Information Security Analyst



ROLE DESCRIPTION

GRADE

Grade 4 (£27,116-£32,344)

LOCATION

Craiglockhart, Edinburgh

LINE MANAGER

Information Security Manager

ROLE SUMMARY

The role of the Security Team is to keep the University and its people safe from all forms of cyber security threat, working to minimise the likelihood of disruption to teaching, research and business activities. It does this through a combination of security technologies, controls, processes, policies and by working in partnership with colleagues across the University to ensure that everyone understands the part they play in staying safe online.

As an Information Security Analyst, you will be an active participant in all of the key operational activities of the Security Team, including monitoring for, and responding to, attacks and alerts, handling requests and queries, performing routine changes to security solutions, updating documentation, assisting other members of the team to complete larger pieces of work. You will develop your own knowledge and skills in the field of information security and promote best practice with colleagues across the University.

LINE MANAGEMENT RESPONSIBILITY FOR:

This role does not have any line management responsibilities currently.

MAIN DUTIES AND RESPONSIBILITIES

- Use the University's SIEM, SOAR and other security solutions to monitor for, and respond to, attacks, intrusions and unusual, unauthorised or illegal activity and respond according to established incident response procedures, or as directed by other members of the Security Team.
- Monitor for, and conscientiously respond to, messages, requests and queries, providing advice and support required to effectively complete the request. This includes communicating with students, staff, suppliers, external bodies. The role holder may be requested to participate in the "Out of Hours Support" scheme if required.
- Contribute to the creation and review of process, system and end user documentation, ensuring full coverage and high quality, filling in gaps, making improvements based on feedback, updating or retiring outdated information and requesting additional documentation from individuals or teams.
- Perform routine operational activities on security solutions e.g. configuration changes or upgrades and other similar tasks as directed by other members of the Security Team or Information Services management. This may occasionally require working outside normal business hours.
- Perform routine security investigations and incident response, audit or project activities, completing the work independently according to agreed standards. This may occasionally require working extended hours as determined by the severity of the incident.
- Assist other members of the Security Team with conducting more complex security investigations and incident response, audit or project activities. This may occasionally require working extended hours as determined by the severity of the incident.
- Maintain an enthusiasm and passion for information security and a commitment to ongoing professional development in this area, by attending relevant conferences or events, obtaining recognised security certifications or developing a specialisation for a particular area of information security or technology.
- Promote security best practice across the University.
- Role model the University's values & behaviours.
- Be responsible for ensuring that the information and records processed (received, created, used, stored, destroyed) on behalf of the University are managed in compliance with ALL applicable legislation, codes and policies e.g. Data Protection, Information Security and Records Management.

PERSON SPECIFICATION

	ESSENTIAL	DESIRABLE
EDUCATION / QUALIFICATIONS		
• A degree in a relevant discipline. Candidates with other qualifications will be considered if they also have practical experience in a relevant role.	✔	
• CompTIA Network+, CompTIA Security+, or any other similar industry/professional certification, ideally related to cyber security.		✔
SKILLS / EXPERIENCE		
• Knowledge of the information security issues faced by organisations.	✔	
• Knowledge of common security threats and how they can be defended against.	✔	
• Knowledge of relevant networking concepts – IP addresses, subnets, protocols/ports, DHCP, DNS, HTTP, TLS, VPN.	✔	
• Knowledge of basic operating system concepts – users, groups, files, executables, processes, sockets.	✔	
• Knowledge of basic system and application access control concepts – roles, permissions, inheritance, nesting, precedence, access control lists, allowlists, blocklists.	✔	
• Experience of working with system and application log files, including correctly establishing the order in which events occurred and combining information from multiple sources.	✔	
• Good analytical, logical thinking and problem-solving skills, with a strong desire to understand how things work and why things are.	✔	
• Good written and verbal communication skills, with an ability to share information clearly and concisely in both styles.	✔	
• Good organisational skills, with an ability to handle multiple pieces of work at the same time and to deliver results within agreed timescales.	✔	
• An independent and proactive learner, but with a willingness to seek advice or support when necessary.	✔	
• Experience of working in an IT helpdesk or end user IT support role.	✔	

	ESSENTIAL	DESIRABLE
• Experience of working in a Security Operations Centre or similar role.		✔
• Knowledge of and experience using SIEM solutions.		✔
• Knowledge of and experience using SOAR solutions.		✔
• Experience of writing simple scripts (in a common language such as PowerShell or Python) to automate tasks, retrieve and manipulate data, integrate systems, etc.		✔
• Experience of using Endpoint Security solutions to detect and remove malware from devices.		✔
• Knowledge of and experience using network-level firewalls, Intrusion Prevention Systems, web filtering solutions and VPNs.		✔
• Experience of using several different operating systems.		✔
• An awareness of the higher education environment and the challenges this can pose for the adoption of rigorous security policies and controls.		✔