Isaac Teague Frayling

AI-native builder · systems design + AI orchestration

Cardiff, UK · UK citizen, open to relocate worldwide · isaac@pantheonlabs.co.uk · pantheonlabs.co.uk

I design systems from first principles and direct AI to build them. I conceived and shipped **PANTHEON** — a governed, multi-tenant AI-agent platform — to production, solo: the substrate, a no-code product on top, and the adversarial audit that hardened it. I don't hand-write code; what I bring is the systems thinking (multi-tenant isolation, a governed agent loop, atomic metering, failure-mode design) and the discipline to make AI-built systems actually hold. Built alongside full-time work outside software. Looking for a founding-builder, 0-to-1, or AI-native role where output and systems judgment beat pedigree.

HOW I BUILD

What I do	Design systems from first principles → decompose into buildable pieces → direct AI to implement → adversarially verify → ship and run in production
Concepts I command	Multi-tenant isolation & trust boundaries, governance tiers & human-in-the-loop, atomic metering & rate control, agent loops / tools / guardrails, prompt-injection defence, failure-mode & blast-radius thinking
Systems I've shipped	Postgres with row-level security, FastAPI services, a governed agent loop, MCP (both directions), React frontends, Docker / nginx deploys — directed the build, understand each end-to-end, don't hand-write the syntax
Keeping AI honest	CI purity boundaries, golden-file snapshot tests, 799 tests green, 80-agent adversarial audits where every finding is refuted before it counts

PANTHEON — CREATOR, SOLO

Governed multi-tenant AI-agent platform · designed the system, directed the build

Dec 2025 – present

Live in production · pantheonlabs.info & pantheonlabs.co.uk

- **Isolation that survives composition** — I designed strict multi-tenant isolation on Postgres row-level security (two-role, `FORCE` + `NOBYPASSRLS`): a shared tool called by tenant B runs under B's scope, never the owner's. An 80-agent adversarial audit couldn't cross it.
- **A governed agent loop, not prompt-glue** — my design: perceive → knowledge → tools → judge → meter, with guardrails, a crisis protocol, overdraft-proof atomic metering, and human-approval gates for consequential (tier-3) actions.
- **A no-code Studio product** — turns a sentence into a themed, customisable website with bespoke generative art and a governed assistant live on web, WhatsApp and Telegram. Idea to production, solo.
- **Adversarial quality discipline** — an 80-agent, 14-facet self-run audit where every finding was refuted before it counted, then fixed; 799 tests; a golden-file snapshot harness; an undoable edit ledger.

SELECTED PROBLEMS I SOLVED

- Diagnosed and killed a quadratic JSON-LD import DoS — a crafted 2 MB page froze the gateway for 70s; redesigned to a bounded linear scan, **70s → 4ms**.
- Designed overdraft-proof metering via atomic check-and-decrement (`UPDATE … SET credits = credits - n WHERE credits >= n`); a turn deflected to a crisis resource is refunded.
- Made safety beat the metric — a person in crisis reaches help even at zero credits, because the crisis check runs before billing on every surface.

BACKGROUND

Self-taught — no CS degree, and I don't write code by hand; I design systems and direct AI to build them, and the live, attackable system is the qualification. PANTHEON was designed and built in evenings and weekends alongside full-time work outside software (most recently as a care worker). Available on request: a live walkthrough of the running system, a code review under NDA, and references.