

PROGRAM AT A GLANCE

Securing the AI supply chain

6 STEPS | 17 ACTIVITIES 7H 45Min

About the program

The program moves from conceptual risk awareness, to AI-specific foundations, to hands-on controls, to pipeline hardening, to attack and detection practice, and finally to crisis decision-making. In short: understand the risk, implement controls, test and detect attacks, then make incident-response decisions under pressure.


● BEGINNER 8 ● INTERMEDIATE 8 ● EXPERT 0

Program structure

AI, LLM, AND AGENTIC SUPPLY CHAIN RISK

4 Labs 65 Min

Explore AI verification expectations and supply-chain risks in LLM, GenAI, and agentic systems.

- OWASP Top 10 for LLM Applications: Supply Chain
- OWASP AISVS: Supply Chain Security
- OWASP Top 10 for Agentic Applications: Agentic Supply Chain Vulnerabilities
- OWASP Top 10 for Agentic Skills: Supply Chain Compromise

AI SUPPLY CHAIN FOUNDATIONS

3 Labs 85 Min

Understand AI-specific supply-chain layers, threat patterns, and defensive controls before assessment.

- Introduction to the AI Supply Chain: The Four Layers
- Introduction to the AI Supply Chain: Threat Landscape and Controls
- Introduction to the AI Supply Chain: Demonstrate Your Knowledge

MODEL ASSURANCE AND PROVENANCE

3 Labs 110 Min

Practice scanning, signing, documenting, and assessing model artifacts before production use.

- Securing the AI Supply Chain: Model Scanning and Signing
- Securing the AI Supply Chain: AIBOM Generation
- Securing the AI Supply Chain: Demonstrate Your Skills

AI AGENTS IN CI/CD PIPELINES

3 Labs 110 Min

Audit and harden AI agents in build workflows to limit prompt, tool, configuration, and secret exposure.

- AI Agents in the CI/CD Pipeline: Workflow Auditing
- AI Agents in the CI/CD Pipeline: Workflow Hardening
- AI Agents in the CI/CD Pipeline: Demonstrate Your Skills

AI SUPPLY CHAIN PURPLE TEAMING

3 Labs 95 Min

Pair red-team supply-chain attack paths with blue-team detection across AI initial-access scenarios.

- MITRE ATLAS: Initial Access
- AI Red Teaming: Initial Access – Supply Chain Attacks
- AI Blue Teaming: Initial Access – Detection

CRISIS SIMULATION EXERCISE

1 Scenario

Apply the learning in a decision-based AI supply-chain incident response exercise.

- Agentic AI compromise: assuring and containing your AI agents