

MICHAEL COCHRAN

Dundalk, MD 21222

(443) 900-7903

RESUME · SENIOR SYSTEMS ENGINEER · CLEARED CYBER · RUST MODERNIZATION

mcochran@cochranblock.org

[linkedin.com/in/cochranblock](https://www.linkedin.com/in/cochranblock)

Owner & Engineer · The Cochran Block, LLC · CAGE 1CQ66 · UEI W7X3HAQL9CF9

[cochranblock.org](https://www.cochranblock.org)

13+ years federal cyber operations across **USCYBERCOM**, ARCYBER Combat Mission Teams, National Mission Teams. Now solo Rust engineer. *31 public Rust products · 32 crates published · 257+ engaged engineering hours.* All non-proprietary work released under the Unlicense.

PROFESSIONAL SUMMARY

Senior Systems Engineer and Title 10 Offensive Cyber Operator with **13+ years of federal cyber operations** supporting mission-critical environments aligned with USCYBERCOM. United States Army Veteran transitioning into **Rust-based, AI-piloted development**, with a proven record of delivering production-grade software across AI infrastructure, fintech, SaaS, and open-source ecosystems. Operates as a solo engineer specializing in high-performance Rust, local AI/LLM integration, and fully Unlicensed (public domain) software aligned with frictionless procurement. Combines offensive cyber expertise, secure systems architecture, and modern AI-enabled development to support scalable, mission-driven service environments.

EXPERIENCE

Owner & Engineer · The Cochran Block, LLC

Feb 2026 - Present

Owned end-to-end architecture, development, and deployment of sovereign, AI-driven Rust systems, delivering production-grade platforms across SaaS, automation, and offline-first applications. Led full-stack engineering from systems design through secure deployment, emphasizing local AI inference, performance optimization, and zero-dependency distribution.

- Architected and deployed **10+ production-grade Rust platforms**, consolidating AI orchestration, SaaS delivery, and secure payment processing – **sub-50 ms API latency** with fully self-hosted, sovereign AI capability across all systems.
- Reengineered legacy automation paradigms into Rust-native frameworks via a **14-crate orchestration system** and lightweight workflow engine – **~10 ms cold start vs. 1-3 s industry baseline**, runtime overhead reduced >90%.
- Developed a distributed AI augment engine with **local LLM inference and agentic tool loops**, enabling autonomous task execution without cloud dependency – **data-privacy compliance +100%, external API costs \$0**.
- Engineered a secure **ISO 8583 payment processing system** with AES-256-GCM encryption and append-only ledger, end-to-end transaction integrity and encrypted vaulting – **0 data exposure incidents**, full audit traceability.

Senior Systems Engineer · MaxisIQ

Sep 2024 - Feb 2026

Engineered and maintained mission-critical cyber infrastructure and automation supporting high-availability operations, focused on secure system orchestration, identity management, and scalable tooling. Aligned Python-based automation with emerging Rust-driven, sovereign AI development models.

- Developed custom **Python-based system survey and remediation tools**, automating server health checks and service repair across distributed environments – **manual intervention -85%, system uptime 99.9%**.
- Automated **SSH and Kerberos authentication infrastructure** with secure provisioning and key rotation workflows – **credential incidents -70%, access control hardened across 200+ nodes**.
- Implemented resilient service monitoring and recovery for high-availability mission ops – **sub-5-minute incident response**, sustained operational readiness.
- Modernized legacy automation by introducing modular, Rust-aligned design patterns and lightweight service architectures – **execution speed 3x, resource consumption -60%**.

Senior Software Engineer · Two Six Technologies

Sep 2022 - Sep 2024

Designed and delivered secure data integration pipelines and backend tooling for large-scale cyber platforms. Hands-on integrations across the **Joint Cyber Warfighting Architecture (JCWA)**: JCC2, JCAP, UDP.

- Engineered **YAML-to-SQL data pipelines** to normalize and ingest heterogeneous datasets into structured environments – **processing throughput 4x, ingestion errors -65%**.
- Built **regex-driven parsing engines** to extract and standardize unstructured data – **data accuracy +80%, real-time processing of 1M+ records / day**.
- Developed **data sanitization and validation tooling** to enforce schema compliance and remove anomalies – **100% data integrity** across critical workflows.
- Integrated modular data services into a unified architecture via Rust-aligned backend components – **pipeline latency -50%**, seamless interoperability across 10+ system interfaces.

J38 JMOC-E co-dev lead on NDAA-directed offensive cyber operations study. Designed and delivered backend systems, APIs, and deployment pipelines for secure, high-availability environments – emphasizing scalable architecture, data integrity, and automated delivery.

