workED

CYBERSECURITY
THREAT MODELING

Presented by:

workED

INTRODUCTION

- Understanding threat modeling, its importance, and methods and frameworks.
- Identify steps of threat modeling and steps to implement a threat modeling framework.

workED

THREAT MODELING QUESTIONS

What are the steps of threat modeling?

Why is threat modeling important?

What are the key steps to implementing a threat modeling framework?

What are the methods and frameworks of threat modeling?

workED

WHAT ARE THE STEPS OF THREAT MODELING?

1. Identify security objectives
2. Create application overview
3. Decompose application
4. Identify threats
5. Identify vulnerabilities

workED

WHAT IS THREAT MODELING IMPORTANT?

- Enables a project team to determine which security controls an application needs
- Prepares teams to resolve problems early on
- Helps developers build security into a project during development and maintenance phases

workED

WHAT ARE THE KEY STEPS TO IMPLEMENTING A THREAT MODELING FRAMEWORK?

1. Form a team (stakeholders).
2. Establish the scope.
3. Determine likely threats.
4. Rank each threat (level of risk).
5. Implement mitigations (avoid, transfer, reduce, or accept).
6. Document results.

workED

WHAT ARE THE METHODS AND FRAMEWORKS OF THREAT MODELING?

- Data flow diagrams visualize how data moves through application/system.
- Process flow diagrams show application/system from user interaction perspective.
- Attack trees visualize attacks on a system, using tree root as goal of attack. (MITRE ATT@CK)
- Attack-centric methods focus on types of possible attacks.
- Asset-centric methods focus on assets to be protected.

workED

WHAT ARE THE METHODS AND FRAMEWORKS OF THREAT MODELING?

- Damage, Reproducibility, Exploitability, Affected users, Discoverability (DREAD)
- National Institute of Standards and Technology's Guide to Data-centric System Threat Modeling
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- Process for Attack Simulation and Threat Analysis (PASTA)
- STRIDE
- Trike
- Visual, Agile, and Simple Threat (VAST)

workED

CONCLUSION

- Threat-modeling methods are used to create an abstraction of the system, profiles of potential attackers and their goals and methods, and a catalog of potential threats that may arise.
- Many threat-modeling methods have been developed that can be combined to create a more robust and well-rounded view of potential threats. Not all threat-modeling methods are comprehensive; some are abstract and others are people-centric. Some methods focus specifically on risk or privacy concerns.
- Threat modeling should be performed early in the development cycle when potential issues can be caught early and remedied, preventing a much costlier fix down the line. Using threat modeling to think about security requirements can lead to proactive architectural decisions that help reduce threats from the start.

workED

CYBERSECURITY
THREAT MODELING

QUESTIONS?

THANK YOU