Fola Adelaja

Atlanta , GA | 678-365-7674 fola.adelaja@gmail.com |
linkedin.com/in/adefolaju-adelaja-4ba502249/ github.com/folaadelaja

PROFESSIONAL SUMMARY

Accomplished **Information Security Analyst** with over a decade of experience in security operations, architecture, and compliance. Specialized in leading **PCI DSS 4.0** initiatives, managing end-to-end vulnerability lifecycles, and securing application development lifecycles. Proven expertise in coordinating complex incident responses and partnering with cross-functional engineering teams to implement robust security controls.

TECHNICAL SKILLS

- **Security Operations:** SIEM (Splunk, Elasticsearch), EDR, Incident Response Coordination, IAM Controls, Privileged Access Governance.
- **Architecture & Engineering:** Secure Network Design, Firewalls (Fortinet, Meraki, FireMon), VPNs, SD-WAN, Wireless Security.
- **Application Security:** SSDLC Integration, Application-layer Penetration Testing, Risk Acceptance Tracking, PCI DSS 4.0 Requirements.
- **Risk & Compliance:** Vulnerability Management (Nessus, Qualys, Wazuh), PCI DSS QSA Engagement, Risk Assessments, ISO27001, NIST.

PROFESSIONAL EXPERIENCE

SageNet | Information Security Analyst | 2015 – Present

Security Operations & Incident Response

- Managed SIEM alert tuning, monitoring, triage, and escalation in coordination with third-party SOC providers to improve detection accuracy and reduce false positives.

- Acted as Incident Response Coordinator, overseeing the full incident lifecycle: investigation, containment, eradication, recovery, documentation, and post-incident review.

- Designed and delivered enterprise security awareness training programs to reduce phishing and social engineering risk.

- Administered Identity and Access Management (IAM) governance including access reviews, role validation, and privileged account oversight.

- Conducted firewall and network security rule reviews to maintain compliance with internal security standards and PCI DSS requirements.

Risk & Compliance Management

- Owned enterprise vulnerability management program across infrastructure and applications including scanning, prioritization, remediation tracking, and reporting.

- Coordinated remediation efforts across Network Engineering, Infrastructure, and Development teams to address security findings and reduce exposure.

- Led PCI DSS compliance initiatives including control validation, evidence collection, audit preparation, and direct collaboration with Qualified Security Assessors (QSA).

TECHNICAL PROJECTS

Security Monitoring and Vulnerability Management Tools
- Deployed and configured **Nessus**, **Splunk**, **Zabbix**, and **Wazuh** to automate threat detection and compliance monitoring.
- Integrated **Qualys** for cloud-based vulnerability management and used **Docker** to streamline tool deployment across **Proxmox** and **Hyper-V**.

CERTIFICATIONS

- CompTIA Security+
- Certificate of Cloud Security Knowledge (CCSK)
- Fortinet Certified Associate in Cybersecurity (FCAC)
- Certified Meraki Networking Associate (CMNA)

EDUCATION

- B.Sc. Network & Communication Management | DeVry University
- CISA & CISSP Training | Cybrary
- Risk & Incident Response Certification | ISC2