Position Description

Specialist – Cyber Security Operations

Position Summary

The Specialist – Cyber Security Operations is a key position in the Cyber Security Operations team responsible for the identification, response, and remediation of security incidents across the University. The Specialist will be involved with configuring and maintaining security controls such as firewalls, endpoint protection, data loss prevention, and identity and access management. The role will be responsible for incident response, performing tasks such as log monitoring, analysis, and remediation of threats working closely together with business units, incident managers, technical leads, customers, and other stakeholders as required.

The role reports to the Head of Cyber Security Operations and has no direct reports.

Accountabilities

Specific accountabilities for this role include:

- Support investigation activities and manage actions in partnership with UNSW IT, business units, legal, HR, external partners, and other stakeholders as required.
- Monitor and analyse security logs across various security controls including firewall, endpoint, application, system, etc. to identify alerts, incidents, trends, and potential threats to the organisation.
- Detect and respond to reported security incidents and requests ensuring they are appropriately triaged, prioritised, and remediated.
- Configure, maintain, and support a broad range of security controls.
- Regular review and assessment of security controls ensuring they are operating as designed.
- Document and update security processes, procedures, playbooks, technical standards, and policies.
• Actively perform threat hunting to identify malicious actors and anomalous activity.
• Gather, analyse, and report on actionable threat intelligence.
• 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 may 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 cyber security operations, incident response, penetration test, or consulting.
• Proven technical skills and operational 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.
• Experience 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.
• Outstanding analytical and problem-solving skills and proven capacity to exercise initiative, flexibility and to be proactive in development of robust solutions to problems.
• Excellent written and verbal communication skills, with a high level of attention to detail for deliverables produced.
• Demonstrated success working effectively and collaboratively on initiatives with a range of people at different levels within an organisation.
• Strong time management skills, with a demonstrated ability to respond to changing priorities, manage multiple tasks and meet competing deadlines by using judgement and initiative.
• 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.

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.