Threat Modeling in a Nutshell

Threat modeling is a systematic process to identify potential threats to a system, assess their impact, and develop countermeasures.

Steps:

Identify assets: Determine what needs protection.
Identify threats: Determine potential dangers.
Assess vulnerabilities: Find system weaknesses.
Analyze impact: Evaluate the potential damage.
Develop countermeasures: Create solutions to protect assets.

Benefits:

Improves system security
Manages risks effectively
Ensures compliance
Saves costs

Example: For an online store, threats might include hacking, data breaches, and denial of service attacks. Countermeasures could be encryption, firewalls, and backups.