AHANAF AKIF

aakif001@fiu.edu ~ 786-535-5600 ~ linkedin.com/in/ahanafaakif

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

SKILLS

Languages: Java, Python, HTML/CSS, SQL, Lua, R
Certifications: SC900 - Microsoft Security, Compliance, and Identity Fundamentals (Azure)
Security Domains: Information Security, Network Security (firewalls, IDS/IPS), Risk Management, Compliance
Technologies: Git, GitHub, VS Code, PyCharm, IntelliJ, Node.js, Pulumi (familiar)

EXPERIENCE

Information Technology Support Specialist **September 2023 - January 2025**

Kwik Stop, Hollywood, FL

- Diagnosed connectivity failures, peripheral malfunctions, and application errors operating remote desktop protocols and log analysis.
- Performed troubleshooting and issue resolution on workstations, POS devices and network hardware; flag and remediate malware alerts.
- Monitored security event logs, investigated malware & phishing incidents, and recorded incidents accordingly.

ACTIVITIES

Intermediate Cybersecurity (CYB102) | Blue Team/SOC, SIEM & IR | Splunk, Snort, Linux, Wireshark

Codepath

- Completed a 10-week cohort simulating blue-team defense, endpoint & network monitoring, incident response, and threat intelligence.
- Demonstrated endpoint & network monitoring through SIEM/IDS tools to detect vulnerabilities.
- Ran incident response drills to identify attack vectors, triage, containment and recovery, documenting IOCs.
- Applied threat intelligence – utilized frameworks (MITRE ATT&CK) to detect & respond to threats.

FlagOps Capture-the-Flag (CTF) — Network Forensics | Wireshark, Linux, VirtualBox

INIT@FIU

- Deployed Parrot Security VM with bridged networking to capture traffic + analyzed PCAPs in Wireshark using display filters to identify anomalies.
- Executed Linux forensic triage using CLI tools to investigate file systems & logs, decrypting obfuscated messages and successfully recovering hidden flag data.
- Collaborated with teammates to document findings, share indicators of compromise (IOCs), and streamline flag discovery.

PROJECTS

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

- Deployed OWASP demo web app via **CloudFormation** for security vulnerability & detection testing.
- Implemented **GuardDuty (with S3 Malware Protection)**; simulated **SQLi** + **command-injection**; triaged findings using **CloudTrail;** Hardened IAM with least-privilege policies and S3 controls.

Splunk SIEM — Boss of the SOC | Splunk Enterprise

- Utilized BOTS v3 Dataset to build interactive dashboards for host authentication attempts and error spikes.
- Configured scheduled **detections/alerts** for brute-force login patterns and mass-encryption behavior.