

- Securing the Adversarial AI Playground
- Performing a Simple Evasion Attack

Poisoning Attacks

- Demonstrating a Simple Data Poisoning Attack
- Demonstrating a Backdoor Data Poisoning Attack

Model Tampering with Trojan Horses and Model Reprogramming

- Exploiting Pickle Serialization Vulnerability
- Crafting a Neural Payload Attack

Supply Chain Attacks and Adversarial AI

- Simulating and Detecting a Data Poisoning Attack

Evasion Attacks against Deployed AI

- Performing a Black-Box Adversarial Attack

Privacy Attacks – Stealing Models

- Performing a Model Extraction Attack

Privacy Attacks – Stealing Data

- Performing a Model Inversion Attack
- Performing an Attribute Inference Attack on the CIFAR-10 CNN Model

Privacy-Preserving AI

- Implementing Image Anonymization Techniques
- Implementing DP in Model Training

LLM Foundations for Adversarial AI

- Building a Basic Chat LLM Application

Adversarial Attacks with Prompts

- Exploiting LLMs Using Direct Prompt Injection

Secure by Design and Trustworthy AI

- Understanding Secure Design, Threats, and Trustworthy AI

Maturing AI Security

- Strengthening Enterprise AI Security Maturity

Here's what you get

18
LIVE LABS

16
VIDEO TUTORIALS

36
MINUTES

You can't stay away! Get

 3187 Independence Drive
Livermore, CA 94551,
United States  +1-415-763-6300  support@ucertify.com  www.ucertify.com