Paul Sobowale

Email: lakky4@gmail.com

Contact: 301.346.3576

Professional Summary

Innovative Information Technology Professional with 3+ years of experience in Cybersecurity implementations and providing comprehensive security solutions and best practices toward improving IT security Operations (SecOps) to provide effective and efficient solutions to safeguard against cyber threats in IT operations and meet business needs.

Technical and Soft Skills

• SOC Security Operations- Endpoint Security, SIEM, IDS/IPS, firewalls, SIEM, IRP, Vulnerability Management, Threat Hunting, Communication, Time Management • IAM, Incident Response Plan.

• Risk Management Cybersecurity • Strategic Planning & Execution

• IT Inventory Management

• Hybrid Cloud and Cybersecurity

• Regulatory requirements, and Cybersecurity Frameworks

• Teamwork, Problem-solving, and Attention to detail.

• Network Security and Policies

• IT and Cybersecurity Project

• Network Management (LAN/WAN)

• Continuous Monitoring (CM)

• Security Management Framework

• SOC Onboarding and implementation

• Decision-making, and critical thinking.

• Critical Technology

Work Experience

CyberSecurity Specialist WIFFIX INC. August 2022 - Present

• Develop, execute, and track the performance of security measures to protect information and network infrastructure and Computer systems.

• Conducted regular vulnerability assessments and penetration testing, identifying and remediating critical vulnerabilities before they can be exploited by hackers.

• Created security metrics to analyze threats, identifying and eliminating 75 viruses and malware over the past two years.

• Managed and created rules and policies for 17,000 end-users in the data protection area, facilitating efficiency and ease of operations.

• Collaborate with the security team to implement security solutions to enhance our overall security posture.

• Develop plans to identify and fix root causes of outages and incidents following agreed-upon change and release management processes.

• Working knowledge and familiarity with Cybersecurity regulatory requirements and frameworks: NIST 800-53 & 171, CMMC, PCI DSS, ISO 27000, GDPR, HIPAA, OWASP, Risk Assessment, Vulnerability Management and Report- scanning and remediation, Continuous Monitoring (CM).

• Develop, maintain, and build effective working relationships with vendors and service providers, including annual security and risk assessments; and performance reviews based on agreed SLAs.
• Develop training materials and guidelines for our users and keep up-to-date technical and SOP documentation.
• Influence exceptional standards of IT management through executing high-quality delivery of client IT services, projects, security needs, IT asset inventory, and management of network infrastructures.
• Working knowledge managing Infrastructure as a Service (Office365, Azure AD Synchronization), VMware, Windows Servers and/or Software as a Service (SaaS) solutions such as Dropbox, Slack, Zoom, Teams, etc.

CyberSecurity Analyst Softlinks systems. April 2020 - August 2022
• Develop, execute, and track the performance of security measures to protect information and network infrastructure and Computer systems.
• Develop security and technical implementation for client's needs towards PCI compliance, SOC-2 audit, Cybersecurity- MFA (Multifactor Authentication, Data encryption, Disaster recovery/Business continuity, DLP (Data Loss
Prevention) and other security needs.
• Implemented and enforced all cybersecurity policies and procedures, as defined by cybersecurity-related documentation.
• Recommended and helped create policies and procedures to ensure the reliability of and accessibility to information systems and to prevent and defend against unauthorized access to systems, networks, and data.
• Working knowledge and familiarity with Cybersecurity regulatory requirements and frameworks: NIST 800-53 & 171, CMMC, PCI DSS, ISO 27000, GDPR, HIPAA, OWASP, Risk Assessment, Vulnerability Management and Report- scanning and remediation, Continuous Monitoring (CM).
• Manage day-to-day activities with installation, maintenance, repairs, and replacements of IT hardware, software, and office productivity applications, including desktops, laptops, mobile devices, servers, storage (SAN), operating systems, network devices, data center equipment, backup systems, Internet/Intranet, LAN/WAN, cloud services, network, systems, and security.
• Develop, maintain, and build effective working relationships with vendors and service providers, including annual security and risk assessments; and performance reviews based on agreed SLAs.
• Develop plans to identify and fix root causes of outages and incidents following agreed-upon change and release management processes.
• Executed best-in-class IT support experiences including Windows updates, patch management, WLAN access points setup, TCP/IP troubleshooting, and mobile device experiences within emailing systems.

• Develop, execute, and track the performance of security measures to protect information and network infrastructure and Computer systems.
• Provide technical support to our end users and workforce.

• Manage IT Service Desk and IT Operations with team members for cloud-based and/or on-premises infrastructure.

• Collaborate with the security team to implement security solutions to enhance our overall security posture.

Education

B.sc Economics

Trainings/Classes

RMF

Database

Certificates

Security +
CAP/CGRC in progress

References are available upon request.