Threat Modeling Checklist

Step-by-step STRIDE threat modeling process

Phase 1: Preparation

- ■ Define scope and objectives of the threat model
- ■ Identify system stakeholders and schedule workshop
- ■ Gather architecture documentation and data flow diagrams
- ■ Identify data classifications for all data in scope
- ■ Select threat modeling methodology (STRIDE, PASTA, LINDDUN)

Phase 2: Decomposition

- ■ Create/update Data Flow Diagram (DFD) Level 0 and Level 1
- ■ Identify all entry points and exit points
- ■ Mark trust boundaries on the DFD
- ■ Document assets and their sensitivity levels
- ■ Identify external dependencies and third-party integrations

Phase 3: Threat Identification (STRIDE)

- ■ Spoofing — Can identities be faked at trust boundaries?
- ■ Tampering — Can data in transit or at rest be modified?
- ■ Repudiation — Can actions be denied without audit trail?
- ■ Information Disclosure — Can sensitive data leak?
- ■ Denial of Service — Can availability be impacted?
- ■ Elevation of Privilege — Can users exceed their authorization?

Phase 4: Mitigation & Documentation

- ■ Rate each threat using DREAD or CVSS scoring
- ■ Define mitigation strategy for each identified threat
- ■ Create tracking tickets for unmitigated threats
- ■ Document threat model and store with project artifacts
- ■ Schedule review cadence (per sprint or per release)