TAWANDA MACHAYA

CYBERSECURITY ANALYST

+1 314 305 6840 • tawandamach@outlook.com

Professional Summary

Cybersecurity Analyst with 4+ years' hands-on experience in online security research, strategic planning, execution, and system maintenance. Proficient in training internal users on security protocols and preventive measures. Proven track record of securing digital assets and mitigating risks, dedicated to creating a secure digital environment. Committed to staying ahead of emerging threats and implementing cutting-edge solutions for enhanced cybersecurity.

Skills

- Network Security
- Incident Response
- Vulnerability Assessment
- Penetration Testing
- Firewall Configuration
- Security Information and Event Management (SIEM)
- Risk Assessment and Mitigation
- Encryption Technologies
- Security Policy Development
- Disaster Recovery Planning
- Team Collaboration and Leadership
- Digital Forensics (FTK Imager, Exiftool, Scalpel, KAPE, Windows File Analyzer, Volatility, Autopsy)
- Governance, Risk and Compliance
- MySQL Database management
- Cloud Security (AWS, Azure)
- **Networking and Security:** AWS VPC, Azure Virtual Network, Security Groups, Network ACLs
- **Tools**: AWS, SIEM, SOAR, Splunk, XDR, Burp Suite, Metasploit, Nessus, Hashcat, Wireshark, VirusTotal, Nmap, Cryptography, Rsyslog, OpenVAS, SET (Social Engineering Toolkit), MSF Venom
- **Cybersecurity Frameworks**: OWASP Top 10, NIST, ISO/IEC27001, CIS Critical Security Controls, COBIT, HIPAA, PCI DSS, CIS Controls, MITRE ATT&CK Framework, Zero Trust Security Model, GRC, CS-VRM

Work Experience

Cybersecurity Analyst, 01/2022 to 07/2024
Econet Wireless – Zimbabwe

- Performed threat analysis in a 24/7 environment, mitigating and managing threats and risks to the company, and achieving 99% data security using tools like Nmap, Nessus, and Wireshark.
- Supervised a team of 40 instructors to deliver company projects on time.
- Managed and created rules and policies for 8,000 end users in the data protection area, DLP, utilizing tools such as OpenVAS and Wireshark, facilitating the efficiency and ease of operations.
- Solely managed a comprehensive database of over 20,000 users, resulting in a significant increase in overall departmental performance.
- Identified over 350 new viruses and hidden malware in under three years, saving the entire company over 15,000 computers from destruction, using tools like Burp Suite and Metasploit.
- Performed random security inspections for a site containing 1,000 employees to ensure the validity and safety of all technical operations, utilizing tools such as Nmap and Nessus.
- Implemented and managed phishing simulation programs, effectively mitigating security risks through targeted training and remediation.

Information Systems Security Analyst, 01/2020 to 01/2022
Econet Wireless Zimbabwe

- Conducted security risk assessments for enterprise technologies, products, services, and operations based on applicable framework requirements from ISO/IEC 27001, ITIL, COBIT, and NIST, as well as PCI-DSS standards.

- Created, published, and maintained engaging training modules and materials, driving increased awareness and compliance for over 8,000 employees.
- Supported and managed the security of Identity and Access Management (IAM) modules on multiple systems and applications for over 7,000 employees, with defined requirements to improve user and data access control.
- Developed User Acceptance Test (UAT) scripts, conducted UATs for in-house developed applications and SaaS products to validate the system's security functionality, and ensured business security objectives were met.
- Promoted cybersecurity best practices by providing security awareness training to stakeholders, ensuring human-related security risks were reduced.

Production / Service Engineer, 01/2011 to 01/2020
Econet Wireless Zimbabwe

- Collaborated with Planning, Commercial, and Telco Vendors in the design and delivery of resilient, secure, and highly available Value Added Services infrastructure aligned with business goals.
- Developed and implemented automation processes through scripting and tooling to identify and respond to service challenges efficiently.
- Planned, coordinated, and informed the NOC team about Business Continuity Process routines to ensure system performance and minimal service impact.
- Led on-premises and remote troubleshooting activities while coordinating with support teams to resolve technical issues within agreed service standards.
- Managed incidents in line with organizational standards and contributed to continual service improvement by reducing repeat incidents and maintaining documentation.
- Handled trouble tickets raised by NOC and escalated complex cases to vendors or technical teams when required.
- Interfaced with customers, Technical Account Managers, and cross-functional teams to ensure reliable service delivery and support for new requests.
- Analyzed application logs, network performance, and service reports to recommend capacity improvements and system optimization.
- Mentored and supervised Graduate Trainees throughout onboarding, training, and placement across different business units.

Projects

Project 1: Hacking Adventures with Kali Linux

- Conducted hands-on penetration testing using Kali Linux to simulate real-world hacking scenarios.
- Explored and exploited vulnerabilities in various systems, enhancing practical cybersecurity skills.
- Applied ethical hacking techniques to identify and address security weaknesses effectively.

Project 2: Vulnerability Assessment with OpenVAS

- Executed comprehensive vulnerability assessments using OpenVAS to identify potential security risks.
- Analyzed scan results to prioritize and remediate vulnerabilities, ensuring a robust security posture.
- Developed a systematic approach to proactively manage and enhance the organization's cybersecurity resilience.

Project 3: Endpoint Analysis with Velociraptor

- Velociraptor for endpoint analysis, enabling deep forensic investigation on individual devices.
- Conducted detailed examinations of endpoints to identify and respond to security incidents promptly.
- Enhanced incident response capabilities by utilizing Velociraptor's powerful endpoint monitoring features.

Project 4: Real-Time Security Monitoring with Wazuh

- Deployed Wazuh for real-time security monitoring, providing continuous threat detection.
- Configured and fine-tuned Wazuh rules to align with the organization's security policies.
- Strengthened the incident detection and response capabilities with effective real-time monitoring.

Project 5: Network Traffic Analysis with Wireshark

- Conducted in-depth network traffic analysis using Wireshark to identify anomalies and potential threats.
- Interpreted packet captures to analyze communication patterns and detect malicious activities
- Improved network security by gaining insights into traffic behavior and implementing proactive measures.

Certifications

- **AWS Cloud Certified Practitioner**
- **PMP Project Management Professional**

Education

Masters: Cybersecurity (In Progress)
St Louis University – Missouri, United States

Bachelor of Science Computer: Science Honors
NUST – Bulawayo, Zimbabwe

Advanced Diploma/Diploma: Telecommunications System
City & Guilds – London, UK