ONE PAGE SUMMARY

IT & Software › Cyber Security › Threat Modeling

Introduction to Threat Modeling

Mastering Threat Modeling for Enhanced Cyber Security

DEFINITION

> Threat modeling is a structured approach to identifying and mitigating potential security threats. It helps organizations understand vulnerabilities and prioritize security measures.

KEY CONCEPTS

Assets

Assets are valuable components of a system, such as data, applications, or hardware, that need protection.

Threats

Threats are potential dangers that could exploit vulnerabilities in a system, leading to harm or loss.

Vulnerabilities

Vulnerabilities are weaknesses in a system that can be exploited by threats to gain unauthorized access or cause damage.

Mitigation Strategies

Mitigation strategies are actions taken to reduce or eliminate the risks posed by identified threats.

Modeling Techniques

Modeling techniques, such as STRIDE or PASTA, provide frameworks for systematically analyzing threats.

EXAMPLES

→ Identifying sensitive customer data as an asset in an e-commerce platform.

→ Using STRIDE to analyze potential threats to a web application.

→ Implementing encryption as a mitigation strategy for data at rest.

MEMORY TIPS

★ Remember 'AVM' - Assets, Vulnerabilities, Mitigations.

★ Use the acronym STRIDE for common threat types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

★ Visualize a shield protecting valuable assets to recall the purpose of threat modeling.

COMMON MISTAKES

✗ Overlooking less obvious assets like user credentials.

✗ Failing to update threat models as systems evolve.

✗ Neglecting to involve all stakeholders in the modeling process.

QUICK RECAP

Threat modeling is essential for identifying and addressing security risks. By understanding assets, threats, and vulnerabilities, organizations can implement effective mitigation strategies. Regular updates and stakeholder involvement are crucial for success.