Akm Ahad Nizum

Cybersecurity Enthusiast

Murphy, TX 75094 | 984-484-4916 | akmahad3@gmail.com

LinkedIn: www.linkedin.com/in/akm-nizum-open-t0-w0rk | GitHub: https://github.com/anizum1

Professional Summary

Motivated cybersecurity professional with hands-on experience in troubleshooting, network infrastructure, and security fundamentals. Strong foundation in governance, risk, compliance, and cloud technologies (AWS, Azure). Skilled in communicating security findings and supporting secure operations. Seeking to contribute to cybersecurity or any related field that requires security.

Technical Skills

- Networking & Infrastructure: TCP/IP, SSH, SMB, DNS, Cisco Routing & Switching
- System Administration: Windows, Linux, Active Directory
- Cloud Platforms: AWS, Azure
- Security: SIEM, IDS/IPS, Firewalls, Hardening, Risk Management, Governance
- Tools: Python, Bash, Splunk, Snort, Burp Suite, Metasploit, Autopsy, FTK Imager
- Other: Pen Testing (basic), Cryptography, Technical Writing

Work Experience

Production Lead/ Machine Specialist — Shutterfly INC, Plano, TX (07/2020 – Present)

- Lead production operations ensuring quality, accuracy, and throughput.
- Troubleshoot technical issues and coordinate with technicians and vendors.
- Train and mentor employees on governance, process adherence, and security.

Education

- Bachelor of Applied Technology in Cybersecurity — Collin College (Expected Dec 2026)
- Associate of Applied Science (Cybersecurity) — Collin College (2024)
- Associate of Applied Science (Applied Science) — Collin College (2024)

Certifications

- Cisco Certified Network Associate (CCNA)— Collin College
- Information Systems Cybersecurity Certificate — Collin College

Projects

- **GitHub Tool:** Made tools to detect vulnerabilities of API endpoints, Mass Random Password generator for ethical brute force, social media scrapping tool for OSINT Etc.
- **Network Intrusion Detection & SIEM Lab:** Built IDS/SIEM lab with Security Onion, Snort, Splunk.
- **Cloud Security Hardening:** Secured AWS/Azure workloads using IAM/MFA/CIS benchmarks.
- **Digital Forensics Project:** Conducted investigations using Autopsy, FTK Imager, ExifTool.
- **Penetration Testing Lab:** Used Nmap, Hydra, Burp, Metasploit on vulnerable environments.
- **Automation & Scripting:** Python/Bash scripts for log analysis and system checks.
- **OSINT Investigation:** Used Maltego, SpiderFoot, Hunchly to map digital footprints.
- **Network Segmentation:** Implemented VLANs, ACLs, and firewall hardening on Cisco networks.