MW ROLE MANDATE - Technical Leader

Date assessed: March 2023

Position	**Specialist Cyber Defence SIEM & Intelligence**	**Reports to**	**Senior Manager Cyber Defence**				**Group**	**3**
Division	**Corporate Services**	**Span of Control**	Direct Reports:	0	Indirect Reports:	0	**Grade**	**17**

Role Purpose

The Specialist Cyber Defence SIEM & Intelligence is accountable for ensuring Melbourne Water's enterprise platforms are being monitored effectively, actively protected against threats & vulnerabilities, and are able to respond and recover from incidents. This includes all aspects of digital technology across the business (including IT and OT) and enterprise business processes.

Measures of success

Time focus: *(see detail over page)*

5% Influencer 5% Strategist
45% Contributor 45% Driver

Key individual accountabilities

- Accountable for the performance of the operational services that enable us to successfully protect our organisation and oversee Cyber Defence services providing detect, protect, and response processes and technologies.
- Accountable and responsible for Security Information & Event Monitoring (SIEM), Threat & Vulnerability Management and Cybersecurity Incident Management & Response and outcomes (e.g. Internal Audit remediation).
- Uplifting relevant control domains maturity as measured by National Institute of Standards and Technology (NIST) cybersecurity framework for both IT and OT, the Australian Signals Directorate (ASD) Essential 8, and other frameworks as identified.
- Monitoring the external threat environment and assessing the impact of changes upon Melbourne Water and reflecting those changes in the operational security controls and incident response plans.
- Responsible for development of the detect and response components of the Cyber Security Strategy for Cyber Defence, including a 'future state' and a risk-prioritised implementation plan.
- Execute delivery of the Service Roadmap for Cyber Defence and process mapping, supported by with other teams and third parties

Qualifications & Experience

- Tertiary degree in Information Technology, Information Security or equivalent working experience is required.
- Extensive experience and expertise in Security Operations, including gathering threat intelligence, managing a Security Information and Event Management Service, Incident Management & Response, and vulnerability management
- Extensive experience and expertise in technology platform operations and management
- Extensive experience and expertise in multiple operational security platforms
- Security qualifications, accreditations and current certification in, for example, CISSP, CISM, CISA, ISO27001 LA and/or CRISC
- Demonstrated practical experience in one or more of the following: VPDSF, NIST 800-53, ISO 27001, ISO 27002, ISO 31000, and/or PCI DSS

Key shared accountabilities

- **Our People:** *Engagement Scores, NNWW, Performance Management, Resource Planning, Team Succession Planning*
- **Financial Sustainability:** *Overall MW Budget and Business plan*
- **Customer and Community:** *Divisions internal NPS score as a service; Overall MW Customer Satisfaction and Reputation Scores*
- **Safety Leadership:** *TRIFR, HPIFR, Claims costs and Safety Scores from C&E survey*
- **Vision and Purpose:** *Communicates and inspires a shared Team vision and strategic direction*
- **Risk:** *Ensures proactive oversight, governance and assessment of risk management consistent with the Risk Management framework.*

Technical capability

- Highly developed Security Operation management skills.
- Knowledge of MITRE ATTACK framework, NIST standards, and relevant legislation and regulatory authorities.

Melbourne Water

MW ROLE MANDATE - Technical Leader

Date assessed: March 2023

Decision Rights – owns	Decision Rights - influences	
• Execution of service roadmap and strategy • Regulator responses and management	• Embedding a Safety culture across the organisation	• Expertise in Security Information & Event Monitoring (SIEM) and Threat Intelligence • Expertise in enterprise vulnerability management • Expertise in incident management response and reporting

Time Focus			
Influencer	**Strategist**	**Contributor**	**Driver**
• Influence change across your teams and organisation to accelerate strategy execution, mindset change and accountability. • Build strategic relationships across business and relevant external markets (peers, partners, govt.). • Ensure Board confidence in division. Support Managing Director	• Position your business and the enterprise for the future (Future Focus), using foresight for innovation	• Leading, coaching and inspiring. Recruiting the right talent to ensure strategy execution	• Focus on efficient operation of business, ensuring risk, compliance and customer outcomes are delivered. • Driving operational effectiveness, process improvement, achieving capital spend targets, and ensure consistent audit outcomes

Melbourne Water