

SEC202 -THREAT MODEL EXPRESS

Course Learning Objectives

Understand the benefits of a traditional threat model versus a threat model express session. Engage in asking valuable questions that will effectively identify potential threats within an application. Learn who should be involved in a Threat Model Express session and how to apply the model within your organization. The course will discuss the outcome of performing a TME session and will discuss potential countermeasures to secure an application.

Description

Students will learn about the attacks that their applications may face and then an informal approach to threat modeling. They will first learn the steps in executing a Threat Model Express, and then they will engage in a guided fictional exercise.

Audience



Application developers / Application architects
Security professionals

Time Required



Tailored learning - 42 minutes total

Exercise 1: Risk ranking

Drag each established risk where you think it should be placed in our impact/likelihood chart based on the following use case.

Anonymous user browses music catalog

| Risk | Impact | Likelihood |
|------|--------|------------|
| T1 | High | Low |
| T2 | High | High |
| T3 | Medium | Medium |

- T1 Anon is able to access a real user's music catalog
- T2 Anon is able to alter user or catalog data in the database from the web application parameter tampering
- T3 Anon performs DDoS attack against web application

Hide answer

click next when ready to continue

Roles of the participants

Click on each of the following roles to learn more about who you should invite to the TME meeting. Click next when you're ready to continue.

Threat Model Express process

START

END

- collect information
- learn the business drivers and risks
- prioritize the risk
- have the SME guide the conversation

DETERMINE GOALS AND SCOPE

- set up a list of goals before the TME
- determine the scope

ENUMERATE THE THREATS

- learn the relevant threats against your application

DETERMINE COUNTER MEASURES

- action items to mitigate risks
- implement

click next to continue

SEC202 -THREAT MODEL EXPRESS

Course Outline

1. Gathering Requirements

- What is threat modeling?
- Traditional vs. express
- Goals of the threat model
- Importance of scope
- TME process
- What kinds of information to gather
- Sources to gather information from
- Finding more about the application
- Distilling an application
- Developing data flow diagrams
- Asking the right questions
- Who to invite
- Roles of the participants

2. Performing a TME Session

- Determining threats
- STRIDE
- Attacker motivations
- Establishing threats
- Determining risks
- Factors of impact
- Impact rating
- Factors of likelihood
- Likelihood rating
- Risk ranking
- Countermeasures
- What's next?