Threat Modeling 101

Map assets, adversaries, and attack paths to prioritized controls; align mitigations to realistic failure modes.

- Inventory of assets (keys, devices, backups, people).
- List of adversaries and capabilities (theft, coercion, malware, insider).
- Risk appetite and budget.

1) Enumerate assets and trust boundaries; draw data■flow diagrams.

2) Identify failure modes: theft, loss, disclosure, corruption, coercion.

3) Score impact × likelihood; pick top risks to mitigate.

4) Align controls: multisig, site separation, PSBT, training, audits.

5) Define metrics and triggers to review the model regularly.

- Don’t overfit to exotic risks; fix the basics first.
- Beware correlated risks (same vendor/site); diversify intentionally.
- Document assumptions; stale assumptions are risk.

- Diagramming tool; checklist templates
- **Nunchuk** for multisig policy expression
- **Coldcard** for constrained signing surface

Quarterly review or after material changes (AUM, team, jurisdiction, devices).