APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Threat Modeling and Secure Design

Applied Technology Academy

Learn design principles and refactoring practices that improve maintainability. The course focuses on structure, trade-offs, and long-term code quality. AI-assisted comparison, smell detection, and review are included where appropriate.

LEVEL	DURATION	COURSE CODE	DELIVERY
Intermediate	**1–2 days**	**MA-87-2**	**Instructor-led**

Course Overview

- Design principles and refactoring practices that improve maintainability.
- Structure, trade-offs, and long-term code quality.

Course Outline

- **Unit 1: Foundations:**
  - core concepts and terminology
- **Unit 2: Application:**
  - guided practice and labs
- **Unit 3: Handoff:**
  - troubleshooting, review, and next steps

Prerequisites

Participants should have:

- working familiarity with the target language or framework
- ability to read and modify existing code
- basic troubleshooting skills
- access to the required tools or accounts before class

Who Should Attend

- Developers, senior developers, and technical leads.
- Teams that want a practical conversation about structure and maintainability.
- Learners who need to recognize design smells and refactoring opportunities.

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

What You'll Learn

By the end of this course, participants will be able to:

- identify high-risk security issues in the target stack
- apply practical defenses and secure coding patterns
- explain trade-offs in authentication, validation, and data handling
- use AI-assisted review where it improves speed and consistency
- carry the lessons into team standards and code review habits

What the Course Covers

In Scope:

- secure coding patterns
- common vulnerability classes
- defensive design and remediation
- AI-assisted review and analysis where appropriate

Not Covered:

- deep penetration testing
- full red-team operations
- formal certification prep unless customized

Hands-On Work

Representative Labs:

- identify and fix a vulnerable code path
- review an OWASP scenario
- harden authentication or input handling
- compare secure and insecure implementations

Practice and Discussion:

- Guided practice with checkpoints
- Scenario discussion using realistic examples
- Review of trade-offs and next steps

Environment and Tools

- Target language/runtime for the branch
- Browser, editor, and lab environment
- Sample insecure app or codebase

- Optional OWASP references

Customization Options

- role-based track variations
- industry or domain-specific examples
- mixed-experience pacing adjustments
- accelerated or extended delivery formats

Next Steps

- advanced secure coding specialization
- cloud security follow-on
- threat modeling or DevSecOps path
- team-specific secure development rollout

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.