Job Description

Job title: Lead Cyber Security Analyst

Grade: 7

Reports to: Head of Cyber Security Operations

Responsible for: The line management, motivation, technical direction, development, training and mentoring of assigned staff

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 Lead Cyber Security Analyst plays a critical role in providing technical expertise and leading the efforts, as part of the Tier 3 level of support, 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 Lead Cyber Security Analyst is expected to have a broad range of knowledge, skills and experience across all security functions and will be asked to provide technical expertise for forensic investigations and security testing, whilst assisting and providing cover as required in other areas.

The Lead Cyber Security Analyst will be engaging with stakeholders across IT Services and the University to understand the security requirements and to gauge the effectiveness of the team's data security initiatives. To maintain the breadth and depth of knowledge, they will need to keep abreast of emerging technologies, security products and threats to ensure these are reflected in the University's security standards and best practices.

Key responsibilities, accountabilities and duties

Forensic investigations

- Leads digital forensics examinations through the entire lifecycle (case planning, intake, acquisition, examination, storage, presentation, retention and disposition). Forms and articulates expert opinions based on analysis.

- Performs comprehensive forensic examinations of computer-based digital evidence and manages information in support of investigations and litigations.

- Develops new techniques and adds to thought leadership in the area of digital forensics.

- Contributes to the development of best practice, including legal matters, to ensure all activities are conducted in a forensically safe manner when handling exhibits. This includes labelling of evidence, not making changes or interfering with evidence and understanding implications and documenting where this has occurred.

- Develops, researches and maintains proficiency in tools, techniques, countermeasures and trends in computer and network vulnerabilities, data hiding, and encryption. Develops and broadens forensic skills through external training and research.

- Leads complex, large-scale digital forensic examinations to include collection in emerging areas such as vehicle, smartphone, live enterprise and volatile environments.

- Provides technical guidance and assistance to other digital forensics and legal staff while ensuring that proper precautions are taken in the preservation and prevention of spoliation of electronic evidence (i.e. intentional, reckless or negligent withholding, altering or destroying of evidence).

- Contributes to the development of policies, standards, procedures and guidelines for laboratory evidence handling and examination, and laboratory safety and security.

- Continually develops and broadens forensic skills, supervising and mentoring others specialising in digital forensic examination. Promotes awareness of policies and procedures.

Security testing

- Provides authoritative advice and guidance on the planning and execution of vulnerability tests. Reviews technical aspects relating to security of customer reports.

- Manages all test processes including test plans, resources, costs, timescales, test deliverables and traceability. Takes responsibility for the integrity and execution of testing activities related to daily operations or change projects.

- Produces test scripts, materials and test packs to test new and existing software, mobile applications, infrastructure and other technical services. Specifies requirements for environment, data, resources and tools.

- Within a development or integration project or programme, coordinates and manages the planning of system, software and hosted platform security testing. Where appropriate, establishes and plans the automated testing strategy for the project or programme, providing a platform for the Security Testing team to automate previously manual scripts.

- Defines and communicates the most appropriate security testing strategy for any projects or programmes. Cooperates with clients/users and senior staff as required to agree the testing strategy to be employed for the projects.

- Ensures that any risks associated with test strategy and the system test plan are clearly documented and reported to the clients/users and colleagues as appropriate, in accordance with organisational processes.

- Manages client relationships with respect to security testing matters for any operational or change activities. Plans, arranges and facilitates meetings, workshops and relationships with key stakeholders during security test planning and throughout subsequent development and testing activities.

- Undertakes investigations to assess and advise on the practicality of security testing process alternatives. Identifies process improvements and contributes to security testing standards and definitions of best practice.

- Takes a lead in designing and implementing simulated attacks on networks, systems or platforms.

- Works with Security Engineers, other developers or integration teams to validate unit tests and/or assist in pair programming techniques to validate code flows.

- Ensures compliance of penetration testing activities with information security policies and standards. Assesses configurations and security procedures for adherence to legal and regulatory requirements.

