Make it matter.

POSITION DESCRIPTION

Specialist – Cyber Security Operations

Position Level	7
Faculty/Division	Operations
Position Number	ADMIN ONLY
Original document creation	March 2019

Position Summary

The Specialist – Cyber Security Operations is a key position in the Security Infrastructure Operations team responsible for the implementation, configuration, and support of cyber security services across multiple environments including on-premises, public, and hybrid cloud.

The Specialist will have knowledge and experience with cloud native security services in AWS, Microsoft Azure, and Microsoft 365, and traditional security controls such as firewalls, endpoint security, secure email gateways, and data loss prevention. The role will be responsible for incident response including monitoring, analysis, and remediation of cyber threats working closely with our MSSP providers, security vendors, and the CSIRT team.

The role reports to the Manager, Security Infrastructure Operations and has no direct reports.

Accountabilities

Specific accountabilities for this role include:

- Implement, configure, upgrade, and optimise security services and technologies hosted on-premises and in public cloud (IaaS, PaaS, SaaS).
- Monitor and respond to operational alerts and incidents impacting security services in partnership with UNSW IT, faculties, divisions, external partners, and other stakeholders as required.
- Document and review operating procedures, technical standards, service management plans, processes, designs, knowledge base articles and other documentation as required.

- Support the CI/CD pipeline following an Infrastructure-as-Code approach to automate security testing and manage security services.
- Regular review and assessment of security controls ensuring they are operating as designed
- Detect and respond to reported security incidents and requests ensuring they are appropriately triaged, prioritised, and remediated.
- 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 and 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 three years of combined industry experience in any of the following areas: security operations, incident response, penetration testing, governance, or consulting.
- Demonstrated experience in managing and configuring security controls such as SIEM, firewalls, endpoint security, and secure email gateways
- Demonstrated experience in managing and configuring cloud native security services across cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and Microsoft 365 to secure cloud infrastructure and hosted enterprise applications.
- Excellent written and verbal communication skills, with a high level of attention to detail for deliverables produced.
- Strong analytical and problem-solving skills and proven capacity to exercise initiative, flexibility and to be proactive in development of robust solutions to problems.
- Demonstrated success working effectively and collaboratively on initiatives with a range of people at different levels within an organisation.
- Knowledge of health and safety responsibilities and commitment to attending relevant health and safety training.
- CISSP, CISM, SANS GIAC GCIH/GCFA, OSCP certifications are highly desirable but not required.