

Daniel Farina

Forward Deployed / Applied AI Engineer · Solutions Architect

Washington, DC (Remote) | elchileno@gmail.com | danielarina.com | github.com/daniel-farina | x.com/Daniel_Farinax

Product engineer and public builder with **10+ years** shipping production systems, now building **on top of and inside the LLM stack**: a sandboxed computer-use agent, an AI-native browser fork, agent terminals and gateways, coding agents, MCP servers, and eval tooling. **146 public repos** and a continuous release cadence across Rust, C++, TypeScript, and Swift. Background spans Fortune 100 platforms serving **10M+ customers** and 0-to-1 startup engineering, plus security research recognized by the DoD.

SELECTED PROJECTS — all public at github.com/daniel-farina

Sub8 — sandboxed computer-use agent (desktop app) sub8.grok.me · 2026

- Desktop product that gives each agent its **own private Linux desktop** in a container, so it never touches the user's files, browser, or machine. The agent sees the screen and drives mouse and keyboard the way a person does.
- **Model-agnostic harness layer**: runs the same task against Claude, Codex, Grok, or local models via Ollama and LM Studio, making harness and model behavior directly comparable.
- Built the safety and control surface that computer-use actually requires: **view-only by default with one-click human takeover**, a credential vault that injects logins per bot so secrets never enter the transcript, and scheduled standing routines for recurring work.
- Ships on macOS, Windows, and Linux on a continuous release cadence (v0.3.19, Aug 2026).

Xplor — AI-native Chromium fork (C++) xplor.sh · 77★

- Forked Chromium and integrated an LLM **at the source level** (model-backed default search, per-page "ask about this", unified agent toolbar) rather than bolting on an extension.
- Ships an **always-on local agent gateway** exposing both Chrome DevTools Protocol and a higher-level API, so any external agent can drive the browser. 11 forks; cross-platform and free.

grok-remote — remote agent control plane (TypeScript) 53★

- Runs coding agents on one machine and drives them from any device on a tailnet. Live web UI speaking the **Agent Client Protocol directly to agent stdio**, with session state surviving disconnects. 14 forks.

GrokTerm & SwitchKit — agent hosting and transport (Rust) grokterm.com

- **GrokTerm**: multi-tab PTY terminal host purpose-built for coding agents, with two-way voice; shipped as a notarized macOS app. **SwitchKit**: connects any local agent (Codex, Claude, Grok, Hermes) to any website through one transport layer.

Agent harnesses, evals & observability 2025 - Present

- **hip**: a lean coding agent built from scratch against a self-hosted MLX inference server. Designed the auto-compaction strategy against measured cache behavior (threshold tuning, round caps, tail budgets) to keep long sessions coherent and cheap; ported to TypeScript to compare runtime and DX tradeoffs.
- **grok-bench**: test bench for tuning agent generation settings via a rewriting proxy and versioned system-prompt control. **grokscope** and **hipdash**: live observability dashboards with per-request metric history and benchmark runs.
- **ai-session-manager** (14★): browse, search, and resume local sessions across Claude Code, Codex, Grok, and opencode. **grok-build-system-prompts**: versioned archive of a frontier agent's system prompt, diffed per release.
- Built a repeatable long-context diagnostic isolating hallucination and malformed-tool-call regressions into distinct root causes (paged attention, dense fallback, speculative draft drop); contributed fixes upstream to the serving runtime.

browser-pilot & Argus — MCP and security tooling 2026

- **browser-pilot**: MCP server plus Chrome extension giving agents control of Chrome over the DevTools Protocol; validated against local open-weight models.
- **Argus** (Rust + Tauri): real-time supply-chain guard for developer machines that blocks malicious npm postinstall scripts and fake-interview malware.

EXPERIENCE

DevOps Engineer & Solutions Architect, Exelon Corporation

2019 - Present

Fortune 100 energy company · Remote · Platforms serving 10M+ customers

- Led enterprise-wide migration from Azure DevOps to GitHub Enterprise: **36+ repositories**, pipeline redesign, access control model, and org-wide developer onboarding.
- Designed CI/CD and DevSecOps strategy (Dependabot, code scanning, workload identity federation, secrets management) for platforms serving **10M+ utility customers**.
- Drove AI adoption across engineering teams: introduced AI-assisted code generation, automated documentation, and agent-accelerated workflows, and trained engineers on where the tools fail as well as where they win. Co-architected Exelon's first online marketplace spanning multiple utility subsidiaries.

AI Solutions Consultant, Mitosis Labs

2024

Remote

- Designed and implemented LLM-powered developer workflows: agents for CI tooling, code review automation, and documentation generation.
- Owned AI adoption strategy end to end: evaluated models, built internal tooling, and trained engineering teams on AI-first development practices. Customer-facing from scoping through delivery.

DevRel & Engineering Lead, Osmosis Labs

2020 - 2023

Remote · Cosmos ecosystem, top-10 DEX by volume

- One of the earliest engineers post-launch. Built the developer portal and documentation from zero and scaled the engineering and DevRel function around it.
- Onboarded protocols, vendors, and partners across APIs, smart contracts, validator infrastructure, and cross-chain IBC integrations. Effectively a forward deployed role: embedded with external teams to get their integration shipped.

Core Developer & Growth Lead, Bitcoin Private

2017 - 2019

Remote · Open-source blockchain

- Contributed to core protocol development and network operations; led growth strategy for the open-source contributor ecosystem.

Full-Stack Engineer to Project Manager, M3D LLC

2014 - 2019

- Built the full-stack crowdfunding and fulfillment platform behind one of the largest 3D printing campaigns ever run, handling millions in pre-orders. Promoted to PM and worked directly with the CEO on product strategy.

SELECTED RECOGNITION

- **Researcher of the Month, DoD Cyber Crime Center (DC3) Vulnerability Disclosure Program** (March 2026). Recognized by the VDP Director for identifying two critical vulnerabilities in a Department of Defense system.
- **3rd place and Most Users award, SpaceXAI Grokathon** (August 2026). Built ThinkVoice, a speech interface combining voice models with brain-sensing input for conversation understanding, next-line suggestion, and selection via subtle motor movements.
- **AI-generated 3D games and procedural experiences** (2025-2026). Among the first to build playable 3D games generated with frontier models; posts repeatedly amplified by Elon Musk, **100M+ cumulative views**.

SKILLS

AI / Agents: computer-use agents and sandboxing, agent harness design, tool-call loops, context compaction, MCP servers, Chrome DevTools Protocol, Agent Client Protocol, evals and benchmarking, system-prompt engineering, local inference serving (MLX, Ollama, LM Studio). Daily production user of Claude Code, Codex, and Cursor.

Languages: TypeScript, Rust, Python, C++, Swift, JavaScript, C, Kotlin, Solidity, SQL, Bash

Systems & Product: Chromium internals, Tauri, native macOS app delivery and notarization, Node.js, React, Next.js, REST and GraphQL APIs, Postgres, Docker, distributed systems

Infrastructure & Security: Azure, GCP, Terraform, GitHub Actions, CI/CD, DevSecOps, Linux, vulnerability research and disclosure

BEFORE THE CAREER

Started writing software at 11. At 15, published one of the first games on the PalmOS app store, years before the iPhone. In high school, built a social platform that reached **150,000 concurrent users**.