Alexander Sorrell

AI Principal / Builder / Breaker — Verification & Evaluation · (817) 996-6123 · alexander.sorrell.it@gmail.com

linkedin.com/in/alexander-sorrell-it · github.com/Alexander-Sorrell-IT

Colleyville, TX (Dallas–Fort Worth) — open to remote, onsite, or relocation

github.com/Alexander-Sorrell-IT/starreckon
npx starreckon

VERIFIED AUDIT · 30.1 MASTERWORK

PROFESSIONAL SUMMARY

Models propose. A deterministic function owns the verdict. Every decision ships with a receipt a stranger can re-check — a rule ID, a cryptographic hash chain, or the OS kernel itself.

PROOF OF WORK

- **I broke my own benchmark.** It reported 100%. Its oracles only tested the features each rebuild had already implemented. I rewrote them to grade the full original surface across the same 72 apps — 52.3%, zero fully passing. I kept both numbers on the record and retracted the headline.
- **Calibrated abstention under attack.** I ran live prompt injection against my own forensics court to find out what it does when someone is actively trying to poison the judge. F1 halved. Planted false positives stayed at zero, and every degraded run abstained. It fails silent, not wrong.
- **Two counters, two authors, one answer.** My token counter (starforge) and an independently written one by a different author — different language, no shared code — read the same 20,217 transcripts from 5 computers, each in its own container with the corpus read-only. They agree exactly on sessions, active days, hours, input and cache tokens, and differ by 0.07% on output. The designed failure mode is INCONCLUSIVE, never PASS.
- **The kernel certifies the boundary, not the code.** A socket probe executes inside the sandbox and outside it; the OS returns EPERM rather than relying on an application-level boolean. Reproducible at your desk — npx starreckon prove prints the exact command.
- **Byte-for-byte ground truth.** Clean-room reconstruction of an NVIDIA HGX factory tool's output to an identical md5 against the closed-source Windows original, non-circular by control. Replaying 10 real H100 boards through the rebuilt suite matches the factory's disposition 10/10, and it caught two boards shipped as BBX Pass while carrying 8 row-remaps.
- **The payout function cannot receive an AI verdict.** Re-derives policy deterministically server-side so nothing upstream can trick it into an unauthorized state. 8 of 8 scripted adversarial attacks held, zero violations.
- **Measured, not remembered.** 5 public repositories since August 2026: 13,896 lines, 174 named tests, 73 commits on 19 active days — counted by my own repo auditor, which strips vendored libraries, other people's code and duplicate copies before it counts anything.

ARTIFICIAL INTELLIGENCE & TECHNICAL SKILLS

AI / ML & Eval Science	LLM-as-judge pipelines; golden-set design & contamination control; self-preference bias calibration; principled abstention; adversarial evaluation & red-teaming; multi-agent orchestration; deterministic QA; MCP
Languages	Python, TypeScript / JavaScript, Rust (→ WASM), Solidity, Bash, C
Platforms & Systems	Splunk / SPL, Foundry, Docker, GitHub Actions CI, Linux namespaces (unshare) / sandboxing, PyPI & npm publishing, MCP servers, Next.js / React, Playwright, REST APIs, SDK design
Infrastructure & Security	NVIDIA DGX/HGX A100/H100 bring-up, diagnostics & firmware (retimer, NVSwitch, FPGA registers), Linux, macOS sandbox confinement, smart-contract & web vulnerability analysis, DFIR

PROFESSIONAL EXPERIENCE

Founder & Principal AI Systems Architect — SignalCore Inc (DE) & Bastion Fold LLC (NM) · Remote · 2025 – Present

Verification infrastructure for AI systems: deterministic evaluation harnesses, agent guardrails, and audit trails where the component that decides is physically separate from the component that acts. Multi-agent orchestration, LLM-as-judge pipelines, MCP servers written from scratch, adversarial red-teaming. SignalCore Inc (DE, Jul 2025) builds agent governance; Bastion Fold LLC (NM, Apr 2025) operates deterministic security verification. Shipped 11 packages and 5 public repositories of my own on github.com/matrixbuilderops (73 commits on 19 active days); won the T3 ADK Bounty Challenge Launch Edition with On the Record; one PR merged upstream at KeeperHub. Python, TypeScript, Rust, Solidity.

