

## SC TM 101: PRACTICAL THREAT MODELING

This class equips students with the knowledge and techniques required to perform a threat model. Threat modeling is a powerful activity to reduce overall cost in application security initiatives by prioritizing threats based on risk. It also allows developers to consider security at the design and architecture phases of the software development life cycle (SDLC).

Threat modeling is gaining traction as a fundamental application security activity. In this class students learn about the attacks that their applications may face and then both formal and informal approaches to threat modeling. Using a fictional scenario, students perform all the activities of a threat model on a complex application – including analyzing design documents and role-playing interviews. Students learn about the industry standard formal threat modeling process as well as Facilitated Application Threat Modeling: a 1-day approach to threat modeling pioneered by Security Compass. Students will also be taught about Security Compass’s unique source-code/design-pattern level threat modeling.

### DURATION & INTENDED AUDIENCE

- Duration: 2 days
- Intended Audience:
  - Developers, architects, tech leads
  - Information security analysts who perform application penetration testing and/or source code reviews

### PRE-REQUISITE KNOWLEDGE

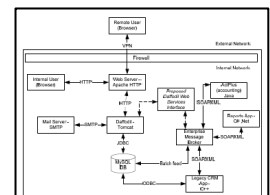
- Basic understanding of Software Development Life Cycle
- Programming experience helpful but not mandatory

### LEARNING OBJECTIVES

- Understand attacks that hackers use to break into web applications
- Create threat models for complex multi-tiered applications
- Prioritize risk of attacks for an application based on potential threats
- Apply security analysis to design and architecture of an application

### LEARNING ENVIRONMENT & TAKEAWAYS

- Students work in teams to decompose a fictional application, determine use cases, analyze threats and prioritize based on risk
- Course book containing printouts of each slide along with detailed notes in paragraph form
- Hard-copy and soft copy of threat model worksheets for both formal and informal threat models



### CONTACT INFO

- Phone: 1-888-777-2211 x 1
- Email: [training@securitycompass.com](mailto:training@securitycompass.com)

## DETAILED OUTLINE

### DAY 1: INTRO

#### Authentication

- Factors of Authentication
- User Enumeration
- Password Reset
- Brute Force
- Password Sniffing

#### Authorization

- Privilege Escalation
- Page Authorization
- Functional Authorization
- Data Authorization

#### Session Management

- Session Hijacking
- Content Caching

#### Cryptography

- Random Numbers
- Hashes
- Rainbow Tables
- Symmetric Key Encryption
- Asymmetric key Encryption
- Cryptographic Flaws

#### Input Validation

- Input Validation Overview
- Parameter Manipulation
- XSS & CSRF
- HTTP Response Splitting
- SQL Injection
- XML Parsers & Validators
- XML Attack

### DAY 2: THREAT MODEL

#### Introduction

- What is threat modeling and what does it achieve
- Why do threat modeling?
- Discussion of formal versus informal threat modeling

#### Threat modeling steps

- Summary of steps used

#### Gather information

- Kinds of information to gather
- Sources to gather information from
- Interview the architect
- Finding more information about the application

#### Distill Application

- Technical components
- User roles
- Data types
- Distilling an application

#### Data Flow

- Developing data flow diagrams

#### Use Cases

- Building use cases
- Establishing threats
- Technical threats and resources
- Business logic threats
- Building countermeasure

### DAY 2 CONTINUED

#### Countermeasures

- Establishing countermeasures
- Attack trees & countermeasures
- Reviewing solution

#### Conclusion

- Comparison of threat modeling methods
- Architecture vs. design threat models
- Practical limitations & tool support