Cyber Threats Intelligence Analyst (Ethical Hacker)

Suitably qualified, experienced and motivated candidates are invited to apply for the position of Cyber Threats Intelligence Analyst which has arisen in the Information Systems and Digital Services Department.

Key responsibilities

Reporting to the IS Processes, Risk and Governance Manager, the successful candidate will be responsible for the following, among others:

- Analyzing targeted attacks by external or internal parties and preparing the Information Systems team to mitigate any cyber security threats, which the organization may face
- Review and refine cyber defense strategies for the Bank
- Responsible for hunting and analysis of cyber threats and recommending threat mitigation measures before the Bank is impacted
- Researching threat actors and analyzing the latest threats and attacks
- Carry out cyber security profiling for new products and recommend threat mitigations
- Takes part in policy reviews to capture new threats
- Prepares reports on the cyber security profile of the bank

Skills and Experience

- Excellent analytical, oral and written communication,
- In-depth knowledge of attack methodologies used against the banking and financial sectors
- Strong technical knowledge of security architecture, tools and controls with specific demonstrated experience in proactive detection, mitigation, and resolution of advanced cyber-attacks and/or threats
- In-depth knowledge of information threat hunting and analysis
- Security testing tools use and result analysis (Nessus, Metasploit, Burp/ZAP, Kali, etc.)
- 1 year in Information Security Analysis and Incident Response

Educational Qualifications

- First Degree in Computer Science, Information Systems or a related qualification.
- Ethical Hacking Training (CEH, CPT/GPEN, OSCP, etc.)

Interested persons that meet the above requirements should submit soft copies of their CVs to **appointments@stewardbank.co.zw** no later than 12h00 on the 12th April 2018 with the title, **Cyber Threats Intelligence Analyst** clearly written in the subject line.