

Tal Onn Sella

Agentsmith — AI agent systems & MCP servers

Haifa, Israel · tal.onn.sella@gmail.com · agentsmith.team · ask my resume directly: claude mcp add agentsmith https://mcp.agentsmith.team

WHAT I DO

I design and ship AI agent systems and MCP servers that run in production — including against my own money. Agent setups, Model Context Protocol servers, and the guardrail architecture that makes autonomous systems safe to trust: approval gates, circuit breakers, signed callbacks, budget caps. Invoices in USDT or fiat.

SELECTED WORK

Voluum MCP server + 11-agent operations layer 2025–present

Production system running my own affiliate operation.

- **43 MCP tools** across 9 categories (campaigns, A/B path optimization, offers, landers, traffic sources, reporting, conversions, affiliate networks, live KPI beacons) — Python, FastMCP 2
- **11-agent DSPy orchestration layer:** task decomposition, write-approval gate (no agent spends money without a signed-off human), circuit breaker, per-source rate limiters, HMAC-signed Telegram approvals
- **293 automated tests;** resilient API client (401 auto-refresh, exponential backoff); TTL caching
- Deployed hardened (systemd + nginx), live SSE dashboards, running against real ad spend today

Agentsmith Inc. 2022–2024, Delaware

Founded an AI company building an agent studio for non-technical creatives — before the GPT moment made "agents" a category. Platform built; smithing services had paying customers. Wrote *The Agentsmith's Code*: "An Agentsmith makes support systems for humans, not replacements for them." Trademark retained; demonym open-sourced.

Nester ongoing

Founder. Mobile-first apartment rental platform for the Israeli market with native roommate compatibility matching.

STACK

- **AI/agents:** MCP protocol design (client + server), DSPy, agent orchestration, prompt architecture, guardrail systems
- **Languages:** Python (FastMCP, httpx, pydantic, Starlette), TypeScript (Cloudflare Workers, Astro), SQL/Cypher
- **Infrastructure:** Cloudflare (Workers, Pages), Neo4j, Redis, systemd/nginx, Telegram integrations
- **Before the agents:** 12 years across copywriting, design, web development, marketing automation, and crypto — in that order. Each layer feeds the next.

TIMELINE

- Age 12: first bots (mIRC). Nobody called them agents yet.
- 2013–2022: copywriting → design → web dev → marketing automation → crypto
- 2022–2024: Agentsmith Inc. — first AI company, agent studio, the Code

- 2022–present: building AI agent systems, four years and counting
- 2025–present: production MCP tooling against live ad spend

The 15-minute call: you bring the operation. You leave knowing exactly what AI can — and cannot — do for your business, and the trajectory to get it done.

<https://agentsmith.team/call>