PROFESSIONAL COURSE OUTLINE

Exploring Adversarial Machine Learning

NVIDIA

Program aligned

Introduces adversarial machine learning concepts, attacks, and applied robustness considerations.

AI | Advanced | Deep Learning Frameworks

PROGRAM CODE	DELIVERY	DURATION	CERTIFICATION
Program aligned	Virtual, On-site, or Hybrid	2 hours	Available on request

AUDIENCE PROFILE

Who This Program Is For

Built for teams responsible for AI robustness and model security.

PROGRAM SUMMARY

What This Course Covers

Official NVIDIA self-paced course exploring adversarial machine learning.

TAILORED DELIVERY

Adapt the program around your team.

This outline can be adapted for virtual, on-site, or hybrid delivery, with emphasis adjusted for yourteam's platform priorities, role mix, and implementation goals.

Enterprise-ready delivery format

VNode ITeS can align labs, examples, delivery pace, and assessment checkpoints to the required audience profile while preserving the official program sequence where applicable.

COMPLETE MODULE SEQUENCE

Module Flow and Topic Coverage

The structure below presents the current delivery flow for this program, including the associated topics covered under each module.

1

MODULE 1

Study adversarial ML risks

Learn core adversarial concepts and what they mean for deployed model robustness.

- Adversarial attack basics
- Robustness considerations