VACANCY

Postbank
Your Bank

JOB TITLE	**:**	**HEAD: IT SECURITY**
JOB GRADING	**:**	**D5**
REPORTS TO	**:**	**CHIEF INFORMATION OFFICER**
BUSINESS UNIT	**:**	**IT**
LOCATION	**:**	**PRETORIA**
POSITION STATUS	**:**	**PERMANENT**

Purpose of the Job

Responsible for developing and implementing Postbank IT security strategy, overseeing security measures to prevent cyberattacks, and managing incident response.

Job Responsibilities

- **Information Security Strategy**: Develop and implement comprehensive information security strategies and programs to protect Postbank's information assets.
- **Risk Management**: Identify, assess, and mitigate information security risks to Postbank
- **Compliance**: Ensure compliance with Postbank Information Security and Cyber Security policies, relevant laws, regulations, and industry standards, such as PCI-DSS.
- Security Awareness: Develop and implement security awareness programmes to educate employees on information security best practices.
- **Incident Response**: Develop and implement incident response plans and procedures to respond to security incidents.
- **Security Architecture**: Design and implement secure architectures for systems, networks, and applications.
- **Vendor Management**: Manage relationships with third-party vendors and ensure they comply with Postbank's information security policies and procedures.
- **Security Operations Center (SOC) Operations**: Oversee and manage the day-to-day operations of the SOC, ensuring timely and effective detection, response, and remediation of security incidents.
- **Threat Detection**: Analyse and interpret security event logs, network traffic, and system data to identify potential security threats and vulnerabilities.
- **Security Monitoring**: Monitor security event logs, network traffic, and system data to identify potential security threats and vulnerabilities.
- **Reporting**: Provide regular reporting and metrics to stakeholders on SOC performance, security incidents, and threat intelligence.
- **Training**: Develop and deliver training programs for SOC analysts and other stakeholders on security best practices, threat intelligence, and incident response
- **Encryption keys**: When authorised to do so, provide overall management of encryption keys, including key generation, distribution, storage, and revocation

Qualifications and Experience

Qualifications:

- Bachelor’s degree in computer science, Information Security, or a related field.
- Relevant certifications, such as CompTIA Security+, CISSP, or CISM.

Years of experience:

- 10+ years of experience in information security, including experience in security leadership roles, 10+ years of experience in security operations, incident response, or threat intelligence.
- Banking industry experience, ability to build and maintain relations with banking regulators (FIC, PASA, Bankserv)

Knowledge and understanding of:

Security Frameworks: Knowledge of security frameworks, such as Cybersecurity Framework, ISO 27001, and COBIT.
Security Technologies: Experience with security technologies, such as firewalls, intrusion detection systems, and encryption technologies. **Cloud Security**: Knowledge of cloud security platforms, such as AWS Security Hub, Google Cloud Security Command Center, or Microsoft Azure Security Center. Identity and Access Management: Experience with identity and access management systems, such as Active Directory. **Security Information and Event Management (SIEM)**: Experience with SIEM systems, such as Splunk. **Penetration Testing**: Knowledge of penetration testing methodologies and tools, such as Metasploit, Burp Suite, or Nmap.

Security Orchestration, Automation, and Response (SOAR): Knowledge of SOAR platforms, such as Phantom, Demisto, or IBM Resilient. **Threat Intelligence**: Knowledge of threat intelligence platforms, such as ThreatConnect, Anomali, or IBM X-Force. **Incident Response**: Experience with incident response frameworks, such as SANS Incident Response. **Security Orchestration, Automation, and Response (SOAR)**: Knowledge of SOAR platforms, such as Phantom, Demisto, or IBM Resilient. **Networking**: Knowledge of networking protocols, such as TCP/IP, DNS, and HTTP. Operating Systems: Experience with operating systems, such as Windows, Linux, or macOS

Attributes

- **Communication:** Excellent communication and interpersonal skills.
- **Collaboration:** Ability to collaborate with cross-functional teams, including security, IT, and business stakeholders.
- **Problem-Solving:** Strong problem-solving skills, including the ability to analyse complex security issues and develop effective solutions.
- **Leadership:** Ability to lead and manage a team of security professionals, including SOC analysts and incident responders.
- **Adaptability:** Ability to adapt to changing security threats, technologies, and business requirements.

How to Apply

If you wish to apply and meet the requirements, please forward your Curriculum Vitae (CV) to **RecruitmentSN@postbank.co.za** Please indicate in the subject line the position you are applying for. To view the full position specification, log on to www.postbank.co.za and click on Careers.

Closing Date

13 December 2024

Disclaimers

The South African Postbank SOC Limited is committed to the achievement and maintenance of diversity and equity in employment, especially with regard to race, gender and disability. In compliance with the bank's employment equity plans, first preference will be given to candidates from designated groups. Correspondence will be limited to short listed candidates only.

If you do not hear from the South African Postbank SOC Limited or its Agent within 3 months of this advertisement, please accept that your application has been unsuccessful. The South African Postbank SOC Limited reserves the right not to fill the positions or to re-advertise the positions at any time.

POPIA provides that everyone has the right to privacy, and it includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. By applying for employment, you consent to the processing of your personal information with Postbank. Your personal information and any attached text or documentation are retained by Postbank for a period in accordance with relevant data legislation.