MAHMOUD (“MICHAEL”) KURDI

Charlotte, NC · (704) 456-8322 · kurdi.michael.it@gmail.com · linkedin.com/in/michael-kurdi · github.com/KM-it-ops · https://km-it-ops.github.io

PROFESSIONAL SUMMARY

CompTIA Security+ certified professional with more than eight years in federally regulated, security-cleared environments, enforcing FAA, OSHA, IATA, and CBP compliance. Obtained a B.S. in Information Technology from Southern New Hampshire University (2025). Experienced in incident response, access control, vulnerability assessment, and building Python-based security detection tools. Targeting SOC Analyst and Cybersecurity Analyst roles.

TECHNICAL SKILLS

Security & Analysis: Threat Detection · Incident Response · Log Analysis · Vulnerability Management · SIEM · IDS/IPS · Malware Analysis · Risk Assessment · RBAC · Endpoint Security · Network Security · Firewall Configuration

Tools & Tech: Python · scikit-learn · pandas · NumPy · Wireshark · Cisco Packet Tracer · Active Directory · React · Flask · SQLite · Machine Learning · Prompt Engineering

Cloud & Compliance: Cloud Security Fundamentals · FAA · OSHA · IATA · CBP Protocols · Security Clearance Procedures · Audit Documentation

EDUCATION & CERTIFICATIONS

B.S., Information Technology — Cybersecurity Concentration *December 2025*

Southern New Hampshire University · Summa Cum Laude · 3.96 GPA · President's List (8 terms) · Alpha Sigma Lambda Honor Society

Certifications: CompTIA Security+ ce (2025) · Security Clearance & CBP Badge Endorsement (2015–2023)

TECHNICAL PROJECTS

Phishing Email ML Classifier · *Python · scikit-learn · Random Forest* · github.com/KM-it-ops/phishing-email-classifier

- Engineered 207 features via TF-IDF vectorization and custom regex pattern matching; achieved 99.68% F1 score validated with 5-fold cross-validation.
- Implemented feature importance analysis to surface highest-signal phishing indicators with real-time classification demo.

Security Log Anomaly Detection System · *Python · pandas · NumPy* · github.com/KM-it-ops/security-log-anomaly-detection

- Built rule-based + statistical detection engine flagging 6 SOC threat categories: brute force, port scans, off-hours access, unknown IPs, privilege escalation, and volume spikes (Z-score).
- Achieved 100% detection rate across all injected threat scenarios; alert output structured for SOC triage workflows.

StockPath Navigator — AI System · *Python · React · Prompt Engineering*

- Deployed 17 prompt engineering techniques (Chain-of-Thought, ReAct) with React dashboard for real-time data processing and behavioral adaptation protocols.

PROFESSIONAL EXPERIENCE

Aviation Security Operations Crew Chief · American Airlines · Charlotte, NC *2015 – 2023*

Held security clearance and CBP badge endorsement managing daily security operations for international wide-body aircraft under FAA, OSHA, IATA, and CBP compliance.

- Led incident response and recurrent security training — reduced critical response times by 30% via improved communication procedures.
- Developed seven training programs that cut operational errors and lowered safety incidents by 15%; maintained federal aviation compliance across all operations.
- Supervised crew operations and security system access controls, succeeding in a 20% improvement in operational efficiency.

Courier & Logistics Specialist · USPS · Kannapolis, NC *2024 – 2025*

- Conducted systematic 26-point safety and security inspections; maintained detailed compliance documentation for operational audits.

Delivery Associate · Fossa Logistics LLC (Amazon DSP) · Charlotte, NC *2025 – Present*

- Monitored real-time tracking systems to resolve service issues proactively; maintained compliance records for operational reporting.