

Mbekezeli Sithole

+447765955527

<https://mbekezelisithole.site>

mbekezelisithole@duck.com

github.com/mbekesithole

linkedin.com/in/mbekezeli-sithole-923145243

SUMMARY

Detail-oriented and proactive Cybersecurity and Network Engineering enthusiast with hands-on experience in cloud configurations, network troubleshooting, and customer IT support. Strong background in implementing robust security measures using Azure, and guiding users to mitigate network issues. Adept at using various technologies including SIEM, Azure services, and firewalls to improve network efficiency and security.

EDUCATION

BSc Cybersecurity and Information Assurance

Western Governors University (Expected 2025)

CERTIFICATIONS

Azure Security Engineer (Expected Nov 2024)

CCNA

CompTIA Security+

Google Cybersecurity Professional

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

- **Static website deployed on Azure**

Source: [GitHub - mbekesithole/portfolio_html_css_js](https://github.com/mbekesithole/portfolio_html_css_js)

Platform and technologies used: Azure tools, Github Actions, Azure Functions App, Azure Front Door

- **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.