

Pete Stergion

Builder. Twenty years in higher education IT. Ships production tools with Claude every day.

Ithaca, NY · github.com/pete-builds · stack.brooksnewmedia.com · linkedin.com/in/pete-builds

Runs a private cluster of about thirty specialized Claude agents against a self-hosted production stack he operates himself. The work spans MCP servers, agentic workflows, and web applications, shipped from a single daily loop: notice a friction, prototype a fix in a weekend, wrap it in a verification pass, ship it, watch how it gets used, iterate. Twenty-plus public repositories on GitHub, several adopted by engineers he has never met.

SELECTED SIDE QUESTS

Each of these started from something he or the people around him were already trying to do. None were assigned.

mcp-unifi (16 stars). Safety-first Model Context Protocol server for self-hosted UniFi networks. 86 tools across Network, Protect, and Access, with dry-run previews, a JSONL audit log, composite rollback, and per-client tool scoping. Started as a spec-first build before the UCG-Fiber hardware arrived, so the full API surface was already exercised in stub mode when the box shipped. Public since v0.15 and hardened over three months of security review, release CI, and IPv6 tooling after real users began filing issues.

github.com/pete-builds/mcp-unifi

strava-mcp-vault (10 stars). Strava MCP server with SQLite caching, automatic token refresh, and rate-limit awareness. Everyone rebuilding Strava tooling was hitting the same authentication quirks; this solves them once, in the open.

github.com/pete-builds/strava-mcp-vault

pete-mcp-core. Extracted after nine MCP servers were built independently and started duplicating the same handful of modules: structured logging, transport wiring, bearer-token authentication, tool-error decoration. One shared substrate now feeds the whole pete-builds fleet, and the fleet is being ported over to it.

github.com/pete-builds/pete-mcp-core

agent-desk. Human-in-the-loop approval board for agent-proposed changes. An agent proposes a change, a human accepts or rejects, the verdict lands in an append-only audit table. Built as the working portfolio piece for a Cornell senior application developer requisition, and shipped as a usable tool.

github.com/pete-builds/agent-desk

claude-research-agent + research-reports. A Claude Code skill that runs deep research with anti-hallucination rules built in: every claim cited, standard and full verification modes, priority-ranked under a fetch budget. The verify pass confirms cited URLs are live and actually support the claim attached to them. Reports live in a public repository so the source pack is inspectable.

github.com/pete-builds/claude-research-agent, github.com/pete-builds/research-reports

mcp-nixreview. Advisory security review and CVE/KEV attestation gate for NixOS configuration changes, exposed as an MCP server. Grades security-relevant diffs against the CISA Known Exploited Vulnerabilities catalog, gates on a human, and keeps an append-only ledger. Same audit-log and human-gate pattern that shows up in mcp-unifi and agent-desk, applied to system configuration.

github.com/pete-builds/mcp-nixreview

mcp-phish, open-setlist-stash, mcp-umphreys. A Phish.net and Phish.in data vault with a phased vault/live/cache design, plus an open-source, self-hostable setlist-prediction game that any band can point at its own MCP server. Live during Phish tour: real-time setlist ingest during the show, guesses scored live. The Umphrey's McGee tenant (mcp-umphreys, wappypicks) proves the multi-tenant story runs in production, not on paper.

github.com/pete-builds/mcp-phish · github.com/pete-builds/open-setlist-stash · github.com/pete-builds/mcp-umphreys

claude-code-statusline (4 stars). Labeled-row status bar for the Claude Code terminal UI: context usage, billing tier, git status, weather, session metrics. Small tool with real adoption from other engineers who run Claude Code all day.

github.com/pete-builds/claude-code-statusline

open-model-arena (3 stars). Blind model comparison arena with an ELO leaderboard. Built for Cornell's AI Hub to give faculty an evidence-based way to choose between models without preloaded assumptions.

github.com/pete-builds/open-model-arena

LiteLLM PyPI supply-chain investigation. Self-initiated security research after spotting a suspicious release. Traced the compromise, documented the payload path, published the report publicly. Not a job function; done because it was worth doing.

github.com/pete-builds/research-reports/blob/main/litellm-pypi-supply-chain-attack.md

ai-upskill-playbook (7 stars). Public map of the AI application stack worth learning in 2026, written for IT professionals coming up the curve.

github.com/pete-builds/ai-upskill-playbook

RECENT OPEN SOURCE CONTRIBUTIONS

- **phishnet/api-v5** PR #3: Phish.net API fixes. Opened as a relationship-first contribution to the maintainer.
- **jcraigk/phishin** PR #467: fixes to the Phish live-audience archive.
- **mattypiper/umtabs** PR #27: Umphrey's McGee tablature community contribution.

EXPERIENCE

Cornell University · 7 yrs 11 mos

Technical Lead, AI Innovation Hub (Cornell AI Program)

Jan 2026 – Present · Concurrent appointment · Ithaca, NY · Hybrid

One of the technical leads in Cornell's central AI program.

