ONE PAGE SUMMARY

IT & Software › Cyber Security › Threat Modeling

Introduction to Threat Modeling

Mastering Threat Modeling: Your Shield Against Cyber Attacks

DEFINITION

> Threat modeling is a proactive approach to identifying and addressing potential security threats in a system. It helps organizations understand vulnerabilities and prioritize their security efforts.

KEY CONCEPTS

Assets

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

Threats

Threats are potential events or actions that could exploit vulnerabilities and cause harm to assets.

Vulnerabilities

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

Attack Vectors

Attack vectors are the paths or methods used by attackers to exploit vulnerabilities and compromise systems.

Mitigation Strategies

Mitigation strategies are measures taken to reduce the risk of threats exploiting vulnerabilities.

EXAMPLES

→ Identifying sensitive customer data as an asset.

→ Recognizing phishing emails as a potential threat.

→ Implementing firewalls to mitigate unauthorized access.

MEMORY TIPS

★ Remember 'AVTM' - Assets, Vulnerabilities, Threats, Mitigation.

★ Visualize a shield protecting your assets from arrows (threats).

★ Use the acronym 'TAM' - Threats, Assets, Mitigation for quick recall.

COMMON MISTAKES

✗ Overlooking less obvious assets like employee credentials.

✗ Failing to update threat models regularly.

✗ Neglecting to involve all stakeholders in the threat modeling process.

QUICK RECAP

Threat modeling is essential for identifying and addressing security threats. Focus on assets, threats, vulnerabilities, and mitigation strategies to enhance system security.