

Junior Cyber Security Analyst

Job Level	3	Korn Ferry Function	KF 13
Directorate	Technology	Function/Service	Cyber Security
Direct Reports	None	Indirect Reports	None
Line Manager Title	Cyber Security Manager	Budgetary Responsibility	None

Our Leadership Framework defines the leadership standards we want to see at the British Red Cross. It shows what great leadership looks like. Our goal is to create a great workplace and deliver excellent services to our users. [Our Leadership Framework - RedRoom](#), along with [Our values and behaviours - RedRoom](#) and Fundamental Principles, helps everyone understand how the leadership capabilities relate to their role and context.

Diversity is something we celebrate, and we want you to be able to bring your authentic self to the British Red Cross. We want you to feel that you are in an inclusive environment, and a great position to help us spread the power of kindness. You can read more about [Equity, Diversity & Inclusion \(EDI\) at the British Red Cross - RedRoom](#) here.

Role Description	
Purpose	<p>The role is responsible for supporting day-to-day cyber security operations and first-line defence of the British Red Cross's digital environment, including monitoring and triaging security alerts and service tickets, perform initial analysis and incident response support, and coordinates with more experienced security analysts and engineers to ensure that cyber security threats and vulnerabilities are identified, prioritised, and addressed in a timely manner.</p> <p>The role covers a broad range of security domains, including vulnerability management, secure operations, identity and access management, cyber threat intelligence, network monitoring and intrusion detection, and incident response, providing the role holder with exposure to multiple facets of cybersecurity as they develop their skills and knowledge.</p>
Key Responsibilities	<p>Security Monitoring & Incident Triage</p> <ul style="list-style-type: none"> Daily monitoring and review of security dashboards, alerts, and logs to identify potential security events or incidents, performing initial triage to determine the nature of alerts, filter out false positives, prioritise genuine threats, and ensuring prompt action. Following standard operating procedures and playbooks, conducting basic analysis of security events and incidents, such as suspicious emails, malware alerts, unusual user activities, collating relevant data and evidence, identifying likely causes, and escalating complex or high-risk incidents to senior team members with clear