AZEEM DIMEJI YUSUF

410-497-4689 |yusuf.azeem01@outlook.com |https://www.linkedin.com/in/azeem-yusuf/

PROFESSIONAL SUMMARY

Results-driven Cybersecurity Analyst with a strong foundation in Linux, DevOps, cloud security, and penetration testing. Currently completing an Associate Degree in Cybersecurity at CCBC and actively engaged in the MyDFIR Cybersecurity Bootcamp (50% completed). Hands-on experience in security operations, incident response, and vulnerability management. Skilled in risk assessments, compliance frameworks (NIST 800-53, FedRAMP, FISMA), and cloud security best practices. Passionate about safeguarding critical assets, mitigating cyber threats, and strengthening security postures in enterprise environments. Adept at collaborating with cross-functional teams to implement proactive security strategies and achieve regulatory compliance.

TECHNICAL SKILLS

- Cybersecurity & Compliance: Incident Response, Penetration Testing, SIEM (Splunk, ELK), Vulnerability Management, Risk Assessments, Security Documentation (SSP, POA&M), Security Audits
- Networking & Cloud Security: CCNA (Routing & Switching), Firewall Configuration, Network Traffic Analysis, AWS Security (IAM, GuardDuty, Security Groups, CloudTrail), Azure Security Center
- Linux & DevSecOps: 5+ years with Linux (Red Hat, Ubuntu, Kali), Bash Scripting, Ansible, Terraform, Docker, Kubernetes, CI/CD Security, Infrastructure Hardening
- Security Tools & Technologies: Wireshark, Nmap, Metasploit, Nessus, Burp Suite, ACAS, eMASS, STIG Viewer, Vulnerability Scanning, Security Testing
- Security Frameworks & Compliance: NIST 800-53, NIST 800-171, FedRAMP, FISMA, HIPAA, PCI-DSS, STIG Compliance, Continuous Monitoring

EDUCATION

Community College of Baltimore County (CCBC) – Expected [September 2025]
Associate Degree in Cybersecurity

- Relevant Coursework: CCNA I, II, III | Penetration Testing & Ethical Hacking | Security Fundamentals

Cybersecurity Bootcamp (50% Completed)

MyDFIR Bootcamp

- Hands-on training in penetration testing, SIEM, network security, and ethical hacking.
- Completed practical labs in incident response, log analysis, and vulnerability scanning.
- Gaining experience in risk assessment, regulatory compliance (FedRAMP, FISMA), and security controls implementation.

PROFESSIONAL EXPERIENCE

DevOps Engineer
Kelly Benefits, Sparks-MD | 6/2023 – 12/2023

- Collaborated with cross-functional teams to design, implement, and maintain CI/CD pipelines for Windows-based applications using TeamCity and Octopus Deploy with Blue/Green deployment methodology.
- Managed and monitored infrastructure on Windows servers, ensuring high availability and performance using VMware and PowerShell scripting.
- Implemented security measures, including Global Protect VPN, to safeguard the organization's

network and data.
- Managed source code repositories and version control using GitHub Enterprise, ensuring code quality and seamless collaboration among development teams.
- Automated infrastructure provisioning and configuration management with Ansible and Terraform across on-premises and Azure cloud environments.
- Implemented continuous monitoring and alerting solutions with LogicMonitor, Graylog, Uptime Robot, Uptime Kuma, and Seq to proactively identify and resolve issues.
- Administered and optimized Microsoft SQL Server databases, ensuring data integrity and performance.
- Optimized applications for performance, security, and scalability in collaboration with development teams.
- Orchestrated deployment and scaling of applications on Azure cloud using Azure DevOps, ensuring cost-effectiveness and reliability.

DevSecOps / Linux Engineer
Select Data LLC, Remote January 2022 | June 2023
- Managed and secure Linux environments for various applications and services.
- Conducted log analysis and monitoring to detect security threats.
- Applied firewall configurations, intrusion detection, and SSH hardening to protect servers.
- Supported DevOps teams with secure deployments and implemented access control policies.

CYBERSECURITY PROJECTS
Penetration Testing & Ethical Hacking Lab
- Conducted penetration testing on a simulated network using Metasploit, Nmap, and Burp Suite.
- Identified and exploited vulnerabilities in a CTF (Capture the Flag) challenge.
- Wrote a report with findings, risk assessments, and mitigation strategies.

SIEM & Log Analysis with Splunk
- Deployed Splunk for real-time security monitoring and log analysis.
- Created dashboards to detect and investigate security incidents.
- Used Sysmon and Zeek for network traffic analysis and forensic investigations.
- Configured IAM roles, Security Groups, and GuardDuty to enforce best security practices.
- Implemented AWS CloudTrail monitoring and Azure Security Center policies.
- Conducted a security assessment of an AWS EC2 instance and applied remediation steps.

CERTIFICATIONS & TRAINING (In Progress)
- CompTIA Security+ (Planned)
- AWS Certified Security – Specialty (Planned)
- Certified Ethical Hacker (CEH) – In Progress
- CCNA (Completed CCNA I, II, II)

ADDITIONAL INFORMATION
- Hack The Box & TryHackMe Profile: Active participant in hands-on cybersecurity challenges.
- Open-Source Contributions: Contributed to security-related GitHub projects.
- Languages: English (Fluent).

REFERENCES
It will be provided upon request.