

Position Description

Position title:	Principal Cyber Security Engineer	**Date:**	01/10/2026
Reports to:	Cyber Defence Technical Lead	**Department:**	Digital Services
Number of reports:	Direct: Total (include indirect): 2*	**Location:**	Auckland
Delegated financial authority:	Yes	**Budget ownership:**	No
Level of influence:	**Leading self** Leading others		

Our Organisation

At Southern Cross Healthcare, our vision is to help people live their best lives by reimagining healthcare.

Across our nationwide network, we combine the skills of more than 4,000 people including nurses and anaesthetic technicians, working with specialists, surgeons, anaesthetists, and allied health practitioners.

As New Zealand's largest private provider of healthcare, our strong "for purpose ethos" and through being recognised as one of New Zealand's leading and most trusted brands, we are poised to amplify the delivery of healthcare services like no other.

Vision	Purpose
Our vision is for what we aspire. **To help people live their best lives by reimagining healthcare.**	Our purpose is why we exist. **To advance the provision of quality healthcare in Aotearoa New Zealand.**

Our Values

Care First: Care is at our heart. It's the foundation of who we are and how we approach our mahi. Through genuine manaakitanga, we deliver a quality of care that makes healthcare more human.

Better Together: Our strength comes from connection and collaboration – we bring together our diverse skills, perspectives, and experiences in the spirit of partnership and kotahitanga. We all play our part creating better outcomes for everyone.

Pursue Excellence: Every day brings a new opportunity to improve, innovate, and excel. We don't settle for 'good enough'. We're here to do our best work, delivering our best care for the people and communities we serve.

Role Purpose

The Principal Cyber Security Engineer is the senior technical specialist responsible for the engineering, technical effectiveness and continual improvement of Southern Cross Healthcare's cyber defence capabilities. Reporting to the Cyber Defence Technical Lead, the role provides deep technical expertise across detection engineering, security tooling, threat hunting, vulnerability management, incident response, cyber resilience and security automation.

The role acts as the delegated technical authority for cyber defence platforms, detection capabilities and associated technical standards. It leads complex engineering activities and serves as the senior technical escalation point during significant cyber security incidents, working under the direction of the designated incident manager.

Drawing on extensive cyber security engineering experience, the role will develop and improve cyber defence capabilities across technology, processes and technical practices. It will work closely with Digital Services teams, business stakeholders and security partners to embed security requirements into technology initiatives, improve visibility and response capabilities, and strengthen the resilience of critical healthcare services.

The role will support the evolution of Southern Cross Healthcare's cyber defence capabilities towards cloud-native security engineering, DevSecOps, Infrastructure as Code, security automation and the secure adoption of AI-driven technologies and autonomous agents, ensuring that security is embedded throughout the technology delivery lifecycle.

The role provides technical guidance, mentoring and task leadership to Security Operations Engineers and Analysts. Formal people leadership, performance management, service management, vendor management and employment responsibilities remain with the Cyber Defence Technical Lead.

This role provides an opportunity to influence and modernise cyber defence capabilities within one of New Zealand's largest healthcare organisations through automation, engineering excellence and modern cyber-defence practices.

Key Relationships

Internal	External

• Digital Services Teams	• Cyber Security Partners • Digital Services support partners and suppliers • 3rd Party Vendors and Supplier technical teams Industry Sharing and Threat Intelligence Groups

Key Accountabilities

Security Operations Leadership

- Provide senior technical leadership across cyber defence engineering and act as an escalation point for complex security incidents and technical issues.
- Lead defined technical workstreams and engineering activities within the priorities and service plans established by the Cyber Defence Technical Lead.
- Provide technical guidance and mentoring to Security Operations Engineers and Analysts, supporting knowledge sharing, capability development and engineering excellence.
- Support reporting on security control coverage, effectiveness, detection performance and cyber defence capability maturity.
- Provide technical evaluation and assurance of MSSP, MDR and security technology partner capabilities and solutions, without responsibility for operational or commercial vendor management.
- Provide technical recommendations to inform the Security Operations roadmap, priorities and investment decisions.
- Provide technical input into technology programmes and operational initiatives so that cyber defence, monitoring and incident-response requirements are addressed early.
- Translate cyber security objectives into proposed engineering activities and measurable technical outcomes for agreement with the Cyber Defence Technical Lead.
- Apply risk-based judgement when balancing security requirements with the safety, availability and continuity of healthcare services.

