Course Duration: 08 hours (1 Day)

Shifting Security Left: Hands-On Architectural Threat Modelling

This comprehensive 8-hour course provides a deep dive into practical threat modelling for secure software development. Participants will learn how to anticipate security flaws before writing a single line of code. The curriculum balances core theoretical concepts with extensive, interactive hands-on laboratory exercises. It covers popular methodologies including STRIDE to systematically uncover architectural vulnerabilities. Students will learn to construct clear Data Flow Diagrams to visually map out application attack surfaces. The course guides learners through the process of evaluating risks and prioritizing security mitigations. Participants will also explore modern automated tools to scale threat modelling across engineering organizations. Real-world case studies are woven throughout the day to mirror industry-specific security challenges. Ultimately, this training builds a proactive security mindset to stop vulnerabilities at the design phase.

Course objectives

- By the end of this course, participants will be able to:
- Deconstruct complex software architectures into structured Data Flow Diagrams (DFDs).
- Apply the STRIDE methodology to systematically identify security threats in an application.
- Evaluate and prioritize discovered vulnerabilities using risk scoring frameworks.
- Formulate actionable security requirements and mitigation strategies.
- Integrate automated threat modelling tools and practices into modern DevSecOps pipelines.

Prerequisites

Participants should have:

- Basic SDLC Familiarity
- Core Web Concepts
- Fundamental Security Concepts like Authentication, Authorization
- Coding/Scripting Exposure: Ability to read basic code or configurations

Intended Audience

- Software Developers & Engineers
- Application Security (AppSec) Specialists
- Software Architects
- DevOps & DevSecOps Engineers

- QA Engineers & Technical Product Managers

Course outline

Module 1: Introduction to threat modeling

- Introduction
- Threat Modeling Phases
    - Design
    - Break
    - Fix
    - Verify

***Hands-on Exercise*:** Brainstorming & setting security boundaries for a sample Web application.

Module 2: Deconstructing the System Architecture

- Data-flow diagram elements
- Process – The task element
- Data store - The storage element
- External entity - The no control element
- Data-flow - The data in transit element
- Trust boundary - The trust zone change element

***Hands-on Exercise*:** Drawing a comprehensive Data Flow Diagram for a multi-tier E-commerce application (Users, API Gateway, Microservices, Databases).

Module 3: Threat Identification with STRIDE

- Spoofing - pretending to be someone or something else
- Tampering - changing data without authorization
- Repudiation - not claiming responsibility for an action taken
- Information disclosure - seeing data I'm not supposed to see
- Denial of Service - overwhelming the system
- Elevation of privilege - having permissions I should not have

***Hands-on Exercise*:** Mapping STRIDE threats to the E-commerce DFD created in Module 2.

Module 4: Prioritize your issues and apply security controls

- Issue prioritization, security control types, and functions
- Prioritize security issues
- Security control types and functions