Threat Modeling and Secure Design Review Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

This intensive, hands-on masterclass establishes Proactive Security as a core competency, moving beyond reactive patching to fully embrace the Shift Left philosophy. In the dynamic landscape of modern software delivery characterized by continuous integration and DevSecOps pipelines security must be integrated at the design stage. Threat Modeling and Secure Design Review Training Course provides participants with structured, repeatable methodologies to systematically identify, analyze, and prioritize threats and vulnerabilities across the entire system development lifecycle (SDLC). By mastering techniques like Data Flow Diagramming and identifying Trust Boundaries, attendees will gain the skills necessary to define security requirements and perform effective Secure Design Reviews (SDRs), ensuring system Resilience from the ground up.

The program is engineered to transform developers, architects, and security engineers into security design champions. It offers deep dives into industry-leading frameworks, including the popular STRIDE model for system decomposition and the risk-centric PASTA methodology for attack simulation. Participants will learn how to articulate risk in business terms, translating complex architectural flaws into clear, actionable mitigations. The ultimate goal is to minimize the Attack Surface and prevent costly architectural flaws, creating an enduring culture of Security by Design that protects critical business assets in environments spanning from traditional monoliths to complex Cloud-Native and microservices architectures.

Programme Curriculum

Threat Modeling and Secure Design Review Training Course

Introduction

This intensive, hands-on masterclass establishes Proactive Security as a core competency, moving beyond reactive patching to fully embrace the Shift Left philosophy. In the dynamic landscape of modern software

delivery characterized by continuous integration and DevSecOps pipelines security must be integrated at the design stage. Threat Modeling and Secure Design Review Training Course provides participants with structured, repeatable methodologies to systematically identify, analyze, and prioritize threats and vulnerabilities across the entire system development lifecycle (SDLC). By mastering techniques like Data Flow Diagramming and identifying Trust Boundaries, attendees will gain the skills necessary to define security requirements and perform effective Secure Design Reviews (SDRs), ensuring system Resilience from the ground up.

The program is engineered to transform developers, architects, and security engineers into security design champions. It offers deep dives into industry-leading frameworks, including the popular STRIDE model for system decomposition and the risk-centric PASTA methodology for attack simulation. Participants will learn how to articulate risk in business terms, translating complex architectural flaws into clear, actionable mitigations. The ultimate goal is to minimize the Attack Surface and prevent costly architectural flaws, creating an enduring culture of Security by Design that protects critical business assets in environments spanning from traditional monoliths to complex Cloud-Native and microservices architectures.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Decompose complex applications and Cloud-Native systems using advanced Data Flow Diagramming
2. Apply the STRIDE methodology to systematically identify and categorize application-level threats
3. Execute the seven-step PASTA methodology to conduct attacker-focused, risk-centric threat analysis.
4. Define and enforce Zero Trust principles across distributed systems and network architectures.
5. Identify and mitigate common design-level vulnerabilities that lead to high-impact data breaches
6. Evaluate and rank threat severity using risk assessment frameworks like DREAD.
7. Integrate Threat Modeling activities seamlessly into Agile and DevSecOps pipelines
8. Perform a structured Secure Design Review (SDR), focusing on critical attack surfaces like APIs and third-party integrations.
9. Develop robust Defense-in-Depth strategies using security controls at every architectural layer.
10. Model threats against modern paradigms, including Microservices and containerized environments.
11. Construct and analyze Attack Trees to visualize multi-stage attack paths and identify critical chokepoints.
12. Analyze emerging threats, including risks associated with Adversarial Machine Learning and AI/ML systems
13. Create high-quality, actionable security requirements from identified threats that can be tracked as engineering tasks.

Target Audience

1. Software Architects.
2. Senior Developers / Engineers.
3. Security Engineers
4. Product Managers / Owners.
5. Technical Project Managers.
6. Quality Assurance (QA) / Penetration Testers.
7. Information Security Managers.
8. Cloud Engineers.

Course Modules

Module 1: Foundations of Proactive Security and System Decomposition

- Security by Design and the Shift Left Mandate.
- Identifying Assets and Value.
- Architecture Modeling and Data Flow Diagrams.
- Trust Boundaries and Attack Surface Definition.
- Threat Modeling Frameworks Overview.
- Case Study: Analyzing the Equifax Breach to demonstrate how an overlooked component and vulnerable external interface created a massive attack surface.

Module 2: STRIDE Methodology and Application-Level Threat Analysis

- Deep Dive into STRIDE.
- Applying STRIDE to System Elements
- Defining the Context of Authentication and Authorization.
- Detecting Integrity and Availability Flaws.
- STRIDE Workshop.
- Case Study: Examining the Yahoo Data Breach focusing on how compromised credentials and lack of multi-factor authentication allowed for initial access and Spoofing.

Module 3: PASTA Methodology and Risk-Centric Threat Simulation

- The Seven Stages of PASTA.
- Attacker Simulation.
- Integrating Threat Intelligence.
- Risk Rating and Prioritization.
- Translating Technical Risk into Business Impact.
- Case Study: The WannaCry Ransomware Attack, analyzing the risk acceptance of patching vulnerable systems and using DREAD to score the high impact of the Denial of Service and Information Disclosure threats.

Module 4: Secure Design Principles and Mitigation Strategies

- Defense in Depth.
- Implementing the Zero Trust Architecture
- Secure Configuration Management and Hardening
- Least Privilege and Segregation of Duties.
- Secure Data Handling
- Case Study: Analyzing the Pegasus Airlines Misconfiguration Incident to highlight how poor privilege separation and unsecured configurations exposed massive amounts of data.

Module 5: Threat Modeling for Modern and Cloud-Native Systems

- Microservices and API Security
- Containerization and Orchestration Threats.
- Serverless and FaaS Security
- Infrastructure-as-Code Review.
- Third-Party and Supply Chain Risk

- Case Study: Reviewing the SolarWinds Supply Chain Attack to model how the compromise of a single trusted software dependency led to wide-scale Elevation of Privilege across customer environments.

Module 6: The Secure Design Review (SDR) Process

- SDR Mandate and Entry Criteria
- Documenting Security Requirements.
- The Review Checklist
- Effective Stakeholder Collaboration.
- Design Artifacts and Documentation.
- Case Study: A simulated review of a fictional FinTech Payment Gateway API, focusing on authentication flows, data validation, and rate-limiting to prevent Denial of Service.

Module 7: Advanced Threats and Specialized Modeling

- Adversarial Machine Learning (ML) Threats.
- Introduction to MAESTRO.
- Privacy Threat Modeling.
- Physical and Operational Technology (OT) Threat Modeling.
- Attack Tree Construction Workshop.
- Case Study: The NYU Admissions Leak to focus on the interplay between Information Disclosure and the LINDDUN principles of Unawareness and Non-Compliance.

Module 8: Continuous Threat Modeling and Automation

- Integrating TM into CI/CD.
- Automating DFD and Threat Enumeration.
- Security Champions Program.
- Metrics and Reporting
- Model Maintenance and Iteration.
- Case Study: Applying the concept of Continuous Threat Modeling to a company undergoing rapid feature deployment and how automation prevents new vulnerabilities from reaching production.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now