AHANAF AKIF

786-535-5600 | akif.ctg05@gmail.com | linkedin.com/in/ahanafaakif | akifcloud.com

EDUCATION

Florida International University (FIU) **Miami, FL**

Bachelor of Science in Computer Science | GPA: 3.6/4.0 *Expected: May 2027*

Honors & Awards: FIU Presidential Merit Scholarship, Florida Bright Futures, Dean's List

Relevant Coursework: Operating Systems, Database Management, Digital Forensics, Programming I-II
Associations: INIT@FIU , CodePath

SKILLS

Languages: Python, JavaScript, Java, C++, SQL, HTML/CSS, PowerShell
Certifications: SC-900 – Microsoft Security, Compliance, and Identity Fundamentals (Azure)
Security Domains & Tools: Information Security, Network Security, Risk Management, Compliance, Splunk, SIEM
Cloud & DevOps: AWS, Docker, GitHub Actions, CI/CD, Linux Administration

EXPERIENCE

INIT Build | FIU **Sep. 2025 – Dec. 2025**

Cybersecurity Team Member

- Collaborated with an 8-member cybersecurity team to **build a scalable IAM Misconfiguration Dashboard**, integrating **OPA, Checkov, and Gitleaks** for automated detection and compliance.
- Assisted migration of core workloads to **AWS (S3, DynamoDB, Lambda, API Gateway, CloudWatch)**, enhancing observability and misconfiguration defense.
- Streamlined policy enforcement and infrastructure automation with **Terraform + Docker**, **reducing onboarding time by 40%** and strengthening deployment reliability.

PROJECTS

NextWave | MDC SharkByte Hackathon 2025

- Developed a multi-agent AI platform website with teammates to help students generate personalized academic and career pathways. **(#1 in MDC Career Challenge + #1 Use of Digital Ocean)**
- Developed full-stack architecture using **React, TypeScript, Tailwind, AWS Lambda, API Gateway, DynamoDB, and Google Gemini**, enabling real-time guidance, salary insights, and cost projections.
- Deployed the platform using **AWS S3 and CloudFront as a CDN**, reducing page latency and supporting 100+ student users.

AWS GuardDuty / Threat Detection Project | AWS (CloudTrail, IAM, S3, CloudShell), JS

- Deployed a vulnerable OWASP web app via **CloudFormation** to evaluate GuardDuty detection coverage.
- Simulated **SQLi and command-injection attacks**, triaged alerts via **CloudTrail**, and hardened IAM + S3 policies using least privilege controls.

ACTIVITIES

Cybersecurity Training & Blue Team Simulation | CodePath CYB102

Codepath

- Completed a 10-week SOC analyst program focused on **SIEM** monitoring, IDS alerting, incident response, and threat intelligence.
- Detected vulnerabilities/anomalies using **Splunk, Snort, Linux, and Wireshark**, documenting IOCs and response steps.
- Conducted incident response drills, practicing triage, containment, recovery, and **MITRE ATT&CK** mapping.

FlagOps Capture-the-Flag (CTF) | Network Forensics & Threat Hunting

INIT@FIU

- Analyzed PCAP traffic in Wireshark and performed Linux forensic triage to recover obfuscated flag data.
- Deployed Parrot Security VM, performed evidence extraction, and validated findings through CLI forensics.
- Collaborated with teammates to correlate logs, accelerate anomaly validation, and improve flag recovery accuracy.