Frontier-Model Red Team & Evaluation — Handshake AI (Project Vox), Mercor (Les Artistes) & Alignerr · Remote · 2026 contracts

Adversarial prompt red-teaming against frontier models, rubric-based response assessment, reference-answer authoring, and multi-turn reasoning data curation used to harden model alignment and truthfulness. Authored paid ML-environment tasks for Alignerr's ML Envs pipeline.

Server Repair Technician L1 → L2 — OnTrack Staffing, then SMS Infocomm · Jan 2024 – Apr 2025

Ran the full factory sort flow on NVIDIA HGX/DGX A100 and H100 AI-compute systems — system check, BBX, functional stress, in-system run-in — isolating GPU-vs-baseboard faults with golden-part swaps and flashing re-timer and NVSwitch firmware; trained incoming technicians. A sort line is a machine for refusing to believe hardware is good until an independent test agrees. That is the exact discipline I build into evaluation software.

Junior Claims Evaluator — Claimplus · Apr 2021 – Jan 2024

Reviewed and validated property-insurance claims data; structured evaluation workflows and deterministic policy checks.

BY THE NUMBERS (MEASURED ACROSS EVERY PUBLIC REPOSITORY)

- **5 public repositories** of my own on github.com/matrixbuilderops: 13,896 lines, 174 named tests, 73 commits on 19 active days, 2026-08-05 → 2026-10-31.
- **By language:** Python 7,428, JavaScript 3,510, TypeScript 2,958 lines.
- *How it is counted:* bundled libraries, other people's code, generated files and duplicate copies are excluded (0 lines left out); a file in more than one repo counts once; commits count only mine and my agents'.

PROJECTS — EVERY REPOSITORY, WRITTEN FROM ITS DOSSIER

Every system separates the component that proposes from the component that decides. Every public repository of mine with code in it, on github.com/matrixbuilderops (2 written up, 3 small ones listed at the end). Descriptions are each repo's own words or verified write-ups; the Code line is what its biggest source files say they do and the grade its executed checks gave it; lines, tests and commits are measured by repo-dossier, with vendored, generated and duplicate code excluded.

AI EVALUATION, VERIFICATION & RED-TEAMING

groundwork — sitemap-mcp and filelens-mcp give agents structured awareness of sites and files; verifier-mcp, sorrell-engine-mcp and package-telemetry — the tool behind every download number on this résumé. 146 tests. TypeScript, Python

Python 5,735 · JavaScript 3,510 · TypeScript 2,958 lines · 146 tests passing (run) · 47 commits on 14 days (2026-08-13 → 2026-10-31) · NPM sitemap-mcp 1,130 downloads · NPM filelens-mcp 1,124 downloads · NPM verifier-mcp 230 downloads · NPM sorrell-engine-mcp 207 downloads · NPM package-telemetry 1,917 downloads · github.com/matrixbuilderops/groundwork

Code: index.ts: FileLens MCP Server Collapses multiple file-reading tool calls into single structured results · index.ts: SiteMap MCP Server Collapses website exploration into single structured results

Run: get · json · logs · check · profiles · blocks · unblock · never | Built on: @modelcontextprotocol/sdk, zod, websocket, webpipe, pytest, bs4, playwright, trafilatura, pydantic

OTHER WORK

workspace

Python 1,693 lines · 17 commits on 3 days (2026-09-09 → 2026-10-11) · github.com/matrixbuilderops/workspace

Code: nexus_os_corrected.py: The 'Multiplicative' Logic: In a traditional cluster, the 'Sum' is reduced by overhead (network latency, memory copying, context switching)

Run: --demo

Smaller repositories: cad-fea-pipeline, endless-watch, matrixbuilderops.

starforge — Token counter for AI-coding sessions, checked against an independently written counter by a different author: over 20,217 transcripts from 5 computers they agree exactly on every axis but output tokens, where they differ by 0.07%. 4,878 npm downloads (starforge-cli). JavaScript

