Position Description

TasNetworks | Powering a Bright Future

Senior Cyber Security Analyst

Digital | Cyber Security

Objectives	• Identify emerging cyber threats, leading complex investigations and threat hunting activities, and influencing enterprise-wide cyber risk mitigation strategies to protect critical infrastructure assets. • Provide advanced cyber security analysis, threat intelligence leadership and specialist advisory services across TasNetworks' IT and OT environments. • Contribute to the strategic uplift of TasNetworks' cyber security capability through the development of security intelligence practices, incident response preparedness, operational resilience initiatives, and alignment with regulatory and industry obligations.
Role Specific Accountabilities	• Lead the development and enhancement of enterprise threat intelligence capabilities, processes and information sources to strengthen organisational cyber resilience and threat-informed decision making. • Assess, prioritise and communicate cyber risks, vulnerabilities and threat impacts to support enterprise risk-based decision making. • Lead complex cyber threat detection, threat hunting and security analysis activities across enterprise IT and OT environments to strengthen enterprise cyber resilience. • Contribute to the ongoing development and implementation of cyber security strategy, roadmaps, standards, operational procedures, control frameworks and capability uplift initiatives aligned with organisational and operational priorities. • Provide authoritative cyber security guidance to asset and system owners regarding secure architecture, system hardening, vulnerability remediation and risk treatment strategies. • Lead cross-functional cyber investigations and coordinate technical response activities during cyber security incidents. • Collaborate with operational, engineering, technology and risk stakeholders to improve cyber resilience across enterprise and operational technology environments, and represent TasNetworks in industry cyber security forums, threat intelligence networks and critical infrastructure security collaborations. • Lead and support alignment with relevant critical infrastructure, cyber security and energy sector regulatory obligations, standards and frameworks, including AESCSF and the SOCI Act. • Any other duty or task as reasonably and lawfully directed by TasNetworks.

To be successful in this role	• A degree in a Security, Engineering or Information Technology discipline, or equivalent level of professional experience. • High level written and verbal communication skills with the ability to listen, understand, and put the stakeholder experience at the heart of service delivery • Demonstrate our core behaviours, which are central to all positions at TasNetworks. • Demonstrated specialist expertise in cyber threat intelligence, incident analysis, threat hunting or digital forensics within complex enterprise or critical infrastructure environments. • Demonstrated ability to exercise sound professional judgement and make risk-based decisions in complex and ambiguous operational environments. • Lead and support alignment with relevant critical infrastructure, cyber security and energy sector regulatory obligations, standards and frameworks, including AESCSF and the SOCI Act. • Highly self-motivated and directed in achieving proactive cyber security outcomes. • Strong organisational and time management abilities to manage multiple and competing priorities. • Strong communication and interpersonal skills. • A demonstrated ability to develop and maintain effective customer relationships and influence others to mitigate business critical cyber security risks in a timely manner. • A high level of Operational Technology Infrastructure knowledge and experience. • An understanding of leading-edge security technology solutions globally. • Have an understanding of the regulatory framework in which Australian energy utilities operate. • Ability to provide threat intelligence and data forensic advice and support to operational incident management teams. • Knowledge of the energy sector cybersecurity capability and maturity frameworks. • Demonstrated ability to innovate and identify opportunities to improve efficiencies. • Advanced analytical skills and a strong ability to adapt skills across a wide variety of systems. • High level written and verbal communication skills with the ability to listen, understand, and put the stakeholder experience at the heart of service delivery.

Compliance Requirements	• A satisfactory National Police Record check to confirm eligibility for the role
	
	• A 'critical worker' suitability assessment for the purposes of the Security of Critical Infrastructure Act 2018 (Cth) (or any successor to that Act) and the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules 2023 (Cth) (or any successor to those Rules), comprised of:
	  ○ a National Security Assessment by ASIO;
	  ○ a Criminal History Check by ACIC; and
	  ○ a Right to Work in Australia check;

Reports to:	Direct reports:	Approved:
Leader Cyber Security Analyst	0	May 2026