**OPS-09 — Threat Modeling & Secure Design Review (STRIDE before GA)**

**Intent**  
Identify and mitigate security threats across Partner Store + integrations **before** GA, with tracked residual risk.

**Preconditions**

* System context diagram (Partner Store, Screening, Gate, Webhooks, Provider Feeds).
* Data classification (PII, tokens, keys) documented.

**Flow (happy path)**

1. **Decompose**: map trust boundaries (tenant UI, APIs, event bus, storage, KMS).
2. **STRIDE workshops** per boundary (Spoofing, Tampering, Repudiation, Info disclosure, DoS, Elevation).
3. **Threat register**: for each threat → likelihood/impact, owner, mitigation, target date.
4. **Design review**: update designs (authN, authZ, token scope, request signing, replay protection, rate limits, isolation).
5. **Abuse cases**: define and test “merge abuse”, “bulk spam”, “webhook replay”, “PII exfil”.
6. **Residual risk**: document anything accepted with justification; get sign-off.
7. **Verification**: add checks into CI (lint for insecure headers, missing auth, missing audit write).

**Edge cases**

* Multi-tenant leakage risks → add isolation tests.
* Third-party connectors → contractual & technical mitigations (timeouts, sandboxing).

**Done when**

* Threat register closed or accepted; design diffs merged; abuse cases in regression suite; sign-off stored in Audit Vault.