CURICULUM VITAE

Munyaradzi Gudo

25 Marlin Crescent, Strandfontein, 7798, Cape Town
Cell: +27 78 803 4287, +27 67 816 6382; Email: munyaradzigudo@gmail.com

CAREER OBJECTIVE

A proactive and motivated Cyber Security Specialist with 7+ years of exceptional experience in network security and administration, seeking a challenging and varied position that will enable me to capitalize on my professional experience, with opportunities for personal and professional development.

BACKGROUND SUMMARY

- Sound knowledge and hands-on experience with IT security technologies and architecture with a strong interest to learn
- Demonstrated excellent verbal and written communication skills, presentation and leadership skills
- Stellar background in Vulnerability Management, Security Incident Management, Forensic Analysis
- A results-oriented and focused team player who derives satisfaction from success
- The ability to spot, document and assess security risk wherever they exist
- Possess good knowledge of threat and security risk modelling
- Creative, independent with expert critical thinking, investigative & analytical problem-solving skills

Key Skills

- Network design, implementation, configuring and troubleshooting enterprise-wide LANs, WANs, WLANs, VPNs
- Proven knowledge in implementing network security solutions and practices in multiple platforms and technologies including Windows, Linux, Android, Oracle, Juniper, Cisco, Palo Alto, Fortinet, etc.
- Strong knowledge of perimeter security controls - IDPS, Firewalls , WAF, Network Access Control systems (NAC), Identify & Access Control Anti-Virus/Malware and patch management
- Endpoint security – Installation, configuration, maintenance & support of Symantec Endpoint Protection (SEP) 12.X, McAfee, Checkpoint and Kaspersky endpoint security solutions
- User activity monitoring systems, data loss prevention systems (DLP) and Security Information & Event Management (SIEM) systems (Splunk, MacAfee, AlienVault)
- Knowledge of integrating security in emerging technologies – Wireless, BYOD, cloud computing, virtualization technologies – VMWare, Hyper-V
- Possess good knowledge of security and risk standards including NIST, ISO 27001 and ITIL
- Ability to seek out and reporting vulnerabilities and security gaps in IT infrastructures - Nessus, GFI LanGuard, ZenMap, Hping3, Netcat, MBSA, OpenVAS, Accunetix, OWASP ZAP, Qualys, etc.
- Hands-on experience in conducting risk assessments, security audits, network mapping, vulnerability assessment and penetration testing – Nmap, Kali Linux, Metasploit, SolarWinds, Cain & Abel, Netcraft, Wireshark, Social Engineering Toolkit, etc.
- Strong background in vulnerability research, cyber threat detection, investigation & containment
- Exceptional knowledge of security vendors and security product capabilities
- Solid experience in administering Identity and Access Management technologies – IBM, System Centre, Active Directory (AD), GPO's, Windows File Services, Active Directory Federated Services, and password/identity management systems, DNS, LDAP, DHCP
- Expert experience with enterprise Information Security, asset/infrastructure security, Compliance, Risk Management and/or IT Governance issues and challenges
- IT Risk Management and Information Security Standards/Frameworks - ISO27001/2, PCI-DSS, NIST 800-30 and NIST-RMF
- Other tools ServerScan, SolarWinds, HackerGuardian, ServiceNow, Jira, CIS CAT, BurpSuite,

CompTIA Security+ CERTIFIED · CE

CEH Certified Ethical Hacker

WORK EXPERIENCE

Senior Systems Security Engineer – University of Cape Town, Cape Town, Aug 2019 to Current

- Provide input to the IT security strategy and IT security enhancements
- Assist with development of the IT security policy, procedures and standards Implement, maintain and ensure adherence to information security framework and information security plan
- Participate in defining and maintenance of enterprise and application security controls, and standards for production systems.
- Perform vulnerability testing, penetration testing, risk assessment and technical and security compliance assessments, recommending mitigating controls for identified limitations and risks.
- Communicate information security and compliance risks to senior level management clearly and concisely ensuring they are fully defined and understood.
- Conduct Network Security and Auditing on infrastructure
- Maintain appropriate security measures and mechanisms to guard against unauthorized access and protect against reasonably anticipated threats and hazards Ensure that vulnerabilities are resolved in a timely manner
- Configure and monitor a variety of security devices and tools, including but not limited to: Anti-Virus, Endpoint Security, IDS/IPS, WAF, Firewalls, SIEM, NAC & patch management
- Devise and communicate incident response procedures, respond immediately to security incidents and provide a thorough post-event analysis.
- Provide Information Security consultancy for Technology and business projects
- Evaluate and select various security technologies for suitable inclusion in IT solution designs.
- Work closely with client project managers to ensure security requirements are effectively addressed in all phases of project lifecycles.
- Develop and support Cyber Security awareness programs and security educational efforts

Cyber Security Specialist (Technical Manager) – SecuriCentrix (CyberGuard Security Group), Jan 2016 to Jul 2019