- ▶ Developed and deployed **RESTful APIs** supporting secure data exchange across distributed systems – **response latency -45%**, integration across 8+ platform services.
- ▶ Designed **CI/CD pipelines** using GitLab and Docker to automate build, test, and deployment – **release cycles -60%**, **99.8% deployment success**.
- ▶ Modeled and optimized relational and semi-structured data systems for high-throughput applications – **query performance 3x**, **500K+ daily transactions without degradation**.
- ▶ Implemented and documented **network protocol interfaces** for reliable system communication and interoperability – **transmission errors -70%**, standardized integration across 10+ services.

Title 10 Offensive Cyber Operator · ARCYBER 103rd Combat Mission Team

Feb 2017 - Jun 2020

Executed offensive cyber operations and developed automation tooling to support mission execution across secure, high-stakes environments – emphasizing rapid data exploitation, system disruption, and operational efficiency.

- ▶ Executed **100+ high-complexity operational cyber missions** across distributed environments requiring precision and real-time decision support – **95% mission success rate**, sustained operational readiness.
- ▶ Developed **Python automation tooling** to streamline mission support and reduce manual operational overhead – **execution time -60%**, task reliability across 50+ mission cycles.
- ▶ Built **custom scripting frameworks** for data collection and system interaction – **data processing speed 3x**, faster decision cycles in time-sensitive environments.
- ▶ Enhanced mission support efficiency through automated system orchestration with modular, reusable components – **repetitive task load -70%**, operator throughput up across multiple concurrent operations.

Digital Network Exploitation Analyst · National Mission Team

Jul 2014 - Feb 2017

Network mapping, traffic analysis, and Intelligence Community reporting in support of National Mission Team objectives.

EDUCATION

M.S. Computer Science

[Recursive Academy](#)

Offensive Operations Foundation Course

[National Security Agency / USCYBERCOM](#)

Joint Cyber Analysis Course (JCAC)

[Corry Station · 2014](#)

CERTIFICATIONS

GIAC Security Essentials (GSEC)

[Global Information Assurance Certification](#)

SPECIALIZED MILITARY TRAINING

- ▶ Cyber Operations Specialist (17C) Course
- ▶ Advanced & Basic Leadership Course
- ▶ JCAC Corry Station 2014

AUTHORIZATIONS

U.S. Citizen · U.S. Army Veteran · 30% service-connected disabled
SDVOSB – Final Review (MySBA Certifications)
Inactive Top Secret / SCI · CI Polygraph · reactivation eligible
U.S. Army MOS 17C Cyber Operations
 All personal output released under the **Unlicense** (public domain)

TECHNICAL COMPETENCIES

Languages Rust, Python, C, C++, Go, Assembly (x86 / ARM), Bash, PowerShell, SQL, JS / TS, YAML, TOML

Rust Tokio, Axum, Hyper, Tonic, Serde, sqlx, Reqwest, Leptos, Dioxus, egui, Candle, Kalosm, MiniJinja, age, rskafka, lapin

Architecture Microservices, Event-Driven, DDD, Hexagonal, REST, gRPC, GraphQL, Protocol Buffers, OpenAPI, Distributed Systems, Mission-Critical

Infra PostgreSQL, SQLite, sled, Redis, Kafka, AMQP, MQTT, Docker, Podman, Kubernetes, Terraform, Cloudflare Workers, AWS (S3, IAM, SigV4, Lambda)

Security Pen testing, OCO, DNE, TDNA, RE, MITRE ATT&CK, Cyber Kill Chain, Zero Trust, Burp, Wireshark, Metasploit, Ghidra, IDA

Crypto AES-256-GCM, ChaCha20-Poly1305, Argon2id, HKDF, Ed25519, X25519, BLAKE3, age, GPG, X.509, TLS / mTLS, Kerberos, OAuth/OIDC, JWT

AI / ML Local LLM inference, Kalosm, Candle, RAG, fastembed, vector embeddings, agentic tool orchestration, multi-agent, Claude API, OpenAI API, function calling

Compliance NIST 800-53, NIST 800-171, CMMC L2, RMF, ATO, FedRAMP, FISMA, STIG, DFARS, FAR, IL5 / IL6, SDVOSB, GovCon

▶ VERIFIABLE RECEIPTS

Public Rust repositories	31
crates.io publications (gotemcoach)	32
Lines of Rust shipped (net)	144,272
Engaged engineering hours	257+
Live production domains	3
License posture	Unlicense · github.com/cochransblock