VACANCY
RE ADVERTISEMENT

REFERENCE NR	**:**	**VAC00470/24**
JOB TITLE	**:**	**Lead Cloud Security Architect**
JOB LEVEL	**:**	**D4**
SALARY	**:**	**R 845 277 – R 1 267 915**
REPORT TO	**:**	**Enterprise Architect**
DIVISION	**:**	**IT Infrastructure Services**
DEPT	**:**	**ITI Hosting: Technology, Strategy and Security**
LOCATION	**:**	**SITA Erasmuskloof**
POSITION STATUS	**:**	**Permanent (Internal & External)**

Purpose of the job

The role is responsible for the design, development, engineering and implementation of cloud security architectures, processes and initiatives for cloud services that fulfil legislative obligations and data protection requirements and ensure alignment with the Government and Corporate security acts, policies, and strategies.

Key Responsibility Areas

- Develop and design cloud security architecture strategies, frameworks and reference models
- Provide the project teams with technical leadership on cloud security projects / solutions implementation.
- Identifies, assesses, monitors and evaluates technical risks for cloud solutions
- Collaborate with all IT functional areas to design and support secure technologies to meet business needs, build security controls and solutions for cloud technology in accordance with approved architecture frameworks and standards.
- Develops tactical response procedures for security incidents.

Qualifications and Experience

- **Required Qualification:** 3 year National Higher Diploma in IT /Bachelor's Degree in Computer Science, Information Systems/ Engineering or relevant equivalent to NQF Level 7 Plus Professional certification such as CCSP, Security certification, ISC2, CISSP, CISM, CISA CCNE, Cloud certification, Cloud Security certifications, Cloud Platform and Infrastructure etc. is strongly preferred.
- **Experience:** 7 - 8 years ICT experience in a large corporate/Public sector Organisation which should include:

✓ Experience as a technical lead and architect for security.

✓ Strong experience with security technologies.

✓ Hands on experience with one or more major cloud technologies.

✓ Experience in deploying and securing cloud platforms.

✓ Experience in cloud security compliance.

- ✓ Experience in Cybersecurity, Distributed Denial of Service Attacks, Shared Cloud Computing Services, Data Loss, Phishing and Social Engineering Attacks, Crypto jacking, etc.
- ✓ Experience in design, implementation and operation of large-scale security architecture solutions in a large and complex multi supplier / multi-platform environment.
- ✓ Experience in designing, implementing, and testing cloud security controls. Experience integrating and migrating legacy platforms and applications with cloud-based systems strongly preferred.
- ✓ Experience with enterprise risk assessment methodologies with the ability to evaluate information security risk implications.
- ✓ Infrastructure Security experience.
- ✓ Experience in Engineering cloud security architecture solutions.

Technical Competencies Description

Knowledge of: Deep understanding of cloud architecture. Deep understanding of operational integration of security functions. Strong knowledge of security, and network architecture. Deep knowledge of security best practices, principles, and common security frameworks. Extensive knowledge of systems architecture Deep working knowledge of cloud security frameworks. Good knowledge and understanding of risk management processes and experience in conducting risk assessments. Good knowledge and understanding of business continuity and disaster recovery.

Deep understanding of security management solutions. Extensive knowledge of developing and documenting security architecture and plans, including strategic, tactical and project. Strong organizational and project management skills Thorough understanding of Information Security frameworks and good practices and ability to strike a balance between an academic and pragmatic approach. Extensive knowledge of security issues, techniques and implications across all existing computer platforms Excellent communication and presentation skills (written and verbal). Ability to create, maintain and organize documentation to support architectural standards and principles. Strong project management skills, with a high aptitude in managing multiple projects. Ability to negotiate with multiple stakeholders Good Knowledge of infrastructure, key processes, and technology-oriented risk issues, specifically around security and privacy. Excellent analytical, decision-making, and problem-solving skills as well as project management. Outstanding presentation and persuasion capabilities that elicit confidence and credibility.

Technical Competencies: Hosting Management, Collaboration, Communicating and Influencing, Honesty, Integrity and Fairness, Innovation, Planning and Organising, Creative Problem Solving, Responding to Change and Pressure, and Strategic Thinking.

Interpersonal/behavioural competencies: Attention to Detail, Analytical thinking, Continuous Learning, Disciplined, Resilience, and Stress Management.

How to apply

To apply please log onto the e-Government Portal: www.eservices.gov.za and follow the following process;

1. Register using your ID and personal information;
2. Use received one-time pin to complete the registration;
3. Log in using your username and password;
4. Click on "Employment & Labour;
5. Click on "Recruitment Citizen" to create profile, update profile, browse and apply for jobs;

Or, if candidate has registered on eservices portal, access www.eservices.gov.za then follow the below steps:

1. Click on "Employment & Labour;
2. Click on "Recruitment Citizen"
3. Login using your username and password
4. Click on "Recruitment Citizen" to create profile, update profile, browse and apply for jobs

For queries/support contact egovsupport@sita.co.za OR call 080 1414 882

CV`s sent to the above email addresses will not be considered.

Closing Date: 24 July 2023

Disclaimer

SITA is an Employment Equity employer and this position will be filled based on Employment Equity Plan. Correspondence will be limited to short listed candidates only. Preference will be given to members of designated groups.

- If you do not hear from us within two months of the closing date, please regard your application as unsuccessful.
- Applications received after the closing date will not be considered. Please clearly indicate the reference number of the position you are applying for.
- It is the applicant`s responsibility to have foreign qualifications evaluated by the South African Qualifications Authority (SAQA).
- Only candidates who meet the requirements should apply.
- SITA reserves a right not to make an appointment.
- Appointment is subject to getting a positive security clearance, the signing of a balance score card contract, verification of the applicant's documents (Qualifications), and reference checking.
- Correspondence will be entered to with shortlisted candidates only.
- CV`s from Recruitment Agencies will not be considered.
- CV's sent to incorrect email address will not be considered.