- Maintain comprehensive knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the identification and resolution of vulnerabilities and threat vectors.
- identify, facilitate risk analysis, documentation, remediation and mitigation of IT risks for clients
- conduct IT risk monitoring reviews and risk assessments to facilitate decision support
- Perform vulnerability and network assessment scanning to determine whether information systems are protected, controlled and provide value to the organization.
- Conduct hands-on penetration testing, through simulation of controlled attacks on the system to highlight or find any attack vectors, vulnerabilities and weaknesses that might be exploited by a hacker e.g. ISO27001, PCI-DSS & GDPR assessments
- Actively participate in the deployment, initial configuration, upgrading, managing, and maintaining Firewalls, IDPS, VPN concentrators, Switches, and other network security solutions
- Apply operating system updates, patches and make configuration changes and apply preventive measures to tighten security.
- Monitoring network traffic and reviewing device logs to detect malicious behaviors and troubleshoot communications problems between systems.
- Network design, implementation and maintenance
- Network performance, security and compliance monitoring
- Setup, configuring and troubleshooting enterprise-wide LANs, WANs, WLANs, VPNs
- Develop a comprehensive security strategy that covers prevention, detection, and response along with the technology stack to support it
- Evaluate the information security and privacy policies, standards and procedures for completeness, alignment with generally accepted practices and compliance with applicable external requirements.
- As part of a Security Incident Response Team (SIRT) help to develop and execute a clear incident response and disaster recovery strategy that effectively monitor and identify security incidents, recover lost data, contain and mitigate security issues.

CompTIA Security+ CERTIFIED · CE

CEH™ Certified Ethical Hacker

- Manage the periodic maintenance of security systems and applications to ensure new threats are identified and managed and the security of the organisation's assets are maintained
- Assist with security breach investigations to guide the refinement of information security policies and practices
- Develop collaborative and trusted relations with key vendors, partners and other IT and Business stakeholders and ensure company compliance with standards and regulatory bodies

Senior IT Security Officer – Cabling for Africa, May 2011 – Dec 2015

- Help management plan and carry out an organization's information security strategy and budget which continues to support the organization's objectives.
- Design, configure, deploy, and maintain the company enterprise security infrastructure
- Actively protect company information technology assets and infrastructure from external or internal threats and ensure that the company complies with statutory and regulatory requirements regarding information access, security and privacy
- Analyze data from threat and vulnerability feeds and use the data for applicability to the organization.
- Configure and monitor a variety of security devices and tools, including but not limited to: Anti-Virus endpoint, IDS/IPS, Firewalls, SIEM, NAC, patch management, and Vulnerability Management tools, etc.
- Perform business, operations and network technology assessments to evaluate your overall security posture.
- Evaluate risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed.
- Review company's security controls, test and evaluate effectiveness of business processes, procedures and controls to ensure they align with the organization's strategies and objectives.
- Performing various other reviews of IT management policies and procedures such as change management, business continuity planning/ disaster recovery and information security to ensure that controls surrounding these processes are adequate
- Information Security/ IT Governance
- Implement the information security (IS) strategy and proactively identify cyber-security threats
- Inform the rules and or configuration and policy settings that should apply on Security controls based on incidents and threat intelligence
- Network design, implementation, configuration and troubleshooting including network performance, security and compliance monitoring
- Configuration management of networking and security technologies
- Conduct patch management and integrating several system hardening tools, processes and procedures to eliminate security risks on client networks.
- Assisting with the monitoring and reporting of all compliance risks and implementation of key compliance policies and procedures across the business.
- Take part in creating and reviewing a solid set of IT security policies to protect sensitive information and corporate Intellectual Property from theft, misuse and abuse
- Implement network security policies, application security, access control and corporate data safeguards
- Execute specific security audits (e.g. vulnerability and network assessment scanning, penetration testing) to determine whether information systems are protected, controlled and provide value to the organization.
- Research, analyze, and formulate recommendations regarding technologies, products, and solutions to ensure systems are protected, controlled and provide value to the organization.
- Conduct need-based awareness and hands-on training to staff on cyber threats, attack vectors and use of security solutions and procedures to protect against cyber security threats and potential data exposure

CompTIA Security+ CERTIFIED · CE

C|EH Certified Ethical Hacker

Systems Administrator – Zimbabwe Reinsurance Company, Mar 2009 – Dec 2010

- Setup, configuring and troubleshooting enterprise-wide LANs, WANs, WLANs, VPNs
- Implementing, configuring, maintaining, monitoring, supporting, and improving all new and existing network hardware, software, and communication systems
- Contributing to distributed computing management, which includes resolving system integration issues, coordinating and prioritizing application upgrade deployments, patch management, configuration management and developing policies, standards, service level, documents and processes
- Ensure that the network is operational and stable through the effective management of security solutions, establishment of effective monitoring tools for the network, including firewalls, patches, antivirus solutions and intrusion detection systems
- Monitor the performance of computer systems, OS hardening and creating baselines and coordinate access and use of IT infrastructure.
- Development of data and information policy
- Find security gaps by performing routine audits of hardware and software entities on the network and closing those gaps.
- Computer security - Development of the company information security policy based on ISO standards, identifying opportunities and implementing solutions for loss prevention, cost serving, and improvement of data integrity and quality, improvement of information delivery and business processes as well as daily backups
- Provide technical input, evaluate and recommend new and emerging security products and technologies to support monitoring local and cloud based dynamic environments
- Provide end user support / problem-solving services for the company employees on all IT related system
- Responsible for management of Service Level Agreements with different service providers
- Actively participate in the didactic and experimental training of users in respect of data analysis and management.

Professional Qualifications

1. Certified Ethical Hacker (CEH), EC-Council, 2017
2. CompTIA Security+, Computing Technology Industry Association (CompTIA), 2018

Academic Qualifications

1. Bachelor of Science Computer Science Honors Degree, Midlands State University, 2008
2. Diploma in teaching, training and assessing learning, City & Guilds, 2015

Research Publications

Gudo, M., & Padayachee, K. (2015, September). SpotMal: A hybrid malware detection framework with privacy protection for BYOD. In Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists (p. 18). ACM Digital Library.

Interests & Hobbies

Research and technology publications.

References

To be provided on request