

Fola Adelaja

678-365-7674

foladelaja@gmail.com

github.com/folaadelaja

linkedin.com/in/adebolaju-adelaja-4ba502249/

EDUCATION

DeVry University - B.Sc. Network & Communication Management

Certified Information System Auditor CISA

Certified Information System Security Professional CISSP

Identifying, Monitoring, and Analyzing Risk and Incident Response and Recovery

DeVry University, 2017

Cybrary

Cybrary

ISC2

CERTIFICATIONS

CompTIA Security+

Fortinet Certified Associate in Cybersecurity (FCAC)

Certified Meraki Networking Associate (CMNA)

PROJECTS

Project: Implementing a SIEM in homelab

Source: <https://github.com/folaadelaja/My-Projects>

Project: Nessus

Platforms and Technology Used: Virtual Machines, Docker, Proxmox, Log Analytics

EXPERIENCE

Company: SageNet

2014 - Present

Title: Information Security Analyst

- The use of Sentinel-one dashboard which is used to monitor and manage our protected endpoints, investigate and respond to security alerts, track and resolve security incidents, configure security policies, generate reports, and perform endpoint remediation actions.
- Vulnerability Assessments and Penetration Testing: Work with Network engineers to conduct regular vulnerability assessments and penetration testing on the network infrastructure. The two teams work together to identify vulnerabilities, test for potential security weaknesses, and recommend appropriate remediation measures.
- Develop training sessions for employees to raise awareness of security risks and best practices for avoiding them.
- Responding to security incidents and taking appropriate action, such as isolating affected systems, containing the damage, and restoring normal operations.
- Implement and maintain security controls, such as firewalls, access controls, and encryption, to help protect the organization's networks, systems, and data.
- Experience in using Security Information and Event Management (SIEM): Elasticsearch's Security and Threat Detection:
- Elasticsearch plays a significant role for log analysis in my operations. It is used for storing and analyzing security-related data such as logs, network traffic, or system events. On a daily basis, Elasticsearch is queried to detect security threats, investigate suspicious activities, and identify potential vulnerabilities. This helps in timely incident response and threat mitigation.
- Firewall Management: FireMon application is part of what I use to administer, manage and optimize firewall policies across multiple vendors and platforms. It allows me to analyze firewall rules, identify redundant or conflicting policies,

and ensure that the policies align with the organization's security requirements.

- By actively participating in the above activities, as an information security analysts I help my organizations achieve and maintain PCI DSS compliance. Contributing my expertise in security assessments, control implementation, risk management, incident response, and compliance monitoring contributes to protecting cardholder data and maintaining the security of payment transactions in accordance with PCI DSS standards.
Continuous assessment and impact of current technology architecture for vulnerabilities, weaknesses and for possible upgrades or improvements
- Oversee information security audits performed internally by the organization or third-party personnel.
- Serve as a security focal point of contact for the IT team and the customer or organization.
- Communicate information security goals and new programs effectively to gain alignment with IT leadership.
- Manage Team Member cybersecurity awareness training program.
- Manage outsourced vendors that provide information security functions for compliance with contracted service-level Agreements.
- Manage the day-to-day activities of threat and vulnerability management, identify risk tolerances, recommend treatment plans and communicate information about residual risk.
- Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and comply with policies and audit requirements.
- Design, coordinate, and oversee security-testing procedures to verify the security of systems, networks, and applications, and manage the remediation of identified vulnerabilities.
- Liaise among internal teams and external vendors to ensure compliance and a strong security posture.
- Consult with IT staff to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications, and software.
- Recommend and coordinate the implementation of technical controls to support and enforce defined security policies.

Company: SageNet

2014 - Present

Title: Information Security Analyst

- Vulnerability Assessments
- Security Awareness Training with Infosec
- Incident response

SKILLS AND TECHNOLOGIES

SIEM, Sentinel, Threat hunting, Log analyst, Linux, Docker, Bash, Ansible, Kubernetes, FortiOS, Git, Cisco IOS, SysAdmin, Help Desk, Ticketing System, Azure, Network Security Groups, Firewalls, ACLs (Access Control Lists), Virtual Machines, Virtual Networks, Cloud Computing, Active Directory, File Permissions, Linux, Networking, Security Training, Compliance and regulations