

Michael Cochran

SUMMARY

Senior Systems Engineer & Offensive Cyber Operator. 11+ years federal cyber operations across USCYBERCOM, Combat Mission Teams, and National Mission Teams. Now building production software as a solo Rust engineer — 10 shipped products spanning AI infrastructure, fintech, fraud detection, and SaaS.

EXPERIENCE

The Cochran Block, LLC

Owner & Engineer | Feb 2026 – Present

Solo full-stack Rust engineer building and deploying production systems end to end.

- **Kova** — AI augment engine with distributed node orchestration, local LLM inference, agentic tool loops, and WASM thin client
- **Rogue Repo** — ISO 8583 payment engine with AES-256-GCM encrypted PAN vaulting and append-only ledger
- **WhyYouLying** — Labor fraud detection tool, DoDI 5505.02/03 compliant, built for DoD IG / FBI investigator use cases
- **Oakilydokily** — Client waiver/resume site with interactive WASM mural — first paying client partnership
- **Wowasticker** — Offline-first mobile student goals app with on-device AI dictation, zero cloud
- **Ronin Sites** — Multi-tenant SaaS platform for tattoo shops and artists
- **Approuter** — Central reverse proxy routing all products through Cloudflare tunnel
- **Intake** — Zero-dependency client deployment portal with async webhooks
- **Cochranblock** — Corporate portfolio site with embedded admin panel
- **illbethejudgeofthat** — Pro se custody case builder, email-to-PDF pipeline

Internal tooling: Custom testing framework (Exopack), multi-AI coordination daemon (Railgun), file sync over SSH (Ironhive), source header automation (Header-Writer)

MaxisIQ

Senior Systems Engineer | Sep 2024 – Feb 2026

Mission critical systems for USCYBERCOM Title 10 Operations. Built custom Python tooling for systems survey and automated server service repairs. SSH/Kerberos infrastructure automation.

Two Six Technologies

Senior Software Engineer | Sep 2022 – Sep 2024

Integrations to the Joint Cyber Warfighting Architecture. Built YAML-to-SQL data pipelines, regex parsing engines, and data sanitization tooling.

USCYBERCOM J38, United States Army

Systems Developer | Jun 2020 – Sep 2022

API development, CI/CD pipeline design, data modeling, and network protocol implementation. GitLab, Docker, documentation systems.

Combat Mission Team

Offensive Cyber Operator | Feb 2017 – Jun 2020

Title 10 Offensive Cyber Operator. Executed 100+ operational missions. Built Python automation tooling for mission support.

National Mission Team

Digital Network Exploitation Analyst | Jul 2014 – Feb 2017

Network mapping, traffic analysis, and Intelligence Community reporting.

SKILLS

Languages:	Rust, Python, C, C++, Assembly, Go
Infrastructure:	Tokio, Axum, PostgreSQL, SQLite, sled, Docker, GitLab CI/CD, Cloudflare
Security:	Penetration Testing, DNE, TDNA, AES-256-GCM, Argon2id, HKDF, Kerberos
AI / ML:	Local LLM inference (Kalosm, Candle), RAG (fastembed), agentic tool orchestration
Frontend:	WASM, egui, Dioxus, Vue 3
Domains:	Offensive Cyber Operations, Fintech (ISO 8583), Fraud Detection, Distributed Systems

LINKS

cochranblock.org | oakilydokily.com | roguerepo.io | ronin-sites.pro | github.com/gotEmCoach