Job Description

Job title: Cyber Security Analyst

Grade: 6

Reports to: Senior or Lead Cyber Security Analyst

Office: Information Security and Identity and Access Management, IT Services

Date: October 2023

Overall purpose of the job

Based within the Security Operations team, the Cyber Security Analyst plays a critical role in the first line (Tier 1) efforts to keep the University's systems and networks secure. The Security Operations Team is responsible for monitoring of all network and computer systems to prevent, detect, investigate and respond to security incidents. Working in collaboration with colleagues within the Information Security and Identity and Access Management Division, the team will install and manage firewalls, SIEM platforms, Vulnerability Detection and Management systems and other tooling and processes to protect data sources. The team members will also be responsible for performing internal and coordinating external penetration testing to ensure the integrity and security of the University's networks.

Security Operations has four key areas of focus: incident response; network monitoring and intrusion detection; security testing and vulnerability management. The Cyber Security Analyst is expected to have a basic knowledge across all security functions but will primarily be responsible for security monitoring and incident detection, investigation and response.

Key responsibilities, accountabilities and duties

Security operations

- Monitors the application and compliance of security administration procedures, and reviews information systems for actual or potential breaches in security.

- Identifies and investigates breaches in security promptly and implements any system changes required to maintain security.

- Investigates security violations, handles issues imaginatively, efficiently and professionally. Obtains factual information and formulates opinions regarding exposed violations. Where appropriate (i.e. involving employees within own organisation) interviews offenders in conjunction with the relevant line manager or on own authority if warranted.

- In consultation with senior security personnel, devises and documents new or revised procedures relating to access control of all IT environments, systems, products or services to demonstrate continual improvement in control and risk management. Implements any system changes required to maintain security.

- Maintains accurate and complete security records and deals with requests for support according to set standards and procedures. Recognises requirements for, and creates, auditable records, user documentation and security awareness literature for all services and systems within scope, ensuring that the records provide a comprehensive history of violations, resolutions and corrective action.

- Provides general security guidance and advice on security administration and wider security issues.

- Contributes to the creation and maintenance of policy, standards, procedures and documentation for security, taking account of current best practice, legislation and regulation.

- Assists with the assessment of the potential impact on existing access security mechanisms of specific planned technical changes, in order to help ensure that potential compromise or weakening of existing security controls is minimised. Also assists in the evaluation, testing and implementation of such changes.

Security Monitoring, Incident Detection and Response

- Responds to alerts from monitoring and detection systems and uses configured tools and scripts to identify potential cyber security breaches.

- Contributes to the investigation of high-impact security incidents with colleagues from the Security Operations team, other Security specialists and service owners.

- Supports digital forensics examinations through the entire lifecycle (case planning, intake, acquisition, examination, storage, presentation, retention and disposition).

- Supports security recovery processes and procedures, following resolution of incidents. Ensures that resolved security incidents are properly documented and closed.

- Contributes to the analysis of the causes of security incidents and informs service owners to minimise probability of recurrence and contribute to service improvement and maintenance of SLAs. Analyses metrics, such as the incidence, status and speed of resolution of incidents, and reports on the performance of the security incident management capabilities, processes and procedures.

- Follows best practice to ensure all activities are conducted in a forensically safe manner when handling exhibits, e.g. not making changes or interfering with evidence and understanding implications and documenting where this has occurred.

- Carries out, maintains and tests security incident management processes and procedures, engaging with other service owners across IT Services as required.

IT Services responsibilities, accountabilities and duties

- You will be expected to demonstrate a commitment to the IT Services Practice Charter and the University's values. The University of Manchester values a diverse workforce and welcomes applications from all sections of the community.

- You may from time to time be required to undertake other duties of a similar nature as reasonably required by your line manager.

Person specification

Experience/education/qualification background:	• Experience of providing first-line support as part of a security operations team. • Strong knowledge of cyber security principles, technologies and best practices. • Experience with analysing event logs and recognising cyber intrusions or attacks. • Experience using tools such as SIEM, IDS/IPS, antivirus and endpoint detection (e.g. Defender). • Knowledgeable about network protocols and devices. • Experience of working with Windows, MacOS and Linux/Unix operating systems. Desirable qualifications: CompTIA Security+, CompTIA CySA+, CEH, ITIL

Competency (Professional, technical or behavioural)	Level	Essential	Desirable
Incident management tools: Including interrogation of incident database, creation of parent and child incidents, creation of queries to seek trends and use of known error logs/ databases.	Proficient in	X	
Infrastructure/system security architecture: The security threats and vulnerabilities that impact and/or emanate from system hardware, software and other infrastructure components, and relevant strategies, controls and activities to prevent, mitigate, detect and resolve security	Proficient in	X	

incidents affecting system hardware, software and other infrastructure components.			
Access control system: Any tool or system which provides security access control (i.e. prevents unauthorised access to systems).	Proficient in	X	
Network data security: Network security and threat mitigation, including physical, electronic, firewalling, encryption, access and authorisation; protecting data at rest and in transit; defending against viruses and malware; the impact of Big Data; and the integration of robust security controls into enterprise services and policies.	Proficient in	X	
Metrics: The collection, analysis and application of historical and synthetic measurements in the estimation of IT activities.	Proficient in	X	
Business continuity planning: Methods and techniques for risk assessment, business impact analysis, establishment of countermeasures and contingency arrangements relating to the serious disruption of IT services.	Familiar with		X
Risk management: Methods and techniques for the assessment and management of business risk including safety-related risk.	Familiar with		X