Mbekezeli Sithole

mbekezelisithole@duck.com
github.com/mbekesithole
linkedin.com/in/mbekezeli-sithole-923145243

SUMMARY

Proactive Cybersecurity and Network Engineering professional with hands-on experience in cloud security, SIEM technologies, and network troubleshooting. Skilled in implementing robust security measures using Azure services and developing KQL queries for threat detection.

EDUCATION

BSc Cybersecurity and Information Assurance — Western Governors University (Expected 2025)

CERTIFICATIONS

Azure Security Engineer AZ500
CCNA
CompTIA Security+

PROJECTS

- **Implementing a SOC and Honeynet in Azure**
  Source: https://github.com/mbekesithole/Azure-SOC
  Platforms and Technology Used: Azure Virtual Machines, Microsoft Sentinel (SIEM), Log Analytics
- **Enabling and configuring Microsoft Azure Firewall**
- **Used TCPdump to capture and analyse TCP traffic**

WORK EXPERIENCE

Company: Log(N) Pacific — 20/03/2024 - Present
Title: Cyber Security Support Engineer (Intern)

- Implement secure cloud configurations using Azure Private Link, Network Security Groups, Microsoft Defender for Cloud, and Azure Regulatory Compliance for NIST 800-53.
- Troubleshoot and support Microsoft Azure services, including Microsoft Sentinel (SIEM), Virtual Machines, Azure Monitor, and Azure Active Directory
- Develop KQL queries to support Log Analytics workspace and Microsoft Sentinel

SKILLS AND TECHNOLOGIES

Routing and switching protocols, Microsoft Office Suite, Network Security Groups, Firewalls, ACLs (Access Control Lists), Virtual Machines, Virtual Networks, Active Directory, File Permissions, Windows and Linux OS, SIEM, Sentinel, Splunk.