HAZVINEI NOMATTER MASIYA

Cybersecurity Analyst | Security Operations & Threat Detection Engineer

Location: Zimbabwe | Domain: masiya-hub.org | GitHub: github.com/hnmasiya

PROFESSIONAL SUMMARY

IT professional with 9+ years of enterprise infrastructure experience transitioning into dedicated cybersecurity engineering and Security Operations (SOC). Currently pursuing a BSc in Computer Science, combining formal academic grounding with practical expertise managing enterprise Windows Server environments, Active Directory, access control, and network defense.

TECHNICAL SKILLS & TOOLING

Security Operations:	SIEM (Wazuh, Splunk), Alert Triage, Log Analysis, Threat Hunting, MITRE ATT&CK
Detection Engineering:	Custom YARA Signatures, SPL Queries, Event Log Analysis (IDs 4728, 4732, 4625)
Network & DFIR:	Wireshark, PCAP Traffic Analysis, Nmap Scanning, Packet Inspection
Systems & Cloud:	Active Directory, Windows Server, Linux, Python, GCP, Terraform

KEY PROJECTS

Active Directory Security Log Parser (Python)

- Engineered automated Python tooling to analyze Windows Event Logs for anomalous privileged group escalation.

Wazuh SIEM Detection Engineering Lab (Wazuh, MITRE ATT&CK)

- Designed custom Wazuh XML detection rules mapped to MITRE ATT&CK tactics with automated response integrations.

GCP Secure Multi-Tier Cloud VPC (Terraform)

- Built production-ready cloud network architecture using Terraform IaC with strict IAM access policies.

EDUCATION & CREDENTIALS

- **BSc in Computer Science** - Ongoing Candidate

- **Diploma in Information Technology** - Macmaine School of Computing
- **CompTIA Security+ Certified**
- **Google Cybersecurity Professional Certificate**