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 challenges of traditional threat modeling. In module 2, we describe the different threat modeling diagrams, from architecture to data flow diagrams, and attack trees. In module 3, we discuss how to leverage STRIDE to find and categorize threats. In module 4, we explain how to run an effective threat model. 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

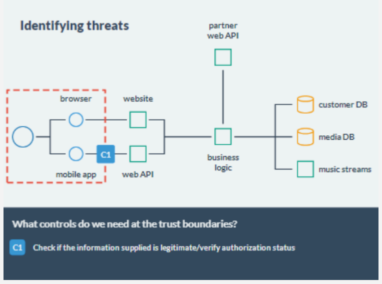
- Security Architects
- Security Champions
- Lead Developers

Time Required

Tailored learning - 80 minutes total (approx.)

Who should be involved in a threat model?

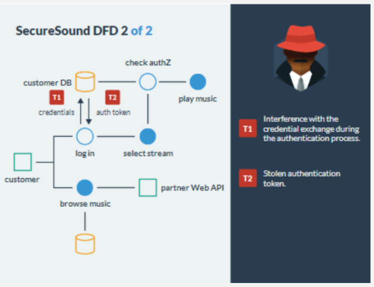
Key
Other
Software Development (Dev) Team
Application Security (AppSec) Expert
Risk Executive
Technology Executive



Identifying threats

What controls do we need at the trust boundaries?

C1 Check if the information supplied is legitimate/verify authorization status



SecureSound DFD 2 of 2

T1 Interference with the credential exchange during the authentication process.

T2 Stolen authentication token.

Security Compass

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
- The four questions interactivity
- Traditional threat modeling challenges
- The Threat Modeling Manifesto
- Key ideas of developer-centric threat modeling
- Conclusion

2. Threat Modeling Diagrams

- Threat modeling diagrams
- SecureSound
- Architecture diagrams
- Trust boundaries
- Identifying threats
- Data Flow Diagrams
- SecureSound DFD
- DFD challenges
- Attack trees
- SecureSound attack tree
- Mitigations
- Attacker-centric threat modeling
- Threat modeling software
- Open source tools

3. Evaluating Threats

- Practicality of a threat
- Threat libraries
- Finding threats
- STRIDE
- STRIDE categories
- STRIDE example 1
- STRIDE example 2
- STRIDE example 3
- STRIDE example 4
- Ranking threats
- Ranking impact, probability, and complexity
- Impact example
- Probability example
- Complexity example
- Other frameworks
- Threat libraries

4. Running an Effective Threat Model

- When to threat model
- Document your approach
- Agile versus waterfall
- Waterfall
- Agile
- Knowledge check
- Identify scope
- Who should be involved in a threat model?
- Every organization differs
- Manage time effectively
- Scheduling a threat model exercise
- Identify trust boundaries
- Discuss countermeasures and mitigations
- Application code
- Document the threat model
- Document scope
- Document threats, countermeasures, and risk
- Document action items and next steps
- Executive summary and conclusion
- Follow-ups and implementation plan
- Marketing success of your threat modeling
- Plan for next threat model

5. Executing Developer-Centric Threat Model

- BitbyBit
- DCTM
- 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
- Conclusion

Security Compass