South East Water

Position description

Position title	*Cyber Security Analyst*
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 and talented Security Analyst. The role will work closely with the Cyber Security team and the wider IT and OT departments to manage alerts, threats, vulnerabilities, exposures and help uplift the posture as per the cyber roadmap.

Key Accountabilities

- Ensure effective monitoring, detection and response to security threats and incidents as per the alert/incident response procedures and playbooks
- Perform threat hunting and provide timely response to the detected alerts
- 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.
- Contribute to the threat intelligence capability within the Cyber Security team and the development of relevant security policies, standards and operating procedures. Align to Security baselines and improve them.
- Administer and maintain the tools and technologies that support the security operations, and contribute to security toolset enhancements and projects
- Conduct technical analysis and investigations to enhance, automate and optimize security operations and implementing application control mechanisms
- Manage vulnerabilities, exposures and associated risks within a Hybrid IT landscape and improve the vulnerability management practices and procedures
- Conduct risks assessments and controls evaluation where needed, and provide assurance that the SEW Information assets and data are appropriately protected
- Ensuring that the response, vulnerability management and resilience metrics are met and exceeded
- Improve the cyber security posture as per the roadmap and contribute to the promotion of awareness and security culture within SEW
- Utilize Microsoft security suite to enhance overall security posture

Security monitoring, alerts and incident management This role monitors, detects and responds to security alerts, events and incidents using various security tools and threat analysis while administering and maintaining relevant security systems, records and documentation. Contributing to the security operations, monitor violations of security policies and standards and support organisational compliance whilst providing recommendations on managing complex situations, having regard to their impact and consequences

Work with different departments in the organization to reduce risk and 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 technologies and improve process As South East Water continues to mature its Security Posture, and the technology landscape becomes more complex this role will be expected to apply and implement as required new controls, processes, playbooks and technology to maintain and uplift the overall maturity. This role is expected to work collaboratively and will challenge and improve established information security standards, processes and procedures.

Knowledge, Skills & Experience

Key skills, knowledge and experience includes:

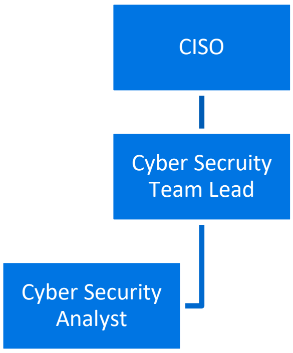
- 5+ years of experience as a security analyst or in a related role that includes cyber security operational functions and duties
- Experience in managing vulnerabilities and exposures in a hybrid environment covering multi-cloud and on-prem IT and OT technologies
- Good understanding and practical application of cybersecurity frameworks such as ISM, NIST, ISO, Essential 8 and Victorian Protective Data Security Standards (VPDSS)
- Strong familiarity with Microsoft security technologies and their integration
- Ability to understand and disseminate industry terminology and concepts to technical and non-technical stakeholders
- Working knowledge in uplift and maintenance of security technology platforms
- Strong knowledge and ability to establish and enforce security baselines 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 Certified Ethical Hacker (CEH)
- Relevant technology certifications across the security platforms and tools (Microsoft, CrowdStrike, Dragos, Tenable etc)

Dimensions

Organisational Chart



Number of people managed: 0

Size of budget managed: N/A

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