

Practitioner's Playbook for RSAIF

Course Duration: 8 Hours

TOC

Module 1: AI Security Foundations – Responsible Development & Secure Design

- 1.1 Overview of AI Security Challenges
- 1.2 Secure Design Principles
- 1.3 Best Practices for Secure AI
- 1.4 Hands-On: Threat Modeling Workshop

Module 2: AI Threat Models

- 2.1 Introduction to Threat Modeling
- 2.2 Creating an AI Threat Model
- 2.3 Tools for Threat Modeling
- 2.4 Case Study: AI in Autonomous Vehicles

Module 3: Secure AI SDLC (Software Development Lifecycle)

- 3.1 SDLC Overview
- 3.2 AI-Specific Security Measures
- 3.3 Continuous Monitoring & Feedback Loops
- 3.4 Hands-On: Integrating Security in AI Development
- 3.5 Use Case: AI Fraud Detection System

Module 4: Enforcement & Model Integrity

- 4.1 Securing AI Systems Post-Deployment
- 4.2 Model Integrity and Auditing
- 4.3 Hands-On: Implementing RBAC

Module 5: Audit Readiness & Red-Teaming

- 5.1 Preparing AI Systems for Audits
- 5.2 Red-Teaming for AI Systems
- 5.3 Hands-On: Red-Teaming Simulation

Module 6: Toolkits & Automation

6.1 Introduction to AI Security Tools

6.2 Automating AI Security and Compliance

6.3 Hands-On: Tool Integration