Security Capability, Engineering and Automation

- Lead the technical development and continual improvement of detection engineering, threat hunting, security automation and cyber defence capabilities.
- Champion automation to improve consistency, operational efficiency, response times and security outcomes.
- Assist with the design, implementation, integration and optimisation of security platforms, including SIEM, XDR/EDR, SOAR, vulnerability management, identity security, email security and threat intelligence technologies.
- Maintain technical ownership of cyber defence platform configurations, integrations, engineering patterns and lifecycle requirements, subject to applicable architecture, change and commercial governance.
- Identify and implement opportunities to automate manual security processes using orchestration, workflow automation and appropriately governed AI assisted capabilities.
- Evaluate emerging threats, attack techniques and technologies, and recommend proportionate improvements to security controls and operational capabilities.
- Improve the scalability, resilience, interoperability, standardisation and rationalisation of the security technology stack.
- Develop and maintain technical standards, patterns and engineering documentation for cyber-defence technologies.
- Support the technical development of security-as-code and policy-as-code capabilities to automate security governance, compliance validation and control enforcement across cloud, infrastructure and application environments.

Security Monitoring, Detection and Incident Response

- Lead the technical design and improvement of monitoring, detection engineering, threat hunting and threat intelligence capabilities across cloud, on-premises, SaaS, endpoint, identity and operational technology environments.
- Act as the technical response lead during significant cyber security incidents, working under the authority of the designated incident manager.
- Coordinate technical investigation, containment, eradication and recovery activities, including the contribution of internal specialists and external response providers.

- Recommend or coordinate the activation of digital forensics and incident response partners in accordance with approved incident response plans and delegated authority.
- Provide clear technical advice to Digital Services and cyber security leadership during incidents, including impact, containment options, operational risks and recommended actions.
- Develop and maintain detection use cases, monitoring requirements, response playbooks and technical procedures.
- Conduct threat informed testing, purple team exercises and adversary simulations to validate detection and response effectiveness.
- Identify detection and visibility gaps and recommend remediation priorities to the Cyber Defence Technical Lead and relevant technology owners.
- Lead post incident technical analysis and ensure lessons are translated into improvements to controls, detections, tooling and playbooks.
- Participate in an agreed on-call or after-hours incident response arrangement where required.

AI & Agent Security

- Support the assessment of AI solutions for security, privacy, model integrity, data protection and regulatory risks.
- Assist with the definition of security guardrails for AI-assisted development, code generation and operational automation capabilities.
- Develop detection, monitoring and response capabilities for AI-related threats, misuse, prompt injection attacks, excessive privilege use and unauthorised data disclosure.
- Collaborate with architecture and technology teams to establish secure patterns for AI integration with enterprise applications, identities and data platforms.

Vulnerability and Exposure Management

- Lead the technical execution of vulnerability and exposure identification, assessment, risk-based prioritisation and remediation validation activities.
- Partner with application, cloud and platform engineering teams to embed vulnerability management, code scanning, secrets management and continuous security assurance across the software development lifecycle.
- Develop risk based prioritisation methods that consider exploitability, threat intelligence, asset criticality, clinical impact and healthcare-service availability.
- Provide actionable remediation advice to infrastructure, cloud, application, operational technology and service owning teams.
- Coordinate with technology owners to track risk treatment while ensuring responsibility for implementing remediation remains with the relevant asset or service owner.
- Analyse and report on vulnerability trends, material exposures, remediation performance and control effectiveness.
- Validate whether remediation or compensating controls have appropriately reduced exposure.
- Support attack surface reduction and cyber resilience initiatives through continuous technical assessment and improvement.

