GEORGE C. EKWEM JR
Sicklerville, NJ | (856) 263-8582 | georgecekwemjr@gmail.com | LinkedIn | GitHub

EDUCATION

Neumann University *Aston, PA*
Bachelor of Science, Cybersecurity *May 2025*

CERTIFICATIONS

- **CompTIA Security+** (SY0-701)

EXPERIENCE

Cybersecurity / IT Intern *May 2023 – Dec 2025*
Widelink Tech (Veteran-Owned Small Business) *Williamstown, NJ*

- Monitored firewalls, IDS/IPS alerts, and endpoint protection consoles; reviewed system logs daily to identify anomalies, suspicious activity, and reported potential incidents to senior staff.
- Developed Python automation scripts for log collection and weekly security reporting, reducing manual report preparation time.
- Participated in security audits and system hardening activities, applying CIS benchmarks and organizational baselines to Windows and Linux endpoints.

PROJECTS

Detection Engineering & CI/CD Pipeline | Detection Engineering & CI/CD Pipeline

- Developed and deployed SQL-based AWS CloudTrail detections in RunReveal for AWS root account activity and S3 bucket encryption modifications.
- Built positive and negative detection test cases and automated validation through GitHub Actions to verify detection behavior before deployment.
- Implemented a detections-as-code CI/CD pipeline using GitHub, protected branches, pull requests, automated validation, and token-secured deployment to RunReveal.
- Analyzed CloudTrail events and tuned detection logic to identify security relevant AWS configuration changes while reducing noisy service-generated activity.

Zero Trust Access Enforcement Engine | Zero Trust Access Enforcement Engine

- Engineered a context-aware Zero Trust authorization engine combining RBAC, device posture, MFA, network context, resource sensitivity, and risk scoring to enforce least-privilege access decisions.
- Built security detection and alerting capabilities for unauthorized access, high-risk activity, critical-resource access, and suspicious access sequences.
- Developed security investigation APIs, persistent audit trails, structured JSON logging, and security metrics to support security operations and incident analysis.
- Implemented controlled security simulations and 31 automated tests covering authorization, detection, investigation, metrics, and security workflows; deployed the platform with Docker and Docker Compose.

Threat Intelligence Dashboard | Threat Dashboard GitHub Repo

- Built interactive dashboards to visualize suspicious activity, attack trends, and security events.
- Integrated external threat feeds and APIs to enrich security data and improve investigative context.
- Developed backend and frontend components using Python, Flask/Django, JavaScript, and data visualization libraries.
- Implemented filtering and visualization workflows to support investigation of indicators and emerging threats.

Phishing Simulation Toolkit | Phishing Sim GitHub Repo

- Developed a controlled phishing-awareness simulation platform for security training and user-awareness testing.

- Created customizable simulation templates and tracked user interactions to measure susceptibility metrics.
- Implemented reporting capabilities for analyzing simulation results and user behavior.
- Applied secure development practices and ethical testing principles throughout the project.

TECHNICAL SKILLS

SIEM & Security Operations: Microsoft Sentinel, Microsoft Defender XDR, Defender for Cloud, Log Analysis, Incident Triage

Detection & Threat Analysis: KQL, SQL, MITRE ATT&CK, AWS CloudTrail, RunReveal

Cloud & Infrastructure: Linux, Microsoft Azure, AWS, GCP

Languages & Scripting: Python, PowerShell, Bash, TypeScript

Tools & Standards: Git/GitHub, Wireshark, Nmap, CIS Benchmarks