THE WORKSHOP

Threat Modelling

Walk a system's architecture with a deliberately hostile eye, using STRIDE as a systematic prompt, so ways the system could be abused become visible and rateable before they become incidents.

DURATION

2

hours

GROUP SIZE

—

people

WHAT YOU BRING

A system diagram on a wall (whiteboard-level is fine), sticky notes, dot stickers, and a STRIDE reference sheet.

WHAT YOU LEAVE WITH

- A prioritised list of specific, rateable threats by component
- Mitigation ideas matched to the top critical and high threats
- An updated diagram showing real trust boundaries and data flows
- Backlog-ready items with owners, severities, and accepted-risk notes

WHO TO INVITE

- **Facilitator.** Holds the hostile frame, enforces systematic STRIDE coverage, stops defensiveness and category-skipping.
- **Developers who know the architecture.** At least two; they know how data moves, which components exist, and where the real weak points are.
- **Operations / SRE.** Know real deployment, network boundaries, and where secrets live; lead when the change is infrastructural.
- **Product owner.** Knows which data matters and the real-world impact of a breach, so severity ratings reflect subscriber harm.
- **Security specialist (optional).** Speeds the session and catches what non-specialists miss; STRIDE compensates if they aren't available.

USE WHEN

Designing a new system, feature, or integration touching sensitive data

Adding a new API, webhook, third-party service, or data source

Exposing something to a new class of user (internal to external, single to multi-tenant)

An SRE team is deploying a new service or changing a trust boundary

AVOID WHEN

Nothing material has changed since the last threat model for this scope

The system has no external interfaces and handles no sensitive data

Nobody in the room actually knows how the system works today

Key participants take findings personally or will shut down inconvenient ones

THE WORKSHOP · THREAT MODELLING

How the session runs

Phase 1 — Scope framing, diagram review (15 min)

Write the scope at the top of the wall diagram and walk each component confirming data, access, auth, and trust boundaries. Correct the diagram against reality and mark boundary crossings in a distinct colour.

Phase 2 — Identify threats with STRIDE (45 min)

Announce the switch from defending to attacking, then apply all six STRIDE categories to each important component. Capture specific, concrete threats on sticky notes placed next to the component they target.

Phase 3 — Break (10 min)

Take a genuine break away from the wall. The hostile framing is cognitively draining and the severity phase needs fresh minds.

Phase 4 — Rate severity (20 min)

For each threat, take a quick show-of-hands on likelihood and impact, read the severity grid, and mark the note. Move fast, force-rank when everything looks critical, and park genuine splits with a question mark.

Phase 5 — Identify mitigations (15 min)

For high and critical threats, brainstorm the simplest technical, process, or monitoring mitigation and place it on a different-coloured sticky next to the threat. Capture the seed of a backlog item, not the full fix.

Phase 6 — Wrap-up, owners, next steps (15 min)

Assign an owner's name to each top mitigation, decide what lands in the backlog this week, and document any explicitly accepted risks so they aren't quietly forgotten.