APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Certified AI Red Team Engineer (CARTE)

Stealth Cyber Authorized Training · Applied Technology Academy

CARTE is a comprehensive AI security certification that teaches you to exploit, test and secure artificial intelligence systems — from prompt injection and jailbreaking to RAG exploitation, agent red teaming and adversarial ML. Applied Technology Academy is the exclusive US instructor-led training partner and reseller for Stealth Cyber: take CARTE live instructor-led with ATA, or as the self-paced asynchronous course.

LEVEL	MODULES	FORMAT	LABS	EXAM
Beginner to Advanced	**18**	**Instructor-led or self-paced**	**Hands-on**	**7-day practical**

Course Outline

- **Module 1: Foundations of AI Security**
  - Understanding AI systems, threat landscape, MITRE ATLAS, OWASP Top 10 for LLMs.
- **Module 2: AI System Internals**
  - Transformers, embeddings, RAG systems, agents, and how they work under the hood.
- **Module 3: Guardrails and Safety Mechanisms**
  - Input filters, system prompts, RLHF, Constitutional AI, output filters, and bypassing defenses.
- **Module 4: Prompt Injection**
  - Basic to advanced injection techniques, system prompt extraction, and defense bypassing.
- **Module 5: Jailbreaking**
  - Role-playing attacks, DAN techniques, multi-step jailbreaks, and adversarial prompts.
- **Module 6: Data Poisoning**
  - Backdoor attacks, training data contamination, and manipulating AI behavior.
- **Module 7: RAG Exploitation**
  - Document injection, retrieval manipulation, and vector database attacks.
- **Module 8: Agent Red Teaming**
  - Tool injection, action hijacking, and compromising autonomous AI agents.
- **Module 9: Model Inversion**
  - Extracting training data, membership inference, and model stealing techniques.
- **Module 10: Adversarial ML**
  - Adversarial examples, evasion attacks, and fooling neural networks.
- **Module 11: API Security**
  - Rate limiting bypass, token manipulation, and exploiting AI API endpoints.

- **Module 12: Real CVEs**
  - Exploit actual CVEs in production AI systems. Hands-on with real vulnerabilities.
- **Module 13: Professional Red Teaming**
  - Methodology, ethics, and running complete red team assessments.
- **Module 14: Ethics and Responsible Disclosure**
  - Legal considerations, ethical frameworks, responsible disclosure practices, and professional conduct.
- **Module 15: Documentation & Evidence**
  - Documenting findings, capturing evidence, and organising results from AI security assessments.
- **Module 16: Pitching AI Red Team Engagements**
  - Sales strategies, proposal writing, pricing models, and winning AI security consulting contracts.
- **Module 17: Exam Preparation**
  - Comprehensive review, exam strategy, time management, and final preparation for the practical exam.
- **Module 18: Final Practical Exam**
  - 7-day hands-on assessment. Hack 15 real vulnerable AI systems and capture 30 flags. 80% pass mark required.

Delivery & certification

No prior AI security experience required. Every module includes hands-on labs where you exploit intentionally vulnerable AI systems — solved through conversation, no pentesting tools or infrastructure attacks. Certification is earned through a 7-day practical exam: hack 15 real vulnerable AI systems and capture 30 flags, 80% to pass.

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.