Position Description

General Information:	
Position Title:	Cyber Security Analyst
Incumbent:	
Function & Team/Program:	Cyber Security - Digital & Transformation
Location(s):	Sydney National Office NSW
Manager's Position Title:	Cyber Security Analyst
Manager's Name:	Nikita Dodemont
Date Prepared:	5 December 2025
Prepared By:	Nikita Dodemont
Approved By:	Prashant Pandey

Primary Purpose of this Position *(In one sentence - why does the role exist?)*

This position is responsible for detecting, analysing, and responding to cyber security threats, while implementing continuous improvements to security tools and processes, to safeguard the organisation's Information and Communications Technology (ICT) environment and uphold compliance standards.

In addition, the role plays a key part in strengthening the organisation's overall cyber maturity by supporting the development of secure practices, contributing to uplift initiatives, and ensuring that cyber security controls remain effective, contemporary, and aligned with emerging risks.

The position provides practical technical support across the organisation, helping staff understand and adopt secure behaviours while working within established governance frameworks.

Scope:

Direct Reports to this Position	Indirect Reports
By Position Title	Total Number
• Nil	• Nil

Financial Dimensions controlled by this Position *(Include key financial metrics such as revenue growth, income & expense budget, etc)*

Direct control	Indirect control
• Nil	• Nil

Other Dimensions of this Position

- *Geographic Scope and Team Collaboration:* Based in the Sydney National Office, this role is a key member of the SmithShield Program, operating within a hybrid/flexible working model. At times on-site work is essential for close team collaboration, strategic planning, and immediate response capabilities.
- *Incident Response and Operational Resilience:* Committing to essential occasional scheduled after-hours work, the analyst must be prepared to travel to the National Office to support and manage critical security incidents, ensuring the non-profit's operational resilience and continuity of service delivery.

- *Stakeholder Engagement:* Collaborating regularly with the broader Digital and Transformation Function (including Information and Communications Technology (ICT) colleagues) and with end-users across the organisation's national footprint.
- Reporting Line Flexibility: While the incumbent may initially report to a designated line manager, the reporting line may change over time to best support organisational priorities, particularly in response to evolving Digital & Transformation requirements.
- Cross-Functional Coordination: The role may work with multiple teams to coordinate incident response, uplift activities, and operational improvements across the organisation.
- The position requires ongoing engagement with emerging cyber threats, tools, and industry practices to ensure the organisation remains protected and informed.

Setting Priorities *(how is work prioritised)*	
How often does employee prioritise their own work? Eg. Daily, weekly, monthly, annually, other	Daily, Weekly, Monthly, Quarterly and Yearly
How often does employee determine the priorities of others? Eg. Daily, weekly, monthly, annually, other	Not Applicable

Key Relationships *(Who does the role interact with? List the titles of individuals, departments and organisations frequently interacts with)*	
Internal	• Cyber Security team • Digital & Transformation colleagues (The Smith Family's ICT department) • End users, this includes all employees and volunteers engaged by The Smith Family • Senior Leadership Team • People Managers across the organisation • Team members across the organisation
External	• External Security Operations Centre • External suppliers of cyber security tools and services • Cyber Security Network

Key Decision Making in this Role: *(What are the key decisions and recommendations made in this role?)*

Decisions Expected

- Determine the urgency and severity of security alerts sourced from the Security Information and Event Management (SIEM) platform and the Security Operations Centre (SOC), Making the decision of which security alert to priorities from SIEM and SOC
- Establish priorities for daily operational tasks and incident remediation efforts.
- Determine the sequence of security uplift and continuous improvement projects based on risk impact and strategic benefit.
- Determine the most appropriate remediation steps for low-risk or routine security issues.
- Evaluate when configuration changes or temporary controls are required to mitigate immediate risks.

Recommendations Expected

- Propose evidence-based enhancements for cyber security tools, services, and associated vendor contracts.
- Advise on improvements and updates to cyber security operations policies, procedures, and response playbooks to maintain best practice compliance.
- Recommend strategic risk mitigation strategies to the broader Information and Communications Technology (ICT) leadership team.
- Recommend configuration changes to reduce recurring alerts or improve system resilience.

