Zephaniah Williams

Information Technology Profile

Cybersecurity and Information Security Graduate Certified with 3+ years of combined experience managing complex security projects, identifying and mitigating security threats, conducting risk assessments, coordinating response planning, and protecting sensitive data and systems.

Demonstrated ability to identify and mitigate security risks while investigating security incidents/events, creating mitigation responses for better threat handling and mitigation via cross-functional collaboration. Offering subject-matter expertise in systems security, network administration, cloud security, software development, and data management. Committed to protecting sensitive data and information by applying security best practices, maintaining data integrity, and enhancing system functioning. Capable of building risk mitigation plans while facilitating compliance programs and security awareness initiatives in collaboration with cross-functional teams. Keen learner, known for learning new skills and technologies as well as adapting to new environments.

Areas of Expertise

- Cybersecurity & Information Security
- Network, System & Cloud Security
- Vulnerability Scanning
- Incident Response Coordination
- Security Audits & Analysis
- Data Protection
- Security Policy Implementation
- Intrusion Detection
- Sysinternals
- Powershell
- Regulatory Compliance
- Hardware Troubleshooting

Technical Proficiencies

Programming Languages:	Python, Java, JavaScript
Security Technologies:	Firewalls, IDS/IPS, Secure Coding Practices, Vulnerability Assessment Tools
Networking:	TCP/IP, LAN/WAN, Routing & Switching, VPN Configuration
Cloud Platforms:	AWS (EC2, S3, IAM), Microsoft Azure
Operating Systems:	Windows, Linux, Mac
SIEM Systems:	Splunk, Sentinel
Monitoring Tools:	Active Directory, Zscaler, CrowdStrike, Powershell, Nessus, Wireshark

Education

Master of Science in Information Technology Management | WGU, In Progress

Bachelor of Science in Cybersecurity and Information Assurance | Western Governors University (WGU)

Certifications

CompTIA
- Security+ | Network+ | A+ | Pentest+

LPI
- LINUX Essentials

AXELOS
- Information Technology Infrastructure Library (ITIL)

ISC2 SSCP
- Security System Certified Professional

Professional Experience

Night Auditor – Information Security | 2/2024 to Present

Play a vital role in improving service delivery by identifying and mitigating security threats while managing front desk operations. Ensure data accuracy, integrity, and security across multiple platforms by utilizing financial auditing systems. Amplify system integrity by mitigating discrepancies in guest billing data as well as analyzing/reconciling daily financial reports via SQL-based software. Protect systems and data by implementing and tracking security policies and procedures.

Key Accomplishments:

- Produced accurate reports by resolving discrepancies based on audits in the reporting process.

- Planned and executed the project of migrating in-house systems to the cloud, which enhanced information security and protected customer data.
- Minimized service downtime by enhancing financial management and reservation management systems.

Senior Sales Engineer | 3/2021 to 11/2023

Contributed to optimizing customer acquisition strategies by overseeing client data management and analysis using the CRM system. Facilitated informed strategies and decision-making by data management insights. Enhanced system reliability and user experience (UX) by identifying and troubleshooting software issues with customer management systems in liaison with cross-functional teams.

Key Accomplishments:

- Boosted performance by 26% by developing automation scripts in Excel and VBA while streamlining client reporting.
- Increase sales productivity by 16% through the integration of cloud-based tools for remote sales teams, which led to seamless operation and secure data management.
- Mitigated 20% of errors in client reporting by training junior agents on data management best practices and software tools.

Logistics Specialist | 3/2021 to 10/2021

Ensured timely delivery of packages to designated locations by collaborating with cross-functional teams while monitoring inventory and maintaining stock levels. Streamline logistics operations by ensuring seamless liaison with logistics staff along with warehouse personnel and drivers as well as resolving problems.

Key Accomplishments:

- Contributed to route optimization through strategic planning, and planning efficient delivery routes.

Key Projects

Workstation VM Deployment | Marvel Lab Project

- Created and configured multiple Windows 10 VM workstations, joining them to the Marvel-themed Active Directory domain.
- Installed and managed security tools, such as antivirus and monitoring agents, to enforce endpoint protection policies.
- Tested domain connectivity, user logins, and group policy application to validate proper domain integration and workstation compliance.

Marvel-Themed Domain Controller Lab | Marvel Lab Project

- Deployed a Windows Server VM to create a Domain Controller in a virtual lab environment.
- Configured Active Directory and Group Policy to simulate a realistic enterprise network with Marvel-themed users and organizational units.
- Implemented user permissions, login policies, and administrative delegation to mirror a real-world enterprise setup.

THM Threat Intelligence Tools | TryHackMe Labs

- Utilized open-source threat intelligence platforms such as VirusTotal, AbuseIPDB, and Maltrail to analyze real-world attack indicators.
- Conducted hands-on threat hunting activities and IOC (Indicators of Compromise) correlation exercises to detect malicious behaviors.
- Enhanced defensive capabilities by interpreting threat feeds, leveraging MITRE ATT&CK, and simulating attacker techniques in lab environments.

Simulated SOC & Honeynet Deployment in Azure

- Built a simulated Security Operations Center (SOC) and honeynet environment using Azure services.
- Deployed Windows Server and client VMs, integrating them with Microsoft Sentinel, Log Analytics, and Azure Monitor for security event detection.
- Configured KQL queries, custom workbooks, and alert rules to identify suspicious activity, enabling proactive threat detection and incident response.

Malware Incidents Response Lab |Tech with Jono Lab

- Simulated a virus infection scenario to practice Security Operations Center (SOC) response protocols and improve incident handling.
- Utilized tools like Microsoft Defender, Windows Event Viewer, and Sysinternals Suite to identify malware behavior and malicious processes.
- Documented containment, eradication, and recovery steps based on SOC workflows, emphasizing communication and escalation procedures.
- Strengthened understanding of real-world detection techniques, endpoint protection, and response strategies used by Tier 1 SOC Analysts.