EXTERNAL VACANCY ADVERTISEMENT

SECURITY OPERATIONS ASSISTANT (1 POSITION)

Job Summary

Reporting to the Systems Security Officer, the job holder will be responsible for among others monitoring the Information Technology infrastructure and supporting investigation of security breaches and incidence response and perform security impact analysis in the change process.

Key Responsibilities

1. Proactively monitor and report the security posture on all information assets as per Security Operations Center (SOC) procedures by utilizing technical tools such as SIEM, Antimalware, Database Activity Monitoring Systems, Fraud Management Systems, etc.
2. Work in 24*7 shifts performing real time monitoring of security alerts generated by various security tools deployed by the SOC. Analyse and assess security alerts and escalate for further investigations and communication
3. Periodically review systems within the Sacco to ensure that they are configured as per the established security baseline standards. Report any non-compliance on information security policies
4. Be involved in the establishment of mechanisms for information and cyber security incident response management including monitoring, detecting, remediating, and fully investigating security breaches to establish and treat the root cause (s) to minimize future occurrences as well as perform impact analysis.
5. Perform threat intelligence research, including collection of global threat intelligence and internal threats then inject actions based on analysis and recommendations.
6. Offer support in cyber security awareness and training campaigns
7. Document and research security breaches and assess any damage caused.
8. Keep abreast with emerging issues by attending educational workshops, seminars, conferences and participating in professional societies.

- **Partners:** Assess external partners such as vendors' and contractors' procedures, processes and security controls to ensure they adequately protect the organization's business information and transactions.

- **Collaboration:** Work with user departments to ensure information technology threats are properly identified, analysed, communicated, investigated and corrective actions taken.

Qualifications

Technical Skills

1. Bachelor's degree in Information Technology, Computer Science, or any other related field with relevant IT Security professional qualifications i.e. CISA/CISM/CEH or other relevant security certifications.
2. 3 years' experience in Security/Network administration with strong technical knowledge of database, network and operating systems security.
3. Knowledge of various security methodologies and processes and technical security solutions (SIEM, EDR, firewall and intrusion detection systems).
4. Knowledge of TCP/IP Protocols, network analysis, network protocols and network/security applications.
5. Working knowledge and experience in penetration testing and vulnerability assessments.
6. Knowledge of common cybersecurity threats and sources of cybersecurity information.
7. Good understanding and knowledge of risk assessment, risk procedures, security assessment, vulnerability management, penetration testing.

Non-Technical Skills

- Good communication skills
- Problem-solving skills

Qualified applicants should apply on or before 5:00pm on 1 December 2025 using the link provided in the Society's Website.

Only Shortlisted Candidates will be contacted.