CONTRIBUTIONS TO OTHER PEOPLE'S REPOSITORIES

- **Open** — claude-builders-bounty/claude-builders-bounty: Add changelog generator script (2026-05-17) · github.com/claude-builders-bounty/claude-builders-bounty/pull/1585

SHIPPED TOOLING & PUBLIC ADOPTION (TELEMETRY VERIFIED)

- **46,179 lifetime downloads** across 11 published packages and 129 releases on PyPI and npm (live, 2026-11-01).
- **PyPI (33,873):** cli-enforcement (10.3k), cli-wikia (9.2k), cli-collective (7.4k), cli-fleet (7.0k).
- **npm (12,306):** starforge-cli (4.9k), starreckon (2.8k), package-telemetry (1.9k), sitemap-mcp (1.1k), filelens-mcp (1.1k), verifier-mcp (0.2k), sorrell-engine-mcp (0.2k).
- *Note:* Gross telemetry includes registry mirrors and CI runs; volunteered as directional proof of real-world usage, not audited human seats.

EDUCATION & CERTIFICATIONS

B.S., Integrative Studies — University of North Texas · 2019 · CompTIA Security+ · Network+ · A+

Alexander Sorrell — Verified Package Telemetry & Live Proof

Identity: Alexander Sorrell (@Alexander-Sorrell-IT) · alexander.sorrell.it@gmail.com · (817) 996-6123

Source: Real-time Registry API query via package_telemetry.py · Executed: 2026-11-01

LIVE TERMINAL TELEMETRY OUTPUT (PACKAGE_TELEMETRY.PY)

```
================================================================================================================================================================
                                                ALEXANDER SORRELL — PACKAGE METRICS & TELEMETRY
================================================================================================================================================================
Type   | Package          | First Rel. | First Date  | Current    | Updated     | Days Live |  Last Day |  Today |  DL / Month |  Lifetime DL
----------------------------------------------------------------------------------------------------------------------------------------------------------------
pip    | cli-enforcement  | v0.1.0     | 2026-06-29  | v0.10.0    | 2026-10-11  |      125d |         6 |      0 |       1,308 |       10,297
pip    | cli-wikia        | v0.10.0    | 2026-06-29  | v0.21.0    | 2026-10-11  |      125d |         6 |      0 |       1,247 |        9,187
pip    | cli-collective   | v0.1.0     | 2026-06-29  | v0.7.0     | 2026-08-29  |      125d |         2 |      0 |         719 |        7,411
pip    | cli-fleet        | v0.1.0     | 2026-06-29  | v0.9.0     | 2026-10-11  |      125d |         5 |      0 |       1,060 |        6,978
----------------------------------------------------------------------------------------------------------------------------------------------------------------
npx    | starforge-cli    | v0.1.0     | 2026-08-07  | v0.14.0    | 2026-08-13  |       86d |         5 |      0 |          67 |        4,878
npx    | sitemap-mcp      | v0.1.0     | 2026-08-13  | v0.7.0     | 2026-08-28  |       80d |         5 |      0 |          37 |        1,130
npx    | filelens-mcp     | v0.1.0     | 2026-08-13  | v0.7.0     | 2026-08-28  |       80d |         0 |      0 |          43 |        1,124
npx    | starreckon       | v0.14.0    | 2026-08-14  | v0.31.0    | 2026-10-11  |       79d |        15 |      0 |         718 |        2,820
npx    | verifier-mcp     | v1.0.0     | 2026-09-04  | v1.0.0     | 2026-09-04  |       58d |         2 |      0 |          31 |          230
npx    | sorrell-engine-mcp | v1.0.0   | 2026-09-04  | v1.0.0     | 2026-09-04  |       58d |         1 |      0 |          22 |          207
npx    | package-telemetry | v1.0.0    | 2026-09-06  | v1.6.0     | 2026-10-11  |       56d |        13 |      0 |         929 |        1,917
================================================================================================================================================================
                                                AVERAGES & SUMMARY
================================================================================================================================================================
Category         |  Packages |  Avg Days Live |  Avg Last Day |  Avg Today |  Avg DL / Month |  Avg Lifetime / Pkg |        Total Lifetime DL
----------------------------------------------------------------------------------------------------------------------------------------------------------------
PyPI (pip)       |    4 pkgs |        125.0d |     4.8 / day |     0.0 / day |     1,083.5 / mo |       8,468.2 / pkg |                33,873
NPM (npx)        |    7 pkgs |         71.0d |     5.9 / day |     0.0 / day |       263.9 / mo |       1,758.0 / pkg |                12,306
----------------------------------------------------------------------------------------------------------------------------------------------------------------
ALL ECOSYSTEM    |   11 pkgs |         90.6d |     5.5 / day |     0.0 / day |       561.9 / mo |       4,198.1 / pkg |                46,179
================================================================================================================================================================


================================================================================================================================================================
                                                PROGRAM DIRECTORY & WHAT THEY DO
================================================================================================================================================================
Type   | Package            | What It Does / Architecture
----------------------------------------------------------------------------------------------------------------------------------------------------------------
pip    | cli-enforcement    | Model-agnostic hook-level behavioral enforcement engine for AI coding agents.
pip    | cli-wikia          | Offline, pip-installable reference wiki & search index for AI CLIs (Claude, Gemini, Copilot, DeepSeek).
pip    | cli-collective     | The Collective bundle: knowledge (cli-wikia) + control (cli-enforcement) + parallel execution (cli-fleet).
pip    | cli-fleet          | Hardware-aware parallel Claude Code agent orchestration via shared filesystem mailboxes.
----------------------------------------------------------------------------------------------------------------------------------------------------------------
npx    | starforge-cli      | Verification CLI auditing AI-coding telemetry with kernel-enforced no-egress proof.
npx    | sitemap-mcp        | MCP server providing website structural awareness without HTML token explosion.
npx    | filelens-mcp       | MCP server for single-call intelligent AST & structural file reading.
npx    | starreckon         | Local-only developer wrapped analyzer for disk logs (Claude Code, Cowork, Codex).
npx    | verifier-mcp       | Deterministic EU e-invoice compliance engine and paradox resolver (DevNetwork 2026).
npx    | sorrell-engine-mcp | Browser-native neural OS & Tiny Model Swarm runtime (OpenAI WebMCP Challenge).
npx    | package-telemetry  | Cross-registry package telemetry engine for tracking PyPI and NPM package metrics, releases, and downloads.
================================================================================================================================================================
Registry Ledger: packages_config.json  •  Canonical Output: package_telemetry_latest.json  •  Scope: PyPI & npm live registries
```

