# HAZVINEI NOMATTER MASIYA

**IT Professional | Cybersecurity Professional | Founder**

Harare, Zimbabwe | **GitHub:** https://github.com/hnmasiya | **Portfolio:** https://masiya-hub.org | **LinkedIn:** https://www.linkedin.com/in/hazvinei-masiya/

**Remote · Hybrid · On-site · Relocation**

## PROFESSIONAL SUMMARY

CompTIA Security+ Certified (SY0-701) cybersecurity professional with 12+ years of enterprise IT experience across infrastructure, systems administration, Windows/Linux environments, Active Directory, networking, access control, endpoint security, system hardening, and business-critical operations. Transitioning this enterprise foundation into security operations, with hands-on capability demonstrated through completed and authorized labs covering Wazuh SIEM, Splunk, detection engineering, incident investigation, DFIR, Windows/Sysmon telemetry, network security, vulnerability assessment, cloud security, threat hunting, and security automation. Professional experience is clearly separated from independent security work.

## CORE COMPETENCIES & TECHNICAL SKILLS

- **Security Operations & SIEM:** Wazuh SIEM, Splunk/SPL, Sysmon, alert triage, log analysis, security-event investigation, FIM
- **Detection Engineering:** Custom Wazuh rules, Sysmon detection logic, Sigma concepts, MITRE ATT&CK mapping, detection validation
- **Incident Response & DFIR:** Linux authentication/system forensics, PCAP analysis, IOC extraction, hash verification, evidence preservation, investigation workflows
- **Enterprise Infrastructure Security:** Windows 10/11, Windows Server, Active Directory, Group Policy, Microsoft 365, RBAC, least privilege, endpoint hardening, patch management
- **Network & Vulnerability Security:** Nmap, Wireshark/Tshark, Burp Suite, DVWA, OWASP Juice Shop, LAN/WAN, Dell Versa SD-WAN, Sophos XG
- **Cloud, IaC & Automation:** GCP, Terraform, Azure Windows security lab, GitHub Actions, Python, Bash, PowerShell, YAML

## PROFESSIONAL EXPERIENCE

**Jan 2021 – Present** **IT Support Specialist (Contract & Consulting)** | Zuetech Technology Solutions

- Provide enterprise IT support, infrastructure administration, network operations, and onsite client deployment services across multiple environments.
- Administer Active Directory, RBAC, least-privilege access, Group Policy and Microsoft 365; troubleshoot authentication, endpoint and application issues.
- Monitor endpoint, network, and system activity for anomalies, applying security-aware triage principles to identify and escalate security-relevant incidents.
- Deploy and configure Dell Versa SD-WAN appliances, including VOS upgrades, IP configuration, migration support, and connectivity validation.
- Deliver endpoint protection, patch deployment, vulnerability mitigation, and technical documentation across client networks.
- Install and configure Yeastar P-Series PBX/UCaaS solutions for reseller clients as part of enterprise communications and infrastructure deployments.
- Client project — Network Infrastructure Upgrade, Mastercard Zimbabwe (Mar–Apr 2022): installed sensor LAN cabling, decommissioned legacy Cisco switches/controllers/APs, and racked/installed new Aruba controllers, switches, and access points.
- Client project — SD-WAN Circuit Deployment, SITA AERO (Jul 2026): configured two Dell Versa VEP1485 appliances via console CLI, connected each to dedicated internet circuits, and verified connectivity.
- Client project — Qatar Airways VOS Upgrade & SD-WAN Migration, Harare Airport Back Office & City Office (Aug 2026): performed VOS upgrading, device onboarding, and SD-WAN migration on Dell VEP1425 appliances.

**Jan 2019 – Dec 2020** **Desktop Support Technician** | Raising Dawn Investment

- Administered user accounts, permissions, and security groups for 120+ users; supported access-control administration.
- Monitored Sophos Endpoint Protection and firewall telemetry, escalating security anomalies and endpoint issues.
- Supported backup, recovery, and business continuity operations, maintaining technical and operational documentation.

**Jan 2016 – Dec 2018** **Information Technology Support Technician** | Compusys Technology

- Delivered desktop, network, and infrastructure support across multiple client environments; managed user access controls and permissions.
- Applied security patches, supported vulnerability remediation, and investigated authentication/access-control issues.
- Client project — IT Equipment Deployment and Configuration, Ericsson Zimbabwe (Nov 2016–Dec 2018): re-imaged laptop fleets, joined devices to the domain, configured email access, and installed network switches/access points.

**Mar 2014 – Dec 2015** **Help Desk Support Technician** | shermanit

- Supported 200+ users across multiple business locations, providing remote and onsite technical support within defined SLA requirements.
- Troubleshot hardware, software, networking, and authentication issues; supported software deployments and infrastructure updates.
- Client project — IT Infrastructure Upgrade, AJP Group (May–Aug 2015): retired outdated systems, onboarded new devices to the domain, implemented VoIP phone systems, and migrated data to new systems.

