DTM101 - DEVELOPER CENTRIC THREAT MODELING

Course Learning Objectives

This course has been designed to explore a more modern approach to threat modeling for the contemporary developer. In module 1, we cover the basics of threat modeling, such as the difference between a threat, a risk, a vulnerability, trust boundaries, and the benefits of the developer-centric threat model process. In module 2, we cover the benefit and impact of threat modeling in general and explain how to run an effective one. In module 3, we discuss different approaches and frameworks involved in threat modeling. In module 4, we explore foundational aspects of performing a threat model, the nature of a threat, how we can leverage STRIDE, and the benefits of open-source and commercial tools. Finally, we put all of it together in module 5 to execute a developer-centric threat model with and without machine assistance.

Description

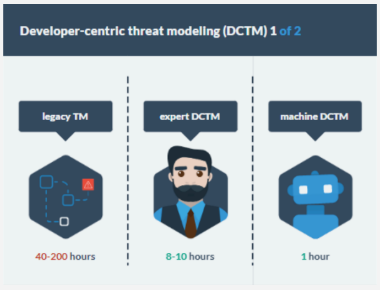
Developer-centric Threat Modeling (DCTM) is a course for Security Architects, Security Champions, and Lead Developers who are interested in threat modeling for today's modern and Agile methodologies. This course covers threat modeling from the ground up and focuses on how developers can not only contribute to, but also run threat modeling in their organization. From best practices to threat modeling frameworks, and issue management to tooling, join Sam—a budding Security Champion—and Antoni—a cybersecurity and threat modeling expert—on their journey to bring developer-centric threat modeling to their organization, BitByBit.

Audience

Security Architects
Security Champions
Lead Developers

Time Required

Tailored learning - 80 minutes total (approx.)



DTM101 - DEVELOPER CENTRIC THREAT MODELING

Course Outline

1. What is Threat Modeling

- What is threat modeling
- Difference between threat, risk, and vulnerability
- What is a trust boundary
- Threat modeling real life example
- Threat modeling infosec example
- Why is threat modeling important
- The four questions of threat modeling
- Knowledge check
- Different types of threat models and when to use them
- Architecture threat model
- Operational model
- Application model
- What is developer-centric threat modeling
- How does it compare to traditional threat modeling

2. Running an Effective Threat Model

- When you should and should not threat model
- Document your approach
- Agile versus waterfall
- Knowledge check
- Running an effective threat model
- Identify scope
- Who should be involved
- Every organization differs
- Manage time effectively
- Scheduling a threat model exercise
- Identify trust boundaries
- Discuss threats and risks
- Discuss countermeasures/mitigations
- Application code
- Document a threat model
- Document scope
- Document threats, countermeasures, and risk
- Document action items and next steps
- Executive summary and conclusion
- What happens after
- Follow-ups and implementation plan
- Marketing success of your threat modeling
- Plan for next threat model

3. Approaches and Frameworks

- Threat modeling approaches
- Asset-centric approach
- Software-centric approach
- Attack-centric approach
- Knowledge check
- Threat model frameworks
- STRIDE
- OCTAVE
- TRIKE
- DREAD
- CVSS
- Attack trees
- PASTA
- MITRE ATTACK
- Knowledge check
- Cyber attack lifecycle
- Threat modeling as code
- Threat modeling in code
- Developer-centric threat model

4. Evaluating Threats

- Practicality of a threat
- Threat libraries
- Why STRIDE
- Overview
- Spoofing Identity
- Spoofing interactivity
- Tampering
- Tampering interactivity
- Repudiation
- Repudiation example
- Information disclosure
- Information disclosure example
- Denial of service
- Denial of service interactivity
- Elevation of privilege
- Elevation of privilege example
- Ranking threats
- Commercial tooling
- Free/open-source tooling

5. Executing Developer-Centric Threat Model

- Developer-centric threat modeling
- Step 1
- SecureSound example
- Automated example
- Step 2
- SecureSound example
- Automated example
- Step 3
- SecureSound example
- Automated example
- Step 4
- SecureSound example
- Automated example
- Step 5
- SecureSound example
- Automated example

SecurityCompass