QR CODE TARGET ENGINE & REPRODUCIBLE VERIFICATION (NPX STARRECKON PROVE)

Routing Destination: github.com/Alexander-Sorrell-IT/starreckon · **Package:** npx starreckon

- **Reproducible Sandbox Execution:** npx starreckon prove prints the exact confinement command without running it, so you read the proof before you trust it. The command runs the scan under Apple sandbox-exec (Linux: unshare -rn) with a profile that denies network egress: (version 1) (allow default) (deny network*) (deny network-outbound) (deny network-inbound).
- **Kernel-Enforced Boundary:** The kernel refuses the socket (EPERM), so network egress is blocked below the application, not by an application-level boolean. A timeout is deliberately not counted as blocked.
- **The Central Engineering Thesis:** *The model proposes; deterministic executed checks own the verdict.*

PUBLIC INDEPENDENT VERIFICATION ENDPOINTS (ZERO INSTALL REQUIRED)

Anyone can query public package registries directly via cURL to independently verify these install metrics:

```
# 1. PyPI Verification (pypistats API, no key) — reproduces the PyPI figures above, which include mirrors
curl -s https://pypistats.org/api/packages/cli-enforcement/overall | jq '[.data[]|select(.category=="with_mirrors").downloads]|add'
#    without mirrors, the four PyPI packages total 9,892:
curl -s https://pypistats.org/api/packages/cli-enforcement/overall | jq '[.data[]|select(.category=="without_mirrors").downloads]|add'

# 2. npm Verification (via npm Registry API)
curl -s https://api.npmjs.org/downloads/point/last-month/starreckon | jq .downloads
curl -s https://api.npmjs.org/downloads/range/2020-01-01:2030-12-31/starforge-cli | jq '[.downloads[].downloads]|add'
```