|  |  |
| --- | --- |
| 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  https://github.com/Watty-1/Watty-1.git  I am a motivated security analyst seeking an entry -level cybersecurity position to apply my skills in network security, security policy, organizational risk management to protect assets and data. |
| **ㅡ** Skills | horizontal line  Ø Linux, Structured Query Language {SQL} & Python  Ø Documenting, Reporting Incidents & Security Mindset  Ø Incident Response & Recovery  Ø Comprehension of MFA, IAM & OWASP principles (Defense in depth, Least privilege, Separation of duties & Fail security)  Ø Ability to use packet sniffers (Wireshark & Tcpdump)  Ø Network security: Firewalls, VPNs, IDS/IPS & employing OS Hardening techniques.  Ø Can help maintain a strong security posture by using Controls & Frameworks like: NIST Cybersecurity Framework (CSF), the NIST Risk Management Framework (RMF), (NIST) Incident Response Lifecycle & CIA Triad model  Ø Threat Landscape knowledge, threat hunting & triaging incidents & understanding the Pyramid of Pain  Ø Communicating with stakeholders & Collaborating with a team  Ø Team work & good people- skills respecting diverse perspectives  Ø Attention to detail & problem-solving skills  Ø Excellent organizational, administration skills  Ø Microsoft Windows, Power Point, Excel & Microsoft Word  Ø Fast to adapt and grasp new concepts with speed & growth mindset |
| ㅡ Experience | horizontal line   1. Using OWASP Principles & OS Hardening Technique   (Principle of less privilege, defense in depth, separation of Duties, MFA)   1. Security risk management by Applying NIST CSF, NIST RMF, assessing risk using NIST SP 800 & Maintain security posture using CIA Triad 2. Security Auditing using audit checklist 3. Automate cybersecurity tasks with Python & filter queries using SQL 4. Phishing incident response using a Playbook 5. Using Wireshark & TCPDump 6. Using Playbooks with SIEM Tools (Splunk & Chronicle) 7. Employing Virus Tool or Metadefender Cloud – OPSWAT for threat hunting/ Intelligence 8. Company/ Organisation: Ministry of Education (Emakhandeni Secondary)   Position: Teacher & Head of Science Department  Responsibility: Teaching and administering as well as managing the day to day running of the entire Science department. Reporting and liaising with the Head of school  REFERENCE: The Head/ Principal Mr. P J Ndlovu  Contact: +263 11821122  9. Company/ Organisation: Self-Empowerment  Position: Facilitator  REFERENCE: Life Skills / Learnerships Administrator Amanda Nxodo  Email: sei04@uiplay.com  Cell: 0810754129  10. Company /Organiasation : Triple E Training  Position: Facilitator  Responsibility: Teaching, facilitating QNF LEVEL 3  REFERENCE: Mayo Agent Management  EMAIL: mayo@eee.co.za/ amc1@eee  Cell: 082 317 5324  11. Company/ Organisation: Qhubani Holdings (Pty) ltd  Position: Project Manager  Responsibility: Administration, Project monitoring & management  REFERENCE: Director Mr. Gideon  Email: qhubanigideon@gmail.com  Cell: 078 903 8120  horizontal line |
| Education | School Name: COURSERACertificate: Google Career Certificate in Cyber Security2023 CompTIA: Studying CompTIA Security +  Try Hack Me: Junior Security Analyst Introduction  Introduction to Offensive Security School Name: Institute of GovernanceDiploma: Governance, Peace, Leadership & Civil Society Studies 2011School Name: St Joseph’s High School Certificate “O” Level & “ A” Level 2005 |
| **ㅡ** Awards | horizontal line  Facilitation & Judging Science Exhibition Certificate  Ministry of Education 201 0 |