Blessing Onokpasah
Phone: +1 (717) 797-7329
Email: Orangetaxservice1@gmail.com
GitHub: github.com/BlessingTega
LinkedIn: linkedin.com/in/blessing-onokpasah-68a7a523a

Professional Summary

A results-driven Cyber Security Engineer with a refined acumen in vulnerability management, incident response, and security infrastructure enhancement. My technical expertise spans across cloud security, SIEM implementation, and compliance with industry regulations, all of which are underpinned by a strong foundation in business administration. With a career that bridges the gap between security engineering and strategic analysis, I thrive on translating complex technical challenges into actionable solutions, all while maintaining a vigilant stance against ever-evolving cyber threats.

Professional Experience

COMET Networks

Cyber Security Support Engineer
April 2017 – Present
Alpharetta, GA 30005

- Spearheaded the implementation of NIST SP 800-53 and PCI DSS controls, driving a 99% reduction in security vulnerabilities. Utilized tools like Nessus and Wireshark to conduct in-depth threat analysis and vulnerability management.
- Enhanced SIEM performance by 30% through advanced configurations of Microsoft Sentinel, improving real-time detection and incident response efficiency.
- Decreased incident response time by 50% by developing custom KQL analytics rules aligned with GDPR requirements, enabling faster identification and mitigation of potential threats.
- Collaborated across multi-functional teams to integrate AI-driven automation into the SIEM infrastructure, reinforcing proactive threat detection and compliance with NIST Continuous Monitoring (CM) standards.
- Implemented robust access control policies per GDPR and NIST SP 800-53, safeguarding sensitive data and ensuring secure operational practices.

- Successfully mitigated cybersecurity incidents by 60%, effectively aligning incident management processes with NIST and GDPR frameworks.

Jos. A. Bank Clothiers

Security Analyst
June 2014 – April 2017
Princeton, NJ

- Led comprehensive vulnerability assessments using Nessus, identifying and mitigating high-risk vulnerabilities in alignment with PCI DSS and GDPR standards.
- Implemented proactive remediation strategies, bolstering system defenses while ensuring compliance with industry regulations.
- Enhanced incident management by simulating real-world cyber threats, which improved organizational preparedness and reduced response times during actual security incidents.

Education

Degree in Business Administration
HACC, Central Pennsylvania's Community College
Graduated: September 2019

Key Projects

Implementing a SOC and Honeynet in Azure

GitHub: Azure-SOC

Designed and deployed a fully operational Security Operations Centre (SOC) alongside a honeynet on Azure, using Microsoft Sentinel and various cloud services to monitor and analyze security events. This project enhanced the organization's capacity for real-time threat detection, leveraging Azure's powerful analytics tools to bolster the security infrastructure.

- **Platforms and Technologies Used**: Azure Virtual Machines, Microsoft Sentinel (SIEM), Log Analytics Workspace, Azure Storage Account, Microsoft Cloud Defender

Implementing Vulnerability Management with OpenVAS

GitHub: Vulnerability-Management-with-OpenVAS

Developed and deployed a vulnerability management framework utilizing OpenVAS, focused on comprehensive risk identification and remediation strategies. This initiative significantly improved security posture through continuous monitoring and analysis.

Implementing Vulnerability Management with Nessus

GitHub: Vulnerability-Management-with-Nessus

Crafted a vulnerability management process using Nessus for Windows-based environments, conducting rigorous scans to detect security flaws. Followed up with targeted remediation to neutralize risks and ensure long-term system integrity.

- **Platforms and Technologies Used**: Nessus, Windows 10 Pro VM

Azure AD Logging and Monitoring

GitHub: Configuring-Azure-Tenant-Level-Logging-And-Monitoring

Configured comprehensive Azure AD tenant-level logging and monitoring to enhance visibility over user activities and potential threats. This project significantly improved detection capabilities and fortified the organization's monitoring infrastructure.

Skills

- **Cybersecurity Frameworks**: NIST SP 800-53, PCI DSS, GDPR, ISO 27001
- **Security Tools**: Nessus, OpenVAS, Microsoft Sentinel, Wireshark
- **Cloud Security**: Azure, Microsoft Defender, AWS
- **Scripting & Automation**: Python, Bash
- **Incident Response & Management**: KQL, Continuous Monitoring, Risk Mitigation
- **Vulnerability Management**: Vulnerability Scanning, Remediation Planning, Compliance Auditing
- **Networking**: Firewalls, Network Protocols, Identity & Access Management