ADNAN BERIK

Cyber Defense Operations | Platform Security and AI Infrastructure
Hampton, VA | Willing to relocate to New York, NY or Washington, D.C.
Email: adnanberik@hotmail.com | LinkedIn: linkedin.com/in/adnanberik | GitHub: github.com/WaffleBits

SUMMARY

TS/SCI-cleared US Air Force Cyber Defense Operations specialist building secure AI inference systems, GPU performance tooling, and deterministic low-level software in Python, Rust, and C++20. Operational experience spans enterprise incident response, vulnerability management, and automation across mission-critical networks.

EXPERIENCE

United States Air Force | Cyber Defense Operations Specialist (1D7X1Q), ACC, Langley AFB, VA | 2023 - Present

- Coordinate enterprise cyber priorities and core service status across 32 sites, delivering 24/7 support for 5 NAFs and 26 Wings at 15 ACC bases; recognized with quarterly award and commanders coin.
- Resolved NORAD NIPR outage by coordinating 4 units to identify a failed $700K relay circuit and implement an enterprise-wide fix, restoring missile sensor warnings for 29M sq mi of US & Canadian airspace.
- Designed and implemented a $1.2M virtual enclave to segregate foreign networks at Mountain Home AFB, preserving CUI access without interrupting flight training for 187 coalition pilots.
- Configured switches and managed 50+ SIPR assets during RED FLAG 24-3, sustaining 2K members from 39 joint units in 8 classified areas and enabling 1.1K aircraft sorties.
- Led 11 Airmen to manage 18 AFCYBER tasking orders, strengthening 5 vulnerable sites and 30K assets and ensuring C4ISR capabilities for 1.3K units at 262 locations.

TECHNICAL PROJECTS

Secure AI Inference Gateway (Python)

- Built an authenticated model-serving gateway with role and reason-for-access policy, request/token budgets, structured audit evidence, Prometheus/OpenTelemetry telemetry, and optional Redis-backed atomic rate limits.
- Added deployment posture checks, dependency auditing, SPDX SBOM generation, container vulnerability gates, resilience drills, and bounded backend probes with aggregate-only artifacts.

Inference Runtime & GPU Performance (Rust, Triton, Python)

- Implemented a deterministic continuous-batching and paged KV-cache scheduler in Rust with replay fingerprints and promote/hold/rollback release gates.
- Developed correctness-gated Triton RMSNorm, SwiGLU, attention, KV-movement, and INT4 kernels; published raw RTX 5070 Ti measurements up to 2.2x faster than torch.compile for the primary kernel set.
- Extended a serving benchmark with open-loop pacing, measured retry budgets, and privacy-safe ingress/backend/success counter reconciliation; added sampled DCGM telemetry, trace checks, and numeric output gates.

Low-Latency Matching Engine (C++20, Python)

- Built price-time-priority matching engines in C++20 and Python with deterministic parity tests; measured the Python reference at 312K orders/second on a Ryzen 9800X3D.

EDUCATION

- Western Governors University | B.S. Cybersecurity & Information Assurance (in progress)
- Northern Virginia Community College | Computer Science coursework (60+ credits completed)

CERTIFICATIONS & CLEARANCE

- TS/SCI Security Clearance
- CompTIA Security+

TECHNICAL SKILLS

Languages: Python, Rust, C++20, TypeScript, SQL, Bash. **AI & Performance:** OpenAI Triton, PyTorch, model-serving benchmarks, latency profiling, continuous batching, KV-cache systems. **Platform:** Linux, Docker, Kubernetes, Redis, Prometheus, Grafana, OpenTelemetry, Git. **Security:** access control, audit logging, vulnerability management, incident response, threat modeling, ACAS, Tanium, eMASS.