- Collaborates with other colleagues in Security Operations and other cyber specialists to keep updated with the latest threats and vulnerabilities. Researches potential vulnerabilities and security mechanisms/methods for addressing these concerns.

Line management responsibilities, accountabilities and duties

- Manages, supports and guides the work of groups of staff in line with the operational needs of the Security Operations Team.

- Allocates responsibilities and assigns packages of work to groups of staff.

- Optimises the performance of people, measuring and reporting on performance against agreed quality and performance criteria. Gives regular feedback to teams and individuals on performance against agreed work.

- Facilitates effective working relationships within and between teams of staff. Motivates groups of staff and teams towards a high level of performance.

- Acts as a role model for groups of staff, setting a standard, acting professionally at all times and working to a professional code of conduct and ethics.

- Advises individuals on career paths and encourages pro-active development of skills and capabilities. Provides coaching and mentoring to support professional development.

- Manages probationary periods, setting out the requirements of the job, monitoring progress (e.g., regular meetings) and reacting to variances from expectations, organising training and

development as required within appropriate timescales.

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 leading and managing first-line and second-line security teams, with a focus on monitoring, analysis and intrusion detection. • Good understanding of forensic investigations and using monitoring and detection tools (e.g. SIEM, EDR, XDR, etc.) • Extensive knowledge of security technologies, e.g. SIEM, firewalls, intrusion detection/prevention systems, anti-virus software, authentication systems, log management, content filtering, etc. • Capable of operating network intrusion detection, forensics, network access control and other information security systems. • Extensive experience of running a penetration testing function with a Security Operations team. • Knowledgeable about cyber security certification, e.g. CHECK, CREST, OSCP, SANS. • Highly experienced with using network and application scanning tools and utilities, e.g. SCCM, Nexpose Rapid 7, HP WebInspect, HCL AppScan, Nessus, Burp Suite and NMAP. • Knowledgeable about configuring networks and encryption protocols and algorithms, as well as troubleshooting issues.

	• Proficient in cyber security frameworks such as ISO/IEC 27001, PCI DSS, Cyber Essentials, etc. • Experience of SIEM deployment (e.g. Splunk, LogRhythm, etc.) and management, as well as vulnerability management tooling. • Solid understanding of network intelligence and analytics tools. • Detailed knowledge of forensic tools, techniques and methods. • Experience of malware analysis and incident response. Desirable qualification: CISSP, CISM, ITIL, CEH/OSCP

Competency (Professional, technical or behavioural)	Level	Essential	Desirable
Inclusive Leadership: Able to encourage and inspire others to act inclusively, to engage and value the diversity of thought and background within and beyond their teams and practice an inclusive approach.	Expected behaviour	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 incidents affecting system hardware, software and other infrastructure components.	Expert 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.	Expert in	X	
Metrics: The collection, analysis and application of historical and synthetic measurements in the estimation of IT activities.	Expert in	X	
Application systems: Technical or functional understanding of Commercial Off-the-Shelf (COTS) applications and/or other bespoke software deployed within the organisation in	Proficient in	X	

order to provide system configuration, audit, technical, and/or functional support.			
Security software, tools and techniques: Specialist tools and techniques used in the pursuit of vulnerability management, penetration testing, digital forensics and other security management disciplines for bug-hunting, abstract interpretation and program analysis, binary analysis and reverse-engineering, exploit development, source code analysis, and static and dynamic application security testing (SAST/DAST) etc.	Proficient in	X	
Network traffic analysis: Methods and techniques for the capture of traffic information (packet level) and the forensic analysis of this information into its constituent elements.	Proficient in	X	
Network data gathering techniques: The selection, implementation and application of network data gathering methods, tools and techniques that are appropriate to the information required and the sources available.	Proficient in	X	
Corporate, industry and professional standards: Applying standards, practices, codes and assessment and certification programmes relevant to the IT industry, and the specific organisation or business domain (e.g. cyber security – ISO/IEC 2700 series, PCI DSS, Cyber Essentials, GDPR, etc.)	Proficient in	X	
Risk management: Methods and techniques for the assessment and management of business risk including safety-related risk.	Proficient in	X	