

Advanced AI Red Teaming AI-300 (OSAI) Training

OffSec Authorized Training · Applied Technology Academy

Applied Technology Academy is a premier provider of OffSec's newest certification, OSAI — hands-on offensive operations in AI environments. The AI-300 (OSAI+) brings OffSec's offensive methodology to AI, with advanced red teaming for large language models and multi-agent systems.

LEVEL Advanced	DURATION 5 Days	EXPERIENCE 3 yrs offensive security	EXAM 48-hour performance exam	AVERAGE SALARY \$140,895
---------------------------------	----------------------------------	--	--	---

Course Overview

The AI-300 (OSAI+) is an enterprise-grade, hands-on offensive AI red teaming certification that proves your team can pressure-test LLMs and agent systems under realistic conditions. It is designed to develop practitioners who can think like adversaries in AI environments and keep pace as the threat landscape evolves. Core focus areas include offensive testing of LLMs and multi-agent systems; RAG compromise and control-surface abuse; AI supply-chain and infrastructure exploits; and post-exploitation with impact analysis that turns findings into real improvement. The certification culminates in a rigorous 48-hour exam built to validate real-world adaptability against novel AI attack surfaces.

Course Outline

OSAI is delivered as modular, self-paced online training, with instructor-led training available. OffSec is finalizing the detailed module outline — contact us for the latest curriculum and upcoming cohort dates.

Intended Audience

OSAI is built for practitioners who need to assess and pressure-test AI-enabled systems the way real adversaries do:

- Red teamers and penetration testers expanding into AI
- Security professionals tasked with evaluating AI-enabled systems
- AI engineers who need to understand adversarial risk
- Security teams building an internal AI red teaming capability

Prerequisites

This course and certification are not an introduction to AI, nor to AI penetration testing. Prior AI experience is not required, but we recommend familiarity with LLMs and some basic LLM pentesting methodology. Learners should also have solid general offensive-security fundamentals — OSCP or equivalent hands-on experience is recommended.

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.