- **Built the Cornell Search MCP server** (in-house integration service, cu-aaii.org) that gives Cornell AI tooling a compliant web-search capability.
- **Engineered the Cornell-wide Claude Desktop deployment proof of concept** and the packaging requirements the Endpoint Infrastructure and Engineering team builds from, for Windows and Mac. Two-package model separates standard from restricted access; per-user credential distribution.
- **Wrote the cross-platform gateway credential helper:** two pluggable backends, an OS credential store bridge and a browser-based OIDC path with RFC 8252 loopback, CSRF state validation, bounded callback timeout, keychain token cache.
- **Co-led the Cornell Treasury unidentified-payments recovery project.** A Python pipeline fuzzy-matches incoming payments against three years of General Ledger history (9,131 resolved records), researches unknown vendors through the Cornell AI Gateway, and returns a ranked recommendation with confidence and a contact to email. The first production batch recovered **\$100,000** against a roughly \$1 million backlog, and replaced about half the workday of two non-technical staff members who still confirm every action before it is applied.

- **Validated the pipeline with holdout backtesting** on the full 9,131-record dataset. When the first version's aggregate metrics hid a real weakness on vendors who pay multiple departments, rebuilt the backtest and reported the limitation to Treasury rather than the headline number. Hardened for production: circuit breakers, per-call timeouts, rate limiting, cost tracking, PII stripped at the parse step.
- **Designed a web-search integration on Cornell's n8n** instance, distributed to Claude clients through the LiteLLM gateway's managed MCP servers. Per-user gateway key auth, no shared master credential, inbound-secret gated, model pinned server-side.
- **Mentors student engineering teams weekly** and teaches AI-assisted development practices as the program adopts them.

Desktop Engineer and Security Liaison, Cornell University Library

Oct 2023 – Present · Full-time · Ithaca, NY · Hybrid

Engineering and automation for Library Computing and AV Services. Library's security liaison to Cornell's central IT Security Office.

- PowerShell automation for endpoint management, deployment, configuration, and compliance reporting.
- Security Liaison to ITSO: vulnerability remediation, compliance coordination, emerging-risk response.
- Vendor and service owner for the Library's Springshare SaaS platform, three years running.
- Designs and delivers the annual Cybersecurity Awareness presentation, translating technical security concepts for a non-technical audience.

Desktop Engineer, Central IT

Aug 2018 – Oct 2023 · Tompkins County, NY · Full-time

- PowerShell and SCCM automation for deployment, patching, and configuration across Cornell's distributed technical service provider environment.
- Partnered with the CIT Security Office on the campus-wide **Secure Connect** (Beyond Identity) rollout: packaging, deployment, configuration, automated updates for Mac and PC.
- Led development of the **Windows 11 task sequence** used by Cornell's technical service providers.

Buffalo State University

Client Systems Engineer

Jul 2006 – Jul 2018 · 12 yrs 1 mo · Buffalo-Niagara Falls Area

- Lead for software packaging and campus-wide distribution on a three-person team supporting the full institution.
- Implemented a BitLocker encryption workflow at scale, including key escrow and recovery.
- Configured and maintained license servers, including firewall configuration and troubleshooting.
- Secondary macOS administrator on Jamf in a multi-platform environment.

Brooks New Media

Founder

2011 – Present · Part-time · Ithaca, NY

Part-time web services practice for small businesses, festivals, and tourism organizations. Fifteen years of client-facing technical work. Now runs on the same self-hosted infrastructure, with Claude agents handling most of the routine work: audits, deploys, monitoring, publishing.

WRITING AND PUBLICATIONS

- **The Stack** (stack.brooksnewmedia.com): a public build log. Each post is written from inside a Claude session on whatever shipped that day.

- **The 53 Report** (the53report.com): NFL analysis site with an editorial pipeline built on four sub-agents (Coach, Scout, Beat, Editor). Editor blocks the publish path on any fabricated stat.
- **LinkedIn**: builder-voice essays on agentic development. Most recent long-form: "How I Built a Research Agent That Doesn't Hallucinate."

SKILLS

AI and agents

Claude Code as daily driver · multi-agent orchestration · MCP protocol design and implementation with FastMCP · prompt and context engineering · evaluation frameworks for repeated agent workflows

Infrastructure

Docker and Docker Compose · NixOS · Ubuntu · Linux server administration · reverse proxying · self-hosted LLM inference · observability stack (Prometheus, Loki, Grafana, Promtail, Alertmanager)

Languages

Python · TypeScript · Bash · PowerShell · working knowledge of Go and Node.js

Enterprise

SCCM · Jamf Pro · Active Directory · Microsoft Entra · Tenable Nessus · vulnerability triage and CISA KEV correlation · vendor management · cross-team delivery

PROFESSIONAL DEVELOPMENT | CORNELL UNIVERSITY

Turning Point, 5-day leadership development program for front-line staff focused on individual effectiveness and Cornell leadership culture

Developing Facilitation Skills (DFS), 5-day program covering facilitation of meetings, project teams, workshops, and learning initiatives (*prerequisite: Turning Point*)

EDUCATION

Medaille University

Bachelor of Business Administration (B.B.A.)