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

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

Security Monitoring and Vulnerability Management Tools

Technologies Used: Nessus, Splunk, Zabbix, Wazuh, Elastic Search, Qualys
Platforms: Virtual Machines, Docker, Proxmox, Hyper-V

- Deployed and configured various security tools such as **Nessus** for vulnerability assessments, **Splunk** for log analysis and SIEM, **Zabbix** for network and server monitoring, **Wazuh** for threat detection and compliance monitoring, and **Elastic Search** for data storage and querying.
- Integrated **Qualys** for cloud-based vulnerability management and policy compliance, ensuring proactive threat identification and remediation.
- Utilized **Docker** containers to streamline deployment processes and manage multiple instances of security tools across **Proxmox** and **Hyper-V** environments.
- Managed and maintained virtual machines to simulate enterprise environments for testing and optimizing security configurations.

PROFESSIONAL EXPERIENCE

Company: SageNet 2015 - Present
Title: Information Security Analyst

Security Monitoring and Incident Response

- Monitored and analyzed security incidents, leading comprehensive incident response efforts to mitigate damage and prevent future breaches.
- Leveraged Endpoint Detection and Response (EDR) systems to monitor, manage, and secure endpoints, investigate

and respond to security alerts, and perform endpoint remediation. Conducted root cause analysis and tracked incidents through resolution.
- Utilized Security Information and Event Management (SIEM) tools, particularly Elasticsearch, for daily log analysis, threat detection, and investigating suspicious activities, contributing to timely incident response and threat mitigation.

Vulnerability Management and Penetration Testing

- Conducted quarterly vulnerability assessments and automated penetration testing to identify and remediate security vulnerabilities across the infrastructure.
- Continuously assessed and optimized the organization's technology architecture for weaknesses and opportunities for improvement, ensuring robust defense against potential threats.

Firewall and Access Control Management

- Managed and optimized firewall policies using FireMon, ensuring compliance with security requirements by reviewing rules, eliminating redundant or conflicting policies, and aligning them with organizational security standards.
- Implemented and maintained critical security controls, including firewalls, access control mechanisms, and encryption, to safeguard the organization's networks, systems, and data.

Security Architecture and Collaboration

- Collaborated with IT and management teams to design and deploy secure architecture capable of defending against advanced threats.
- Consulted with IT teams to integrate security into hardware, application, and software evaluations, ensuring that security requirements are prioritized during installation and configuration.

Security Awareness and Training

- Developed and led security training sessions to raise employee awareness of cybersecurity risks and best practices, reducing organizational exposure to phishing and other social engineering attacks.
- Managed the cybersecurity awareness training program for team members, enhancing security literacy across the organization.

Compliance and Risk Management

- Led initiatives to ensure PCI DSS compliance, providing expertise in security assessments, control implementation, and risk management to protect cardholder data and payment transactions.
- Managed third-party vendors providing security services, ensuring compliance with contracted service-level agreements (SLAs).
- Oversee information security audits, both internal and external, to ensure compliance with policies and audit requirements.

Security Operations Management

- Managed security operations, including threat detection, monitoring, incident response, and vulnerability management, identifying risk tolerances and recommending appropriate treatment plans.
- Ensured audit trails, system logs, and other monitoring data sources were reviewed regularly, complying with internal

policies and audit standards.

Security Testing and Remediation

- Designed, coordinated, and oversaw security testing procedures to verify the security of systems, networks, and applications. Managed the remediation of identified vulnerabilities, ensuring systems remain secure and operational.

Communication and Leadership

- Served as the primary information security point of contact for IT teams and external customers, ensuring alignment on security initiatives and incident response strategies.
- Communicated security goals and programs effectively to IT leadership, gaining buy-in for new security initiatives and programs.

TECHNICAL SKILLS

- **Risk Management:** Risk assessment, Risk mitigation, Security risk management, IT governance
- **Vulnerability & Threat:** Vulnerability management, Threat intelligence, Threat modeling, Security threat analysis
- **Security Policies & Compliance:** Security policies, Security frameworks (NIST, ISO27001), Security regulations, Compliance, Regulatory frameworks (PCI DSS), Security standards, IT policies, Security documentation
- **Incident Management & Response:** Incident detection, Incident response, Security incident management, Security awareness training, Security testing
- **Security Operations:** Security audits, Security monitoring, Security controls, Network security, Endpoint security, Firewalls, Intrusion detection systems, Intrusion prevention systems, Log analysis
- **Security Technologies:** Data protection, Data encryption, Identity and access management, Identity management, Security administration, Cloud security (Azure, Virtual Machines, Virtual Networks)
- **Tools & Platforms:** Docker, Bash, Ansible, Kubernetes, FortiOS, Git, Cisco IOS, SysAdmin, Help Desk, Ticketing System, Active Directory, File Permissions
- **Business Continuity:** Security architecture, Business continuity planning, Security strategy, Security governance, Security operations, Information assurance, Physical security
- **Cloud & Network Security:** Cloud computing, Network Security Groups, ACLs (Access Control Lists), Networking
- **Security Awareness & Training:** Security awareness, Security training, Security compliance