Siddharth Srivastava

Systems & Backend Software Engineer | AI Agent Security

Lucknow, India (UTC+5:30) • +91 9219022881 • sidsri1502@gmail.com • github.com/sidsri14 •

linkedin.com/in/siddharth-srivastava • sidsri14.github.io

EXECUTIVE SUMMARY

Systems and backend software engineer with a proven track record of production-grade open-source contributions (**25 merged upstream PRs** across OpenTelemetry, LiteLLM, Yamale, ClickHouse, and DataDog) and author of **4 specialized cybersecurity & governance linters** (`agentsec`, `toolshield`, `mcpguard`, `flowguard`). Specialized in high-throughput distributed backends, Model Context Protocol (MCP) agent governance, deterministic failure cascades, and static analysis linters in **Go, Python, TypeScript, and Rust**. Maintained 100% test coverage across **107 automated production tests** across 9 repositories.

TECHNICAL SKILLS

Core Languages:	Go, Python, TypeScript, JavaScript, Rust, SQL, Bash
Backend & Distributed:	Node.js, Express, Fastify, aiohttp, RESTful APIs, GraphQL, Model Context Protocol (MCP), SSE/Streaming, WebSockets, BullMQ, Redis, PostgreSQL, Docker, Linux/systemd
AI Agent Security:	Runtime Governance, Pre-debit Token Budget Controls, Tool-Manifest Poisoning Defense, Prompt Injection Mitigation, Static MCP Config Linting, LiteLLM AI Gateway, SARIF 2.1.0
Cloud, CI/CD & DevOps:	GitHub Actions CI/CD (Hardened Commit SHA Pinning, Token Isolation), Docker Compose, AWS, GCP, Nginx, Prometheus Telemetry
Testing & Reliability:	Vitest, Jest, pytest, Node.js native `node:test` runner, Idempotent Workflows, Circuit Breakers, Regression Test Infrastructure

OPEN SOURCE ENGINEERING & SECURITY TOOLING

Upstream Open-Source Core Contributor *• 25 Merged Upstream PRs across Global Projects* GitHub Profile

- **OpenTelemetry Python Contrib:** Authored and landed documentation & pattern standardization for database semantic convention opt-in across 16 database instrumentations (PR #4993) with 416 CI check matrices passing.
- **LiteLLM AI Gateway (BerriAI):** Implemented error-handling and HTTP operation mappings for fine-tuning & batch endpoints (PR #52870); mapped HTTP 403 to `PermissionDeniedError` (#50039).
- **ClickHouse JS Driver:** Implemented Named Tuple support (`TupleParam`) with 70 passing unit tests (PR #1162) and validated DateTime64 precision [0:9] and syntax (PR #1161).
- **Curated AI Governance Index:** Authored `mcpguard`, officially merged and indexed in **awesome-ai-agent-governance** (PR #202) under Claude Code and MCP Governance.

AgentSec — Unified Autonomous Agent Security Scorecard & Meta-Linter *• Author & Maintainer* Repository Live Report

- Engineered zero-dependency security meta-linter evaluating MCP configs (5 rules), tool manifests (7 rules), and GitHub Actions workflows (7 rules) across 19 rules.
- Emits executive letter grades (A+ to F), 0–100 health scores, terminal ASCII tables, JSON, and **SARIF 2.1.0** for GitHub Advanced Security code scanning integration.
- Published drop-in composite GitHub Action (`uses: sidsri14/agentsec@v0.1.0`); dogfooded across 9 workspaces to achieve 100/100 Grade A+ CI security.

ToolShield & FlowGuard — Specialized Security Linters *• Author & Maintainer* ToolShield FlowGuard

- **ToolShield:** Zero-dependency linter for Model Context Protocol (MCP) tool manifests; flags instruction injection, invisible Unicode steganography, and unbounded schemas (14/14 automated tests).
- **FlowGuard:** Static analysis linter for GitHub Actions workflows; detects pwn-requests, unpinned actions, script injection, and token persistence (8/8 automated tests).

FLAGSHIP SYSTEMS & SOFTWARE PROJECTS

Otari Agent Sentinel — Agent Governance & Budget Guardrails *• Systems Architect* GitHub Live Console

- Engineered autonomous agent governance plane on Mozilla Otari Gateway conforming to Open Agentic Web specifications.
- Built pre-debit budget reservation algorithms preventing runaway reflection loops and token exhaustion; implemented circuit-breaker failover cascades routing across semantic tiers with zero agent downtime on HTTP 429 errors.

Cloud9 Fearless Draft & Scouting Engine — Esports Analytics *• Core Developer* GitHub

- Engineered 20-step pro League of Legends draft state machine enforcing mutual lockout Fearless Draft rules in Python 3.12 and async `aiohttp`.
- Indexed 745 pro series and 45 teams from GRID esports data; calculated real-time champion pool depletion and opponent choke-point alerts.

DreamDEX Trading Bot & ERC-4626 Vault Manager *• Protocol Engineer* GitHub

- Built autonomous perpetual trading engine featuring non-custodial session key delegation on Somnia CLOB contracts.
- Integrated ERC-4626 vault compounding 30% protocol trading fees with dynamic collateral rebalancing corridors; verified by 21/21 tests.

EDUCATION

Bachelor of Computer Applications (BCA) — Manipal University Jaipur, India 2024 – 2027 (Expected)