**Jul 2012** **IT System Migration and Setup (Contract)** | Abbeydale Group

- Engaged as outside technical support prior to formally joining shermanit: migrated servers, installed HP switches, re-imaged PCs, joined computers to the domain, connected VoIP phones, decommissioned outdated computers with secure data disposal, and reconnected IP cameras to new PoE switches.

## SELECTED CYBERSECURITY PROJECTS

**Windows Sysmon / Wazuh LSASS Detection Validation**

- Captured and validated Sysmon Event ID 10 telemetry from a self-owned Windows Server lab through Wazuh Agent 003 (dc01-lab).
- Correlated process access to `lsass.exe` with custom Wazuh detection logic, including observed event records and `GrantedAccess` values.
- Mapped the investigation to MITRE ATT&CK T1003.001 and T1059.001 while distinguishing observed LSASS access from proof of successful credential dumping.

**Wazuh SIEM Rules & FIM Lab**

- Authored custom XML detection rules for authentication and privilege-related activity and validated rule behavior against controlled

test events.
- Configured File Integrity Monitoring across critical Linux system binaries and configuration files and documented validation methodology.

**Splunk SOC Lab Track**

- Completed a six-lab Splunk SOC track covering SSH authentication hunting, Windows/Sysmon process investigation, web-attack investigation, SPL detection engineering, SOC monitoring/dashboarding, and end-to-end incident investigation.
- Built and validated SPL searches, detection/alert logic, dashboards, synthetic telemetry ingestion, investigation reports, and reproducible evidence; portfolio artifacts distinguish controlled local training from production experience.

**Linux Incident Response & DFIR**

- Analyzed Linux authentication and system logs to reconstruct post-incident attack timelines.
- Verified SHA-256 evidence integrity and mapped unauthorized SSH activity to MITRE ATT&CK.

**Active Directory Security Event Automation**

- Developed Python tooling to parse Windows Security XML event logs (4624, 4625, 4728).
- Automated identification of suspicious authentication and privileged group-membership activity for investigation.

**PCAP Traffic & Triage Automation**

- Processed captured network traffic using Tshark and custom Python parsing scripts to identify suspicious HTTP requests, hosts, protocols, and indicators of compromise.
- Automated triage of web-application scanning and SQL-injection patterns in controlled laboratory traffic.

## CYBERSECURITY VIRTUAL EXPERIENCE

**Mastercard Cybersecurity Job Simulation — Forage | Completed September 20, 2026**

- Designed a phishing email simulation and analyzed supplied phishing-campaign results to support security-awareness training.
- Created a phishing-awareness presentation covering phishing tactics, red flags, reporting and prevention.
- **Skills:** cybersecurity, security awareness, phishing analysis, security training, data analysis, data visualization, communication, problem solving and strategy.

**Datacom Cyber Security Operations Job Simulation — Forage | Completed September 20, 2026**

- Investigated a simulated cyberattack and documented findings, indicators, response priorities and security recommendations.
- Conducted a comprehensive cybersecurity risk assessment using a 5×5 likelihood/consequence approach across phishing, ransomware, third-party exposure, e-commerce/AWS and remote-access risks.
- **Skills:** information security, OSINT, research, risk assessment, risk management, security analysis, analytical skills and communication.

> Forage virtual job simulations; not employment with Mastercard or Datacom.

**Deloitte Australia Cyber Job Simulation — Forage | Completed October 4, 2026**

- Analysed simulated web activity logs to investigate suspicious automated API activity and identify abnormal request patterns.
- Applied networking and web-security concepts to assess authentication/session behaviour and potential public-internet exposure.
- **Skills:** log analysis, web security, networking, incident investigation and suspicious-activity analysis.

**AIG Shields Up: Cybersecurity Job Simulation — Forage | Completed October 4, 2026**

- Researched CISA advisories and reported vulnerabilities, identified affected infrastructure and assessed security risk in a simulated environment.
- Drafted a remediation advisory and completed a controlled ransomware-recovery exercise using Python against provided training material.
- **Skills:** threat analysis, vulnerability research, incident response, security communication and Python.

> Forage virtual job simulations; not employment with Mastercard, Datacom, Deloitte Australia or AIG.

## CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

- **CompTIA Security+ (SY0-701)** — CompTIA
- **ICSI/CNSS Certified Network Security Specialist**
- **Google Cybersecurity Professional Certificate** — Google
- **Google IT Support Professional Certificate** — Google
- **Cisco Junior Cybersecurity Analyst Career Path**
- **Cisco Network Technician Career Path**
- **Cisco Introduction to Cybersecurity**
- **Google AI Essentials** — Google
- **IBM SkillsBuild AI Fundamentals** — IBM SkillsBuild
- **GRC Fundamentals**

## EDUCATION

- **BSc in Computer Science** — Unicaf University (In Progress)
- **Diploma in Information Technology** — Macmaine School of Computing
- **Diploma in PC Maintenance and Networking** — Macmaine School of Computing