SECURITY · TEMPLATE

A *Pragmatic* Threat Model for Regulated SMBs

KAANSYSTEMS.COM/LIBRARY/PRAGMATIC-THREAT-MODEL · MAY 30, 2026

ABOUT THIS TEMPLATE

Most threat-modeling guides target big tech. Regulated SMBs face a different attacker mix and need a different model. The one-page version.

THE TEMPLATE

The one-page threat model for an SMB system or feature looks like this. Fill it in for any new system before launch, and re-review annually.

System / feature: _____

Owner: _____

Data sensitivity: ☐ Regulated (PHI / PII / PCI) ☐ Confidential ☐ Internal ☐ Public

Spoofing threats

- Primary scenario: _____
- Existing mitigation: _____
- Residual risk (1-5): ____

Tampering threats

- Primary scenario: _____
- Existing mitigation: _____
- Residual risk (1-5): ____

Information disclosure threats

- Primary scenario: _____
- Existing mitigation: _____

- Residual risk (1-5): ____

Aggregate risk score: ____ / 15

Risk acceptance: Above 9 → don't launch. 7-9 → launch with documented mitigation plan + 90-day review. Below 7 → launch.

Notes / open questions: _____

Sign-off: _____ Date: _____

Three categories, one page, scored honestly. The model takes 30 minutes to fill in for a new system, surfaces the threats that matter, and gives leadership a defensible record of what was considered before launch.

WHAT THIS BUYS YOU

Two things.

First, the security program becomes legible. When a customer, an auditor, or a board member asks "how do you think about security?", you have a structured answer that doesn't hand-wave. The answer is "we threat-model every new system, here's the template, here are the last six completed models."

Second, the team stops doing security theater. No more two-hour threat-modeling sessions for a feature that ships in a week. No more 200-question threat assessments that nobody reads. One page, three categories, ship.

The first time the model surfaces a real risk, and it will, the model has paid for itself.