Position Description

Position title:	Security Operations Specialist
Reports to:	Security Operations Manager
Business unit:	IT
Employment category:	[Contract (Employment Agreement) / Enterprise Agreement and pay point]

About CitiPower and Powercor

As electricity distribution companies we provide safe, reliable and affordable power to 1.9 million Victorian customers. We use our network of poles, wires and infrastructure to bring power to homes and businesses across almost 65% of Victoria — that's more than 120,000 kilometres of wires and 850,000 poles.

But we do so much more than manage poles and wires. We're also the gateway to a clean energy future, dedicated to finding solutions and harnessing new technology to benefit our customers, communities and the environment. This includes industry leading projects in community batteries, demand management, smart charging for electric vehicles (EVs) and microgrids.

And as more customers choose solar, batteries, EVs and smart appliances — the electricity system is becoming increasingly complex, and so too is the level of innovation required to manage it.

About the IT team you'll be part of

Information Technology provide the business with technology, tools and solutions that help us achieve our strategic objectives. The team are responsible for managing and enabling our core business systems, digital transformation, IT security, IT architecture, along with overseeing all desktop and network management applications.

Our core values

Purpose of the position

This role manages the day-to-day operations within the Security Operations Centre across IT and OT, in a multi cloud environment, including vulnerability scanning and support remediation, security monitoring and incident investigation and response, network security operations and governance, and other security related functions for both IT and non-IT units.

Your key responsibilities

Vulnerability Management

- Conduct vulnerability assessments and prioritise identified risks.
- Collaborate with IT and business teams to remediate vulnerabilities
- Manage and maintain vulnerability management systems ensuring proficiency in best practices for threat and vulnerability management.

Security Monitoring and Incident Response

- Monitor security alerts, assess potential threats, and the investigation of security incidents, ensuring accurate root cause analysis.
- Ensure detailed and accurate documentation of each incident, including timelines, actions taken, and lessons learned for future improvement.
- Contribute to the development and maintenance of incident response playbooks.

Network Security

- Implementation of security administration policy and standards to ensure they are fit for purpose, current and are correctly implemented.
- Monitor the application and compliance of security administration procedures across the IT Network Security function.
- Implementation of recommendations arising from IT audits, including any defined corrective measures necessary within the IT Network Security area.

Team Player and Development

- Consistently demonstrates behaviours aligned to the organisations' values and leads others to do the same
- Empower a team culture that is focused on customer engagement, satisfaction, and continuous improvement to deliver operational excellence in management of IT infrastructure

What you'll bring to the business

Education / Qualifications:

- Tertiary qualifications in IT/Computer Science or business-related discipline preferred
- Understanding of Mitre ATT&CK, D3FEND, ATLAS, ENGAGE frameworks
- Understanding of ITIL frameworks and ITSM application advantageous

Knowledge:

- Working knowledge of IT in electricity distribution network assets
- Working knowledge of SIEM, EDR, IDS, SOAR, CASB, DLP, DFIR and Firewall tools
- Technical knowledge of OT or energy industry Cyber Security highly desirable.

Experience:

- Strong demonstrated ability to research Cyber vulnerabilities and issues, develop and present solutions, and train colleagues on how to remediate
- Experience with networks architecture, databases, TCP/IP, VLANs, Cyber vulnerability remediation, and Cyber risk analysis

The skills and competencies you'll have

'Thought' competencies

1. Cultivates innovation: Creating new and better ways for the organisation to be successful
2. Tech savvy: Anticipating and adopting innovations in business-building digital and technology solutions
3. Balances stakeholders: Anticipating and balancing the needs of multiple stakeholders

'Result' competencies

1. Ensures accountability: Holding self and others accountable to meet commitments
2. Action oriented: Taking on new opportunities and tough challenges with a sense of urgency, high energy, and enthusiasm
3. Being resilient: Rebounding from setbacks and adversity when facing difficult situations

'People' competencies

1. Collaborates: Building partnerships and working collaboratively with others to meet shared objectives
2. Manages conflict: Handling conflict situations effectively, with a minimum of noise
3. Interpersonal savvy: Relating openly and comfortably with diverse groups of people

'Self' competencies

1. Courage: Stepping up to address difficult issues, saying what needs to be said
2. Manages ambiguity: Operating effectively, even when things are not certain or the way forward is not clear
3. Situational adaptability: Adapting approach and demeanour in real time to match the shifting demands of different situations

Other relevant information

- Availability duty will be required
- Travel to other work locations / sites may be required
- Direct reports - FTE direct reports: 0 Contractor direct reports: 0
- Budget: OPEX 0, CAPEX 0