Ontebile Paul Ntwaetsile

Gaborone, Botswana | (+267) 74458311 | ntwaetsilepaul@gmail.com
LinkedIn: linkedin.com/in/paul-ntwaetsile-a46067244

Professional Summary

Results-driven Cybersecurity Analyst with hands-on SOC experience in vulnerability management, security monitoring and incident response. I am skilled in monitoring, triaging and escalating threats in Microsoft security tools (Defender & Sentinel), applying secure configurations across Linux environments and leveraging tools like Rapid7 InsightVM, Fortinet, and Endpoint Central. Proven ability to reduce vulnerabilities, harden endpoints and support compliance standards. Holds ISC2 Certified in Cybersecurity and Microsoft Azure Fundamentals, with strong networking and system administration foundations.

Education

Bachelor of Science in Computer Science
University of Botswana | Aug 2021 - May 2025

Certifications

- Certified in Cybersecurity | ISC2 | Dec 2024 – Dec 2027
- Play It Safe: Manage Security Risks | Google | Aug 2024
- Foundations of Cybersecurity | Google | May 2024
- Microsoft Certified: Azure Fundamentals | Microsoft | Aug 2024

Professional Experience

Junior SOC Analyst

Cyber Intelligence Agency, Gaborone, Botswana | July 2025 – present

- Monitored and triaged security incidents in Microsoft Defender, escalating threats for remediation.

- Managed vulnerability scans in Rapid7 InsightVM and applied patches and secure configurations via Endpoint Central to close vulnerabilities and strengthen endpoint security posture.
- Involved in day-to-day SOC operations, enhancing incident detection and escalation workflows.
- Perform daily incident and alert monitoring reports supporting continuous improvement in SOC visibility and response.

Information Security Analyst (Industrial Attachment)
Mascom Wireless, Phakalane, Botswana | June 2024 – July 2024

- Conducted vulnerability assessments on 50+ endpoints, documenting and prioritizing exposures.
- Investigated and responded to security incidents using Microsoft Defender and SIEM tools.
- Applied DISA STIG-compliant configurations on RHEL systems using OpenSCAP and shell scripting.
- Monitored network traffic and login attempts via Fortinet tools, identifying security threats.
- Collaborated with infrastructure teams to maintain compliance and strengthen IT security posture.

Technical Skills

Cybersecurity & Tools: Microsoft Defender for Endpoint, Rapid7 InsightVM, Fortinet, Endpoint Central, Microsoft Sentinel(SIEM), Threat Hunting
Networking & Systems: TCP/IP, Firewalls, Windows, Linux Administration
Databases & Query Languages: PostgreSQL, MySQL, KQL(Microsoft Sentinel)
Programming : Python, Java, JavaScript
Cloud : Microsoft Azure
