Fola Adelaja

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

EDUCATION

DeVry University - B.Sc. Network & Communication Management — DeVry University, 2017
Certified Information System Auditor CISA — Cybrary
Certified Information System Security Professional CISSP — Cybrary
Identifying, Monitoring, and Analyzing Risk and Incident Response and Recovery — ISC2

CERTIFICATIONS

CompTIA Security+
Certificate of Cloud Security Knowledge (CCSK)
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, Splunk, Zabbix, Wazuh, Elastic Search, Qualys
Platforms and Technology Used: Virtual Machines, Docker, Proxmox, Hyper-V

EXPERIENCE

Company: SageNet — 2014 - Present
Title: Information Security Analyst

- Monitored and analyzed security incidents, leading incident response efforts to mitigate damage and prevent future breaches.

- The use of EDR which is used to monitor and manage our 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: Conduct quarterly vulnerability assessments and automating penetration testing on the infrastructure.
- 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 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 has helped us to meet timely incident response and threat mitigation.

- Collaborated with IT and management teams to design and deploy security architecture that protects against advanced threats.
- Firewall Management: FireMon application is used to review 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 analyst my contribution in the organizations is to make sure we are PCI 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.
- Managed security operations, including threat detection, monitoring, and incident response.
- 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.

SKILLS AND TECHNOLOGIES

Risk assessment, Vulnerability management, Threat intelligence, Security policies, Penetration testing, Incident response, Security audits, Data protection, Compliance, Security frameworks, Security controls, Incident detection, Security monitoring, Firewalls, Intrusion detection systems, Intrusion prevention systems, Identity and access management,NIST, ISO27001 Security awareness, Security training,Security assessments, Security architecture, Business continuity planning, Risk mitigation, Security standards, Security governance, Security regulations, Security technologies, Security operations, Security incident management, Threat modeling, Security assessments, Security risk management, IT governance, Data privacy, Security strategy, Security documentation, Security awareness training, Security incident response, Security testing, Security threat analysis, Security administration, Security best practices, Information assurance, Physical security, IT policies, Security compliance, Endpoint security, Data encryption, Identity management, Log analyst, Docker, Bash,Ansible, NIST, 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, Network security,