POSITION DESCRIPTION

Specialist – Cyber Operations

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

Position Summary

The Cyber Security Analyst is a key position in the UNSW Cyber Security Operations team responsible for the identification, response, and remediation of security incidents across the University.

The experienced Analyst has strong technical skills managing and supporting security controls including next-generation firewalls, endpoint security, data loss prevention, key management, and encryption for both on-premise and public cloud environments. The role includes monitoring, analysing, and responding to cyber threats ensuring timely resolution of incidents working closely together with incident managers, technical leads, and directly with customers and stakeholders.

The Cyber Security Analyst contributes to the IT security operational management and change implementation requirements of UNSW IT, Faculties, Divisions, Affiliate and stakeholders. This role is required to engage, collaborate, and negotiate effectively and to adjust personal style and approach to optimise outcomes.

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

Specific accountabilities for this role include:

- Configuration, implementation, and maintenance of technical security controls
- Regular review and assessment of security controls ensuring services are effective and operating as designed
- Managing service requests and ensuring adherence to service level agreements
- Analysing security events and logs for threats including operating system logs, application logs, network traffic (pcaps), access logs, binaries, and source code
- Engaging with partners, vendors, and other service provider groups to resolve complex issues and incidents
- Updating security documentation including processes, operating procedures, and playbooks
- Gather, review, and act on structured and unstructured threat intelligence from multiple sources
- Generating security reports on a regular basis identifying trends and patterns
- Comply 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

- Minimum five years of experience in a SOC or similar environment with a focus on security infrastructure operations and incident response, or an equivalent level of knowledge gained through a combination of education, training and/or experience.
- Experience managing and maintaining security controls and policies across enterprise-scale Office 365, AWS, and Azure environments
- Demonstrated strong technical skills and operational experience across at least four of the below areas (on-premises or public cloud):
  - Next-Generation Firewalls
  - Web Application Firewalls
  - Vulnerability Management
  - Data Loss Prevention (DLP)
  - Secure Email Gateways
  - Security Information and Event Management (SIEM)
  - Endpoint Security (EPP and EDR)
  - Encryption and Key Management
- Knowledge and practical experience in incident response and incident handling as well as understanding of adversary tactics and techniques.
- Understanding of ITIL processes.
- CISSP, CISA, SANS GIAC GCIH/GCFA, OSCP certifications are highly desirable
- 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.