What is threat modelling, and how can a development team start?

20 November 2026 · 4 min read · blogs.iictp.org/what-is-threat-modeling

Threat modelling is a structured way of asking what could go wrong with a system’s security before it happens, and deciding what to do about it. It works best as a short, regular team conversation during design, not as a large document produced once.

TL;DR The short version

- Threat modelling asks what could go wrong with a system's security before it happens, best as a short, regular team conversation.
- Draw a simple data flow diagram, then use STRIDE's six prompts to find threats.
- For each threat decide to mitigate, remove, transfer or accept it with an owner, and repeat whenever a change moves a trust boundary.

Read online, listen to it, or change the text size: https://blogs.iictp.org/what-is-threat-modeling

What questions does it answer?

Adam Shostack frames it as four questions: What are we working on? What can go wrong? What are we going to do about it? Did we do a good enough job? The Threat Modeling Manifesto uses the same four questions.

How do you describe what you are working on?

Draw a simple data flow diagram: the people and systems involved, the processes, the data stores, and the flows between them. Mark trust boundaries, the places where data crosses from something you control to something you do not, such as the internet, a third-party API or another team’s service. Most threats sit on those boundaries.

How do you find what can go wrong?

STRIDE, developed at Microsoft, gives six prompts: spoofing identity, tampering with data, repudiation, information disclosure, denial of service and elevation of privilege. Walk each flow that crosses a trust boundary and ask which of the six apply.

What do you do with the threats you find?

For each one, decide to mitigate it, remove the feature that creates it, transfer it, or accept it with a named owner. Turn mitigations into tickets in the normal backlog, so they are tracked like other work, and record accepted risks so they are revisited.

When should a team do it?

When designing a new feature or service, and when a change moves a trust boundary: a new external integration, a new kind of user, new sensitive data. An hour with the right people and a whiteboard is often enough. It pairs well with DevSecOps and the OWASP Top 10.

> Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. Shostack, A. Threat Modeling: Designing for Security. Wiley, 2014.
2. Threat Modeling Manifesto. threatmodelingmanifesto.org, 2020.
3. OWASP. Threat Modeling Cheat Sheet. cheatsheetseries.owasp.org.

Published by IICTP, an independent technical credential body, on 20 November 2026. The current version of this post is at https://blogs.iictp.org/what-is-threat-modeling. More guides: blogs.iictp.org.