PHATSIMO PHEKO

Cybersecurity Consultant | Security Operations & SIEM (Wazuh) | OCI Certified — Architect · Observability · Foundations

Gaborone, Botswana | +267 770 289 08 | phatsimopheko11@gmail.com | LinkedIn | phatsimopheko.com | GitHub

PROFESSIONAL SUMMARY

Cybersecurity consultant with experience in SOC operations, SIEM deployment, and security event monitoring. Hands-on practitioner in threat detection, alert triage, log analysis, and incident response using Wazuh SIEM across cloud and on-premises environments. Produces daily SecOps reports, assesses alert impact, and drafts remediation recommendations for clients — including authoring internal documentation that standardizes the security reporting methodology. Holds three OCI 2025 certifications with a focus on cloud security, cloud infrastructure architecture, and observability. Actively developing toward a cloud security engineering role at the intersection of security operations and cloud infrastructure.

EXPERIENCE

SOC Analyst / Cybersecurity Consultant

TechBulls Botswana · Gaborone, BotswanaOctober 2023 – Present

- Deployed and configured Wazuh SIEM in a SOC environment, managing agent deployment, log ingestion, and endpoint security monitoring across client infrastructure.
- Performed daily alert triage and security event analysis, investigating potential threats, assessing impact, and escalating incidents through defined response workflows.
- Produced independent SecOps reports detailing threat detection findings, alert severity, and remediation recommendations — enabling the organization to reduce reliance on external security vendors.
- Authored internal documentation standardizing the security reporting methodology, ensuring consistency and quality across daily incident reports.
- Coordinated incident response workflows with clients during security events including agent disconnections and anomalous endpoint activity.
- Monitored client asset health and network security posture continuously, maintaining full endpoint visibility and supporting vulnerability management processes.

Tech Support Intern

Botswana Accountancy College · Gaborone, Botswana *January 2020 – August 2020*

- Delivered technical support to staff and students, resolving hardware, software, and network security issues efficiently.
- Configured and maintained IT equipment and systems, contributing to a stable and secure IT environment.
- Supported network monitoring and troubleshooting activities, gaining foundational experience in network security operations.
- Provided technical onboarding and training to new staff on IT systems and security best practices.

EDUCATION

BSc (Honours) in Computer Systems Engineering *University of Sunderland*

CERTIFICATIONS

- Oracle Cloud Infrastructure 2025 Certified Foundations Associate
- Oracle Cloud Infrastructure 2025 Certified Architect Associate
- Oracle Cloud Infrastructure 2025 Certified Observability Professional
- Cisco CyberOps Associate

TECHNICAL SKILLS

Security Operations: SIEM Deployment & Configuration (Wazuh), Alert Triage, Threat Detection, Log Analysis & Correlation, Security Event Monitoring, Incident Response, Endpoint Security, Vulnerability Management

Cloud Security: Oracle Cloud Infrastructure (OCI), Identity & Access Management (IAM), Cloud Security Monitoring, Cloud Observability, Cloud Infrastructure Architecture

Network Security: Network Security Monitoring, Network Traffic Analysis, SOC Operations, Threat Detection Lifecycle

Reporting & Documentation: Security Incident Reporting, SecOps Report Analysis, Remediation Documentation, Security Policy Writing

Programming: JavaScript

Web: React, Next.js, HTML/CSS, TailwindCSS

Databases: MySQL, OracleDB, SQLite

Tools: GitHub, Figma