Role Name: Senior Security Operations and Platform Specialist

Role data

Position no.	E12331	**Work Area Profile**	IT Management
Work Level Classification	Level 8	**Directorate/Business Unit**	IT Directorate
Reports to (role)	Manager – Information Security	**Location**	Melbourne
No. direct reports	Nil	**No. of indirect reports**	Nil
Version date	February 2022	**Tenure**	Agency Worker 12 Months

Work area profile

Ahpra's overall mission is to protect the public by regulating health practitioners efficiently and effectively in the public interest to facilitate access to safer healthcare for all the community. Website: www.ahpra.gov.au

The IT Directorate provides technology services and solutions that advance the Ahpra vision, mission and strategic goals. The Directorate supports Ahpra's users, leadership, external stakeholders and practitioners with customer-oriented service and a robust and reliable technology environment that encourages effective and innovative ways of using technology in all facets of Ahpra's operations.

IT Management shapes IT policy and drives IT performance for cost effectiveness and seamless working with stakeholders.

Role purpose

The Senior Security Operations and Platform Specialist provides specialist expertise and advice to support the Manager, Information Security in day to day operations of the 'Security Operations and Platform' Function within the Security Team, by minimizing security risks in both the daily BAU operations as well as the development process. This is achieved by predicting, monitoring and addressing possible risks and vulnerabilities through automation, and resolving issues as they are identified.

Key accountabilities

- As a senior SME practitioner, you will support and advise the Manager, Information Security in relation to business priorities for security operations, planning and capability improvements across the business.
- Lead the Security Operations and Platform function.
- Investigate current processes, workflow and procedures for cybersecurity best practice and implement a streamlined and automated approach to identify and protect against risk.
- Investigate vulnerability alert and management processes and implement a streamlined and automated approach, integrated into the organisations service desk system.
- Lead subject matter expert (SME), advise, support and integrate Cyber Security Program deliverables to ensure a smooth transition and implementation to BAU security operations.

- Lead and deliver security audits and risk assessments, including the development of mitigation strategies, advice and recommendations to management and staff in relation to security risks across the organisation.
- Lead the response and investigation into incidents, including co-ordinating internal Ahpra teams, managed service providers and third-party vendors as required to triage security and cybersecurity risk mitigation and resolution, recommending and implementing solutions expediently to protect Aphra's posture.
- Monitor and appraise the ever changing cybersecurity landscape for developing / actual cybersecurity threats to Ahpra and manage the appropriate risk mitigation and defence.
- Deliver outcomes from the security risk register to guide effective business decision making and the implementation of adequate security risk controls. Monitor the performance of security risks controls and address issues with the effectiveness of those controls.
- Support the development and delivery of standards, procedures, plans and related guidelines that underpin and operationalise the organisations information security framework, ensuring compliance with external requirements.
- Provide guidance, direction and mentoring to security staff.
- Foster a culture of continuous improvement by seeking opportunities to review and improve processes across the role scope and system/services.
- Proactively develop, maintain and effectively manage constructive working relationships with internal teams, delivery partners and key external agencies.
- Health Safety and Wellbeing: Ensuring the workplace provides a safe working environment with the required level of care and respect for its participants meaning to:
    - Take reasonable care for own and others' health, safety and wellbeing.
    - Adhere to Ahpra's workplace health, safety and wellbeing policies and procedures.

Capabilities for the role

The Ahpra Capability Framework applies to all Ahpra employees. Below is the complete list of capabilities and proficiency level required for this position.

Capabilities	Proficiency level
Commits to customer service	Advanced
Displays leadership	Advanced
Generates and delivers the strategic vision	Advanced
Demonstrates an awareness of the National Registration and Accreditation Scheme (the National Scheme) and the National Law	Foundation
Builds constructive working relationships	Highly Advanced
Communicates effectively	Highly Advanced

Demonstrates accountability in delivering results	Highly Advanced
Uses information and technology systems	Highly Advanced
Displays personal drive and integrity	Advanced

Qualifications/Experience	Required
Qualifications	Relevant tertiary qualification and/or equivalent level of experience across required areas of expertise. Formal qualifications or relevant experience in Security Operations, Security Project Management or other related Security fields.
Experience	Advanced technical skills and capabilities in the development and management of operational security programs. Advanced experience within planning, identifying, monitoring, analysing and prioritising business security related risks (threats and opportunities), creating response plans and managing the risk if it occurs. Advanced practitioner level using Microsoft M365 (E5) and Azure, ManagedEngine, Qualys, CrowdStrike, Darktrace, Mimecast, Secureworks and Algosec. Expertise in embedding security practises into an organisation to ensure the protection of its people, assets and information. Very strong interpersonal skills: able to build and sustain effective working relationships at all levels, but particularly with senior business and IT stakeholders. Strong consulting skills and an ability to discuss IT requirements with the business in non-technical terms when required. Able to exercise influence over decision-making, without reliance on formal authority. Experience and understanding of ITIL Incident, Change and Problem Management practices.

Key relationships

Internal relationships	External relationships
CIO & IT National Directors	Technology vendors
IT Security peers	Service providers
IT Service Management & Operations peers	
IT Service Delivery peers	
IT directorate teams	
Cross directorate stakeholders	