Threat Modeling Frameworks:

MITRE ATT&CK Framework

The federally funded R&D group MITRE maintains the MITRE ATT&CK cybersecurity framework (and related Shield framework. This framework supports cybersecurity by helping teams structure security practices like penetration testing and threat modeling.

MITER ATT&CK divides the cyber attack lifecycle into 14 phases called tactics. Each tactic covers a specific sub-goal within the overall attack—for example, account compromise and privilege escalation.

MITRE ATT&CK is not an exhaustive list of all potential attack techniques, but it covers an impressive range of threats and offers clear criteria to identify vulnerabilities.

OWASP Top 10

The Open Web Application Security Project maintains the OWASP Top 10, which focuses on common vulnerabilities in web applications. The group periodically updates the list to reflect the most relevant vulnerabilities and unsafe practices.

The OWASP Top 10 list offers a useful reference for web application development teams to conduct threat modeling exercises. Cybercriminals also use the list as a starting point to identify easy targets.

While OWASP focuses on web app vulnerabilities, it is also relevant for developing other software like blockchain apps.

STRIDE

STRIDE is a Microsoft framework that focuses on the impact of various threats, including spoofing, tampering, repudiation, data leaking, privilege escalation, and denial of service. It helps temps identify potential attack vectors, assess their impact and risk, and establish mitigation measures.

DREAD

DREAD is an add-on to STRIDE that helps threat modelers rank threats after identifying them. DREAD is an acronym for the considerations for understanding threats:

- Damage
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Each criterion receives a score from one to three.

PASTA

The Process for Attack Simulation and Threat Analysis (PASTA) describes seven steps to match cybersecurity policies to business objectives. These steps are complex and include substeps

- Defining objectives
- Defining scope
- Decomposing the application
- Analyzing threats
- Analyzing vulnerabilities
- Modeling attacks
- Analyzing risk and impact

TRIKE

Trike is an open source threat modeling and risk evaluation tool and framework. It identifies threats from a defensive perspective by modeling the protected system and identifying who can read, create, edit, or delete each entity. It focuses on two threat types: privilege escalation and denial of service.

VAST

Visual, Agile, Simple Threat Modeling (VAST) is the underlying framework of the automated ThreatModeler platform. It integrates into DevOps workflows and focuses on automation and collaboration to support scalable threat modeling solutions.

OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology focuses on organizational risks (as opposed to technical vulnerabilities). It involves building threat profiles, identifying infrastructural weaknesses, and establishing security measures.

NIST

The National Institute of Standards and Technology offers a threat modeling methodology focusing on data security. It includes the following steps:

- Identifying the data assets of interest.
- Identifying attack vectors.
- Characterizing security controls to mitigate the threats.
- Analyzing the model.