South East Water

Position description

Position title	Junior SOC Analyst
Group / Branch	Finance & Technology/Enterprise Security & Resilience
Reports to (Title)	Security Operations Manager
Competency level	Individual Contributor

Job Purpose

The **Junior SOC Analyst** will be responsible for detecting, analysing, and responding to cybersecurity incidents to protect the South East Water's assets and data. The Junior SOC Analyst will be part of the Security Operations team working closely with the Security Architecture and Engineering team and the broader technology, business stakeholders to investigate security threats, mitigate risks, and improve incident response capabilities.

Key Accountabilities

- Monitor security alerts and events from SOC, SIEM, EDR, and other security tools.
- Perform triage, analysis, and investigation of security incidents to determine scope and impact.
- Lead incident response efforts, including containment, eradication, and recovery.
- Conduct forensic analysis of compromised systems to identify root causes and attack vectors.
- Develop and refine playbooks and standard operating procedures (SOPs) for incident response.
- Collaborate with threat intelligence teams to track emerging threats and attack patterns.
- Work with Information and operational technology teams to implement security controls that reduce risk.
- Document incident findings and provide detailed reports for internal and external stakeholders.
- Assist with red teaming and tabletop exercises to improve response readiness.
- Provide recommendations for security improvements based on post-incident analysis

- Able to obtain security clearance as needed

Knowledge, Skills & Experience

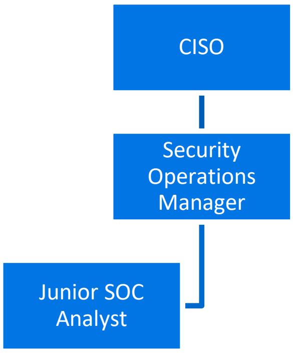
- 2+ years of experience in incident response, SOC operations, or digital forensics.
- Strong knowledge of cybersecurity threats, attack techniques (MITRE ATT&CK), and incident response methodologies.
- Experience working with security tools such as SIEM (Sentinel, Splunk, etc.), EDR (CrowdStrike, Microsoft Defender, etc.), and forensic analysis tools.
- Familiarity with network security concepts, log analysis, and malware analysis techniques.
- Ability to quickly assess security incidents and provide effective response strategies.
- Strong analytical and problem-solving skills.
- Excellent communication skills for technical and non-technical audiences.
- Hands-on experience with scripting (Python, PowerShell, Bash) for automation.
- Understanding of cloud security incident response (AWS, Azure).
- Experience with threat hunting and proactive security monitoring.

Education and Formal Certifications:

- Bachelor's degree in Cybersecurity, Computer Science, or a related field (or equivalent experience).
- Certifications such as GCIH, GCFA, CISSP, CEH, or OSCP (preferred).

Dimensions

Organisational Chart



Number of people managed: N/A

Size of budget managed: N/A

Value of Assets 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