Make it matter.

POSITION DESCRIPTION

Senior Specialist - Security Infrastructure Operations

Position Level	
Faculty/Division	Operations
Position Number	*ADMIN ONLY*
Original document creation	February 2022

Position Summary

The role of Senior Specialist - Security Infrastructure Operations is responsible for the management of our catalogue of cyber security services. This includes the implementation, configuration, and support of cyber security services deployed across multiple environments including on-premises, public, and hybrid cloud in close collaboration with our vendors and suppliers.

The Senior Specialist, Security Infrastructure Operations will have thorough knowledge and experience with cloud native security services in AWS, Azure, and Microsoft 365, as well as security controls deployed in on-premises environments such as network security, endpoint security, application security, etc.

The role reports directly to the Manager, Security Infrastructure Operations.

Accountabilities

Specific accountabilities for this role include:

- Implement, configure, update, and optimise security services and technologies hosted on-premises and in public cloud environments ensuring they are configured and updated in accordance with our design and standards.
- Monitor and respond to requests, operational alerts, and incidents working together with UNSW IT, faculties, divisions, external partners, and other stakeholders as required.
- Document and review operating procedures, technical standards, service management plans, processes, designs, and other documentation.
- Report on the effectiveness of security services and provide recommendations following a continuous improvement model.

- Review and update the CI/CD pipeline to automate both security testing and management of security services.
- Lead response activities for incidents working together with our partners and vendors.
- Adhere to IT Service Management practices across UNSW IT, Faculties, Divisions, and Affiliates.
- Oversee and finalise effective communications with key stakeholders, both internal and external and provide influential input with stakeholders to achieve business outcomes.
- Align with and actively demonstrate the UNSW Values in Action: Our Behaviours and the UNSW Code of Conduct.
- Cooperate with all health and safety policies and procedures of the university and take all reasonable care to ensure that your actions or omissions do not impact on the health & safety of yourself or others.
- You will be required to participate in a rotating on-call roster.

Skills and Experience

- A relevant tertiary qualification with subsequent relevant experience or equivalent competence gained through any combination of education, training, and experience.
- Minimum five years of industry experience in any of the following areas: security operations, incident response, or security consulting.
- Strong technical skills and experience in the management, configuration, and support of security controls including network security, endpoint security, application security, data protection, and/or identity and access management across different environments including on-premises, public, and/or hybrid cloud.
- Knowledge and experience in:
    - Security services and technologies such as SIEM, EDR, EPP, SEG, NGFW, IAM
    - Cloud native AWS security services such as WAF, GuardDuty, Inspector
    - Microsoft 365 Defender services
- Experience in CI/CD pipelines and infrastructure-as-code.
- Sound understanding of DevSecOps delivery models and practices.
- Comprehensive analytical and problem-solving skills and proven capacity to exercise initiative, flexibility and to be proactive in development of robust solutions to problems.
- Strong written and verbal communication skills, with a high level of attention to detail for deliverables produced.
- An understanding of and commitment to UNSW's aims, objectives and values in action, together with relevant policies and guidelines.
- Knowledge of health and safety responsibilities and commitment to attending relevant health and safety training.
- Relevant industry certifications such as CISSP, CISM, SANS GIAC GCIH/GCFA are highly desirable but not required.

About this document

This Position Description outlines the objectives, desired outcomes, key responsibilities, accountabilities, required skills, experience and desired behaviours required to successfully perform the role.

This template is not intended to limit the scope or accountabilities of the position. Characteristics of the position may be altered in accordance with the changing requirements of the role