Note: These duties may change from time to time to meet operational or other requirements.

Health, Safety and Wellbeing

- All employees are responsible for complying with health and safety policies and procedures.
- You are responsible for your own health and safety while at work and ensuring that your actions or inactions do not put others at risk.
- Identify, report and self-manage hazards where appropriate.
- Ensure that you complete early and accurate reporting of incidents at work.
- Participate and co-operate for shared health and safety responsibilities
- Actively participate where improvements to health and safety at SCHL can be made

Commitment to the principles of Te Tiriti o Waitangi

- Demonstrate awareness and understanding of Te Tiriti o Waitangi obligations through manaakitanga (respect) and kawa whakaruruhau (cultural safety) as evidenced in interpersonal relationships.

Commitment to Diversity, Equity and Inclusion (DEI)

- Honour diversity by acknowledging and respecting others' spiritual beliefs, cultural practices and lifestyle choices as evidenced in interpersonal relationships.
- Seek opportunities to include diversity, equity and inclusion practices in everyday work.

Commitment to Environment, Social and Governance (ESG)

- Engage in sustainable practices whenever possible. Try to reduce the environmental impact of your work and take an active role to initiate change to meet Southern Cross' ESG (Environmental, Social and Governance) commitments.
- Actively engage to improve your knowledge regarding sustainable practices whenever possible.

Role Requirements

Experience and skills required:

- 10+ years' experience in cyber security, including extensive experience in Security Operations, incident response, detection engineering and security engineering roles.
- Demonstrated experience acting as a senior technical authority, principal engineer, lead engineer or equivalent role within a complex enterprise environment.
- Experience operating within critical infrastructure, healthcare, government, financial services or other highly regulated environments.
- Proven ability to influence outcomes across teams and stakeholders without direct line-management authority.
- Experience in building cyber security operations capabilities.
- Hands-on experience with security operations technologies, including SIEM, XDR/EDR, SOAR, identity security, endpoint security, and network security controls.

Education and qualifications required:

- Relevant tertiary qualifications in cyber security, information technology, engineering, or computer science or equivalent industry experience.
- Demonstrated expertise in Security Operations, Incident Response, Detection Engineering, and Cloud Security Engineering.

Education and qualifications desirable:

- Industry-recognised certifications such as CISSP, CISM, GCIH, GCIA, GCFA, OSCP, CDP, Microsoft Security, Palo Alto Networks, or equivalent.

- Strong understanding of cloud, network, infrastructure, identity, and application security concepts
- Hands-on experience securing cloud-native application delivery pipelines and Infrastructure as Code environments.
- Expertise in cyber security incident response, threat hunting, and detection engineering.
- Experience developing and implementing security automation and orchestration solutions using scripting and automation technologies such as PowerShell, Python, KQL, or similar.
- Working knowledge of MITRE ATT&CK frameworks, threat intelligence, and modern cyber defence practices.
- Strong analytical, communication, and decision-making skills, including the ability to lead during cyber security incidents.

Experience and skills desirable:

- Good understanding of cyber security architecture principles, models, and best practices.
- Experience with Microsoft and/or Palo Alto Networks security platforms including Next-Generation Firewalls
- Practical understanding of AI security risks, AI governance frameworks and secure deployment of generative AI solutions.
- Experience managing or overseeing MSSP, MDR, or other third-party security service providers.
- Experience in reporting on security operations metrics, KPIs, and capability maturity.
- Experience leading cyber resilience exercises, incident simulations, or digital forensics investigations.

Leadership Attributes

Human Centred Leadership • Empathy • Adaptability • Connection **Performance Coach** • Accountability • Engagement • Collaboration	**Change Enabler** • Execution • Energy • Contribution