

ART-Hub: AI Red-Team Training Hub

A hands-on training platform where students learn how AI systems can be misused, and how to defend them, inside a safe, isolated lab.

PARTNER UNIVERSITY

George Mason University, Cyber Security
Engineering senior design (CYSE 492/493)

TIMELINE

September 2026 – May 2027 (two semesters)

FOCUS AREAS

Emerging Technology Readiness · Workforce
Upskilling

SPONSOR

Intelligent Futures

STATUS

Design → Pilot: first iteration for student user
testing

AUDIENCE

Students, instructors and schools

Overview

AI red-teaming means deliberately testing an AI system to find where it can be tricked, misused or made to fail, so those weaknesses can be fixed. ART-Hub turns that professional practice into a classroom experience: quizzes on key concepts and hands-on labs against a sandboxed AI model, while instructors track progress across their class.

The team

Intelligent Futures built the first version of ART-Hub. A five-person senior design team from George Mason University's Cyber Security Engineering program is now turning it into a secure, cloud-hosted platform that multiple schools can use.

What the team is building

- Three learning tracks: Foundations, Attack and Defense
- Secure, isolated AI sandbox for every lab
- Role-based accounts and instructor dashboards
- Certificates and full cloud deployment documentation

Want ART-Hub for your school or program? Join the pilot.

intelligentfutures.tech/contact-us · Intelligent Futures is a 501(c)(3) research and innovation nonprofit.