

MAHMOUD ("MICHAEL") AL KURDI

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

PROFESSIONAL SUMMARY

Security+ certified recent IT/cybersecurity graduate with hands-on portfolio work in SOC-style analysis, defensive security automation, MITRE ATT&CK-aligned reasoning, AI-assisted tooling, and reproducible benchmarking. Strongest evidence includes AgentForge and the AgentForge ATT&CKLens Benchmark: projects with specifications, safety rules, acceptance tests, scorecards, final reports, and clear defensive-security constraints. Targeting SOC Analyst, Security Operations Analyst, Cybersecurity Analyst, Incident Response Analyst, Junior Detection Engineering, and security automation roles.

TECHNICAL SKILLS

SOC / Security Operations: Alert triage · security monitoring · incident documentation · log analysis · evidence review · authentication events · DNS investigation · vulnerability awareness · remediation planning · escalation notes

Cybersecurity: MITRE ATT&CK · defensive security · prompt-injection resistance · access control · least privilege · security documentation · confidence scoring · "No Clear Mapping" handling · analyst follow-up questions

AI / Automation: AI coding-agent evaluation · reproducible benchmark design · rubric-based scoring · agent workflow documentation · prompt architecture · safety rules · acceptance criteria · automated reporting

Programming / Tools: Python · Gradio · JavaScript · Node.js · PowerShell · Bash · Git/GitHub · Markdown · JSON · YAML · HTML/CSS · pytest · npm

SELECTED PROJECTS — GITHUB.COM/KM-IT-OPS

AgentForge · *AI agent configuration · verification · documentation* · github.com/KM-it-ops/AgentForge

- Built and documented a framework for configuring, evaluating, and benchmarking AI coding agents across real engineering workflows, including adapters for Claude Code, Codex, Cursor, and generic agent workspaces.
- Organized the project around reproducible proof: adapter round-trip tests, package install smoke tests, readiness runbooks, and a local visual demo.

AgentForge ATT&CKLens Benchmark · *MITRE ATT&CK · Gradio · safety rules · scorecards* · github.com/KM-it-ops/AgentForge-ATT-CKLens-Benchmark

- Designed and evaluated a defensive cybersecurity benchmark focused on MITRE ATT&CK mapping discipline, prompt-injection resistance, evidence citation, uncertainty handling, detection ideas, remediation guidance, and analyst follow-up questions.
- Compared seven agent artifacts with rubric-based scoring and preserved reproducibility through scripts, scorecards, raw outputs, logs, branch inventory, acceptance tests, and a final report.

Vulnerability Management Mini Program · *Python · Flask · SQLite · REST workflows* · github.com/KM-it-ops/Vulnerability-Management-Mini-Program

- Built a dashboard-style vulnerability workflow with CRUD, KPI cards, search, filtering, severity states, and operational status views aligned to analyst workflows.

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

- Built SOC-style detection work for authentication and network anomaly triage using readable rule-based and statistical output.

PROFESSIONAL EXPERIENCE

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

- Worked in federally regulated aviation operations with security clearance and CBP badge endorsement, supporting international flight operations under FAA, OSHA, IATA, and CBP requirements.
- Completed recurrent incident-response and safety/security training in a high-accountability environment where documentation accuracy, identity validation, access control, and procedural discipline mattered.
- Coordinated with management and operations teams during time-sensitive incidents, inspections, and compliance-driven workflows.

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

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

EDUCATION & CERTIFICATIONS

**B.S. Information Technologies — Cybersecurity
Concentration**

***Completed December 2025; diploma conferred January 1,
2026***

Southern New Hampshire University · Summa Cum Laude · 3.96 GPA · Sigma Psi chapter of Alpha Sigma Lambda

Certifications: CompTIA Security+ ce (SY0-701), issued January 7, 2025, valid through January 7, 2028