Mokube Fritz

Waukee, IA 50213 | 6465446156 | mokubeotte@gmail.com

Professional Summary

Results-driven Cybersecurity Analyst with over 5 years of experience in protecting enterprise systems from threats and conducting vulnerability assessments. Proficient in utilizing SIEM tools, IDS/IPS systems, and cloud security frameworks to enhance information security. Achievements include improving security postures and reducing vulnerabilities while fostering a culture of cybersecurity awareness. Expertise in planning, analyzing, and implementing effective security initiatives and developing secure network designs.

Skills/Tools

- Threat detection and incident response
- Risk management
- Vulnerability assessment
- SIEM technologies (Splunk, QRadar)
- Intrusion detection and prevention systems (Snort, Suricata, pfSense)
- Cloud security (AWS, Azure)
- Penetration testing
- Digital forensics
- NIST and ISO 27001 compliance
- Security awareness training
- AI & ML
- Data protection
- Firewall management
- IoT security
- Network security
- Disaster recovery
- Analytical thinking
- Endpoint protection
- DDoS prevention
- Firewall configuration
- Two-factor authentication
- Patch management
- Information security policies
- Identity and Access management
- Business continuity
- IDS integration
- System hardening
- Application security
- Compliance monitoring
- Social engineering prevention

- Security frameworks

Experience

CYBERSECURITY ANALYST | 05/2023 - Current

VA

- Monitor network activity via Splunk Enterprise and ArcSight SIEM, analyzing logs from over 5,000 endpoints across VA hospitals and clinics.
- Detect, triage, and escalate security incidents to the VA Computer Security Incident Response Team (CSIRT), ensuring timely containment and remediation.
- Perform weekly vulnerability scans using Tenable Nessus**,** validate findings, and track remediation via Plan of Action and Milestones (POA&M)**.**
- Collaborate with system owners to maintain System Security Plans (SSPs) in alignment with NIST SP 800-53 and FISMA requirements.
- Support Risk Management Framework (RMF) processes and Authority to Operate (ATO) renewals for VA systems under FedRAMP guidelines.
- Strengthened firewalls and endpoints to ensure compliance with NIST 800-53 and CIS Benchmarks.
- Participate in security audits and inspector general (OIG) reviews; respond to compliance findings with corrective action documentation.
- Led phishing awareness programs, resulting in 60% drop in human-related security incidents.
- Conduct phishing awareness training and develop user guidance on secure data handling for Protected Health Information (PHI) and PII.
- Collaborated on cybersecurity awareness training sessions to enhance organizational resilience.
- Create daily and weekly SOC activity reports summarizing detected incidents, vulnerability trends, and overall risk posture for management.
- Responded to cyber incidents by analyzing attack signatures and restoring normal operations.

INFORMATION SECURITY SPECIALIST | 02/2020 - 04/2023

Lending Club

- Perform continuous monitoring of network and cloud infrastructure using Splunk Enterprise Security and Microsoft Defender for Cloud, identifying and mitigating potential threats to Lending Club’s digital banking platforms.
- Conducted enterprise risk assessments under HIPAA, SOX, and PCI DSS frameworks for financial clients.

- Conduct vulnerability assessments and configuration audits using Tenable.sc, OpenVAS, and Qualys, ensuring remediation aligns with CIS Controls and NIST 800-53.
- Collaborate with IT, Engineering, and DevOps teams to implement secure configurations across AWS workloads, containers, and CI/CD pipelines, reducing exposure to cloud misconfigurations by 35%.
- Managed Splunk SIEM deployment to improve real-time threat visibility.
- Support incident response operations, including triage, containment, root-cause analysis, and documentation of phishing, malware, and unauthorized access incidents.
- Developed and implemented security policies for data protection across networks.
- Lead third-party vendor risk assessments, verifying compliance with SOC 2 Type II and ISO 27001 standards prior to integration with Lending Club's systems.
- Develop and enforce access control and MFA policies via Okta, Azure AD, and AWS IAM, improving authentication security and reducing privileged access risks.
- Delivered incident analysis reports and security recommendations to leadership teams.
- Assist with annual security audits and penetration tests, coordinate with external assessors and ensure timely closure of findings.
- Author and update security policies, playbooks, and standard operating procedures (SOPs) for data protection, password management, and secure software development.
- Created comprehensive reports detailing current network and application security postures.
- Participate in BCP/DR (Business Continuity and Disaster Recovery) planning and tabletop exercises to ensure organizational resilience against cyber disruptions.
- Collaborated with stakeholders to enhance overall information security initiatives.

Education

Southern New Hampshire University - Manchester, NH | Master of Science
Cybersecurity

Southern New Hampshire University - Manchester, NH | Bachelor of Science
Business Administration in IT Management

Websites, Portfolios, Profiles

- linkedin.com/in/mokube-fritz-3948a5b3

Certifications

- CompTIA CYSA+

Reference:

Upon Request.