Hands-On Threat Modeling

Course Description

Threat Modeling is considered as one of the most effective ways to reduce the risk and increase the security of applications and systems of any kind (PC, Mobile, Web, Server/Cloud, Embedded, IoT, Automotive, Aviation, Medical, etc.).

As a structured process, it can be used to help to identify potential threats, attacks, vulnerabilities, and countermeasures that could impact your applications. Whether you're a developer, executive, security engineer, or just interest in protecting your product, this training is for you!

You cannot protect something unless you understand what you're protecting it from.

In this hands-on training, you'll be the ins and outs of Threat Modeling:

- What Threat Modeling is?
- The pros and cons are of common Threat Modeling methodologies.
- How to choose the best Threat Modeling methodology suited for you.
- How to perform the generic Threat Modeling process.
- How Threat Modeling can be used to identify attacks that your products might be vulnerable to?
- How to successfully draw architecture diagrams for Threat Modeling.
- How to use Threat Modeling outcome to ensure you your product is secured.
- What are the challenges and pitfalls you might face when attempting to use Threat Modeling and how to work around those.
- How to successfully apply Threat Modeling in your day-to-day activities, projects, or environments.

The techniques we discuss are applicable to all system types (mobile, , web, embedded systems, IoT, cloud, etc.)

Target Audience

- Software engineers / Development managers
- Software designers / architects
- Security engineers
- Product Managers

Our Hands-on approach

Although traditional training methods will always have their place in learning, some things can't be taught using simple knowledge transfer techniques.

Without practicing Threat Modeling and showing real examples, the knowledge you gain remains in your head.

Our approach to teaching was always "Hands-On" approach, which has clear benefits:

- Employees Learn Best by Doing
- Employees Find It More Fun and Engaging
- A Hands-on Approach Appeals to Almost Every Learning Preference
- Employees Leave Feeling Confident and Empowered by What They Learned
- Learning Continues Back on the Job

Training Agenda:

- Module 1 - Introduction
- Module 2 - Threat Modeling Basics
- Module 3 - System Modeling Techniques
- Module 4 - Threat Identification
- Module 5 - Threat Mitigation
- Module 6 - Threat Modeling Validation
- Module 7 - How to succeed in Threat-Modeling

Prerequisites

Course participants should have knowledge of basic security fundamentals like Confidentiality, Integrity, and Availability (CIA). Basic knowledge of application development is preferred but is not necessary.

Course Material

1. Course Slides
2. Exercise notebook
3. Threat Modeling Handbook – A Step by Step Guide
4. Students MUST bring a laptop with approximately 15GB of free space.