- Suggest opportunities to streamline security processes to improve efficiency and reduce operational overhead.

Every Team Member at The Smith Family:

- Is expected to uphold The Smith Family Values and Culture.
- Understands and complies with the Child Protection Framework.
- Takes reasonable care for the health and safety of themselves and others.
- Understands and comply with the Workplace, Health and Safety Systems.
- Reports hazards and incidents and participates in risk management as required.

Key Responsibilities / Accountabilities:		
Major Area:	***Cyber Operations***	***% of Job Total: 50%***
Investigate and triage alerts escalated by the Security Operations Centre (SOC) and the Security Information and Event Management (SIEM) system. Investigate alerts raised by SOC and SIEM		
Coordinate and drive the resolution of security alerts by liaising with internal Stake holders, Digital and Transformation teams and external partners.		
Deliver technical support and guidance to end-users for cyber security tools and services.		
Maintain vigilance by monitoring the organisation's systems to identify, assess, and report on potential vulnerabilities.		
Contribute to and support recurring cyber assurance activities, including penetration testing coordination and security policy reviews.		
Engage proactively with both internal and external teams to manage security alerts and tickets through to complete resolution.		
Perform in-depth root cause analysis (RCA) on security incidents to prevent recurrence.		
Respond and support during critical security incidents, adhering to established incident response procedures.		
Major Area:	***Continuous Improvements***	***% of Job Total: 50%***
Research, evaluate, and test emerging cyber security tools and services to enhance protection capabilities.		
Drive and implement activities within the broader cyber security uplift program.		
Refine and streamline existing security processes to maximise efficiency and effectiveness.		
Audit current security configurations, propose configuration enhancements, and implement approved changes		

Key Challenges in Achieving Goal(s): *(What are the key challenges faced by this role in meeting goals/objectives)*

- *Balancing Risk and Velocity*: Effectively managing the pressure of competing operational (Business As Usual) and strategic (Continuous Improvement) priorities while maintaining a consistent focus on high-priority security threats.
- *Enabling vs. Restricting:* Maintaining a customer-centric approach that supports The Smith Family's mission and user workflows, while upholding rigorous security policies, procedures, and Essential Eight or NIST-aligned best practices without compromise.
- *Resource Constraints*: Navigating the typical resource and budget constraints of a non-profit environment to deliver high-impact security outcomes and justify investment in essential security uplift programs.

Qualifications, Experience and Competencies: *(What background, knowledge, experience or competencies are required to perform the role at the expected level?)*

	Essential	**Desirable**
Education / Qualifications / Memberships:		• Tertiary qualification in Cyber Security, Information Technology, Computer Science, or a related

		discipline; or equivalent relevant experience. • Industry-recognised professional cyber security certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or certifications from Global Information Assurance Certification (GIAC). • Vendor certification e.g. M365 Certified Endpoint Administrator Associate, M365 Certified Security, Compliance and Identity Fundamentals
Experience:	**Essential**	**Desirable**
	• 1+ years of experience in a security focussed role • Experience implementing and/or maintaining security best practises such as the Essential 8 or NIST cyber security frameworks • Experience with SIEM, vulnerability management, EDR and related technologies • Managing support tickets through to resolution	• Experience with application control tools • Experience with M365 and MS security tooling • Experience with Entra ID • Experience with Azure
Competencies:	**Essential**	**Desirable**
	• Effective communication skills, both written and verbal, with the ability to explain technical concepts to non-technical users • Strong organisational and time-management skills, with the ability to manage competing priorities. • Good problem solving and troubleshooting skills • Commitment to knowledge sharing • Good interpersonal skills • Self-directed and able to manage concurrent and competing priorities and challenges • Strong understanding of security concepts • Ability to interpret detailed requirements Strong analytical and problem-solving skills with the ability to interpret technical information.	• Proven track record of documentation and knowledgebase creation • Ability to understand big picture concepts