Position description

Position title	Cyber Security Architect
Group / Branch	Finance & Technology/Business Technology Services
Reports to (Title)	Enterprise Architecture and Platform Manager
Competency level	Individual Contributor

Job Purpose

The Cyber Security Architect will be responsible for evaluating, designing and implementing security architectures to ensure the protection of South East Water assets, data and infrastructure. Reporting to the Enterprise Architecture and Platform Manager, design and maintain the security architecture required for the technology portfolio aligned to the organisational strategies.

You will work closely with the Enterprise security & resilience, IT and OT teams ensuring security is embedded by design across the technology projects, platforms, systems and business solutions.

Key Accountabilities

- Develop and maintain the security architecture blueprint that aligns with the enterprise architecture
- Design and maintain security reference architectures and patterns for use across data, digital platforms, systems, Hybrid cloud infrastructure and operational technologies
- Provide specialist advise on architecture supporting major programs, projects and initiatives
- Contribute to the Enterprise Architecture repository ensuring security capabilities are tracked and visible across the technology portfolio
- Support selection, integration and architecture alignment of key security tools and platforms
- Ensure architectural designs and security controls are aligned with industry frameworks (NIST, VPDSS, ISA 62443, Essential 8, CIS, etc.) and security best practices
- Secure data governance, infrastructure, BTS NWW/SDLC and support DevSecOps
- Contribute to architecture and security forums such as Architecture and Security Review Board.
- Able to work on multiple tasks spanning; strategies, roadmaps, projects and BAU activities.

- Assist in the development of security policies, standards, and guidelines.
- Provide architecture inputs into security audits, risk assessments, compliance reviews and operations

Knowledge, Skills & Experience

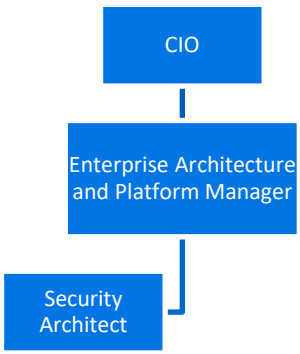
- 5+ years of experience in cybersecurity architecture and consulting
- Hands-on experience with threat modelling, advanced security designs and automation
- Expertise in enterprise security architecture with a focus on cloud (Azure, AWS), network, SaaS\PaaS\IaaS and application security
- Expertise in on-prem infrastructure and network security architecture
- Expertise in multi-tier application architecture
- Familiarity with security frameworks and compliance requirements (e.g., NIST, VPDSS, ISA 62443, CIS, ISO 27001, SOC 2).
- Familiarity with DevSecOps, secure-by-design and zero-trust architectures
- Strong knowledge of architecture practices and security technologies (SIEM, SOAR, XDR, IAM, DLP, WAF, CASB, Cryptography)
- Ability to communicate complex security concepts to technical and non-technical stakeholders
- Strong analytical and problem-solving skills with the ability to assess security risks and applying appropriate architectural patterns

Education and Formal Certifications:

- Bachelor's degree in computer science, Cybersecurity, Information Security, or a related field (or equivalent experience)
- Industry certifications such as CISSP, TOGAF, CCSP, SABSA, or equivalent.

Dimensions

Organisational Chart



Number of people managed: N/A

Size of budget managed: N/A

Value of Assets managed:

Describe the level/type of responsibility the role has over the organization's assets, both physical and non-physical

Ensuring a sustainable, resilient organisation:

Authorities outlined in **Instrument of Delegations** None

Compliance management responsibilities outlined in the **compliance and obligations register** None

Security for Critical Infrastructure identified role: No