Position description

Position title	*Cyber Security Engineer*
Group / Branch	*Finance & Technology/Business Technology Services*
Reports to (Title)	*Cyber Security Team Lead*
Competency level	Individual Contributor

Job Purpose

South East Water is looking for an experienced Security Engineer, who will work closely with the Cyber Security team and the broader IT and OT departments to manage the tools and technology, threats, reduce risks and vulnerabilities, and implement new security technologies and processes to improve overall security posture.

Key Accountabilities

- Perform advanced threat hunting based on the security alerts from various monitoring channels including SOC and initiate appropriate response to mitigate risks in a timely manner
- Manage security threats and incidents as per the cyber response procedures and playbooks, feeding the intel into improving the security posture and organisation resilience
- Deliver security risks assessments and controls evaluation where needed, including business impact analysis and provide assurance that the SEW Information assets and data are appropriately protected
- Configure, maintain and enhance the security tools and operating procedures, thus ensuring their effectiveness and optimization for security operations
- Investigate and manage complex vulnerabilities and exposures implementing appropriate remediation controls and change management in a hybrid multi-cloud, on-premise managed IT and OT environment
- Secure SEW identities including privileged accounts through frequent reviews and managing identified risks.
- Implement security controls to protect hybrid IT infrastructure including Cloud and SaaS Apps
- Represent Cyber Security on internal governance forums such as Architecture and Security Review Board, Change Advisory Board and industry forums; support projects, procurement, and business activities
- Review, develop and maintain the response plans, procedures and playbooks as per the evolving threat landscape and changing South East Water technology and business environments

- Ensuring that the alert response and resilience metrics are met and exceeded
- Contribute to the threat intelligence capability within the Cyber Security team and the development of relevant security policies, standards and operating procedures
- Improve the cyber security posture as per the roadmap and contribute to the promotion of awareness and security culture within SEW

Manage threats and security response The role will ensure South East Water incident response plans are updated to the evolving security threats, changing technology and operational landscape. Enhancing and optimizing security tools, technologies and processes, utilizes the threat intel to improve response plans, security baselines and assist with reporting.

Maintain all security tools and technology Responsible for the currency, integrity, monitoring and appropriate alerting of security appliances and technology within South East Water.

Work with different departments in the organization to reduce risk and mitigate vulnerabilities This role will work with different technical teams across the organisation to discover, evaluate and mitigate/eliminate security vulnerabilities and weaknesses. Protects against threats and managing risks and applying controls through functional and technical assessments and evaluation.

Implement new technology and process. As South East Water continues to mature its Security Posture, and the technology landscape becomes more complex this role will be expected to advise, lead and implement as required new controls, processes, playbooks and technology to maintain and uplift the overall maturity.

Knowledge, Skills & Experience

Key skills, knowledge and experience includes:

- 10+ years of experience as a security engineer or in a related role that includes security engineering and operational functions
- Experience in managing vulnerabilities and exposures in a hybrid environment covering multi-cloud and on-prem IT and OT technologies
- Experience in uplifting and maintenance of security platforms, application control, XDR, SIEM platforms and SOC processes
- Deep understanding and practical application of cybersecurity frameworks and standards such as SOCI, ISM, NIST, ISO27001, Essential 8, Victorian Protective Data Security Standards (VPDSS), and supporting controls
- Ability to understand and disseminate industry terminology and concepts to technical and non-technical stakeholders
- Strong familiarity with Microsoft security technologies and their integration.
- Strong knowledge and ability to establish and enforce security baselines CIS and best practices
- Excellent written and verbal communication skills with a demonstrated ability to convey complex technical concepts to non-technical stakeholders.
- Prior experience in the Utilities sector and/or critical infrastructure may be beneficial but not essential

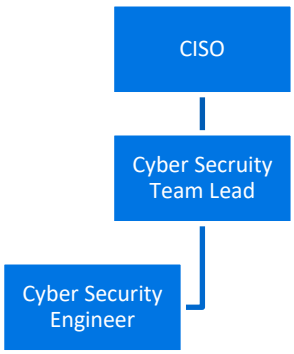
Education and Formal Certifications:

- Tertiary qualifications in an IT/Cyber Security discipline highly desired or relevant work experience

- Industry specific certification Certified Information Systems Security Professional (CISSP) or Certificate in Risk and Information Systems Control (CRISC)
- Relevant technology certifications across the security tooling (Microsoft Security, CrowdStrike, Dragos, Tenable etc.)

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