|  |  |
| --- | --- |
| WATSON NKOMO  Security Analyst  **Summary Statement:** | horizontal line Watson Nkomo 504 Dundonald Mansions  272 Bree Street  City of Johannesburg  +27 83 724 8693  [wattienk@gmail.com](mailto:wattienk@gmail.com)  linkedin.com/in/watson-nkomo-188216a6  Dedicated and detail-oriented **Cybersecurity Analyst** with a strong background in network security, vulnerability assessment, and incident response. Passionate about safeguarding critical systems and data from cyber threats. Holds industry-recognized certifications including **Google Cybersecurity Certificate** and **CompTIA Security+** |
| **ㅡ** Key Skills & Experience | horizontal line   * Conduct regular vulnerability assessments using tools such as Metasploit and Nessus. * Monitor network traffic for suspicious activity and respond to security incidents promptly. * Collaborate with cross-functional teams to implement security best practices. * Maintain and configure firewalls, intrusion detection systems, and SIEM tools. * Investigate security breaches and recommend remediation strategies using OWASP Principles, OS Hardening Technique & Zero Trust (Principle of less privilege, defense in depth, separation of Duties, MFA). * Security risk management by Applying NIST CSF, ISO 27001, NIST RMF, assessing risk using NIST SP 800 & Maintain security posture using CIA Triad. * Security Auditing using audit checklist and Trouble shooting. * Automate cybersecurity tasks with Python & filter queries using SQL. * Conducting Cybersecurity training or awareness and integrating AI into Cybersecurity. * Using Wireshark & TCPDump to capture packets. * Ethical Hacking into systems- (offensive security /Pentesting). * Using Playbooks with SIEM Tools (Splunk & Chronicle). * Threat Landscape knowledge, understanding the Pyramid of Pain, threat hunting & triaging of incidents & Employing Virus Tool or Metadefender Cloud – OPSWAT for threat hunting/ Intelligence employing MITRE ATTACK analysis -Diamond Model & Cyber Kill Chain framework * Documenting, Reporting, escalation of Incidents & effective communication with stakeholders and collaborating with a team. * Attention to detail & problem-solving skills * Excellent organizational, administration skills, project management and can help companies maintain budget, good reputation   horizontal line |
| Education | * **Google Cybersecurity Certificate**   + Issued by Google   + Completion Date: October 2023   + Topics Covered: Cybersecurity fundamentals, network security, and threat detection. * **CompTIA Security+**   + Issued by CompTIA   + Completion Date: April 2024   + Topics Covered: Network security, risk management & cryptography   + **Try Hack Me**:   + Junior Security Analyst Introduction -Offensive & Defensive   + Security   + Completion Date: November 2023   + **Institute of Governanc****e**   + Diploma In Governance, Peace, Leadership & Civil Society Studies   + Completion Date: 2011   + **St Joseph’s High**   + “O” Level & “   + A” Level   **Languages:** Proficient in Python & SQL  **Operating System:** Linux & Windows |
|  |  |