UNSW
SYDNEY

Make
it matter.

POSITION DESCRIPTION

Specialist – Cyber Security

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

Position Summary

The Specialist – Cyber Security is responsible for supporting the Security Operations team in the delivery of our portfolio of security services. This includes the configuration and optimisation of security services and technologies hosted on-premises and in public cloud, and supporting incident investigation and response activities. Additionally, the role will work closely with our Managed Security Service Providers (MSSPs) and technology partners to ensure that they continue to meet the needs and expectations of UNSW.

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

Accountabilities

Specific accountabilities for this role include:

- Monitor the SIEM and cyber security queue for events, incidents, and requests to ensure they are appropriately triaged, prioritised, and assigned.
- Support the design, build, implementation, and operation of security services and technologies across multiple environments.
- Support incident investigation in partnership with UNSW IT, MSSPs, business units, legal, HR, external partners, and other stakeholders as required to contain and remediate threats.
- Conduct vulnerability assessments and scans to identify security weaknesses
- Co-ordinate and communicate incidents with internal stakeholders or external partners, as required, ensuring they are informed of the status, actions, recovery, and other information as necessary in a timely and clear manner.
- Review and update operating procedures, technical standards, service management plans, processes, designs, and knowledge base articles.

- Document and present security reports on a regular basis identifying trends, patterns, insights, and providing recommendations. This includes vulnerability reports, incident reports, and threat intelligence reports.
- Actively engage with internal and external stakeholders to build and maintain collaborative working relationships with them and understand relevant business drivers.
- Adhere to IT Service Management practices across UNSW IT, Faculties, Divisions, and Affiliates.
- 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.

Skills and Experience

- A relevant tertiary qualification with subsequent relevant experience or equivalent competence gained through any combination of education, training, and experience.
- Minimum two years of industry experience in any of the following areas: Security Operations, Incident Response, or Governance Risk and Compliance.
- Strong written and verbal communication skills, with a high level of attention to detail for deliverables produced.
- Knowledge of cyber security services such as identity and access management, detection and response, network security, application security, and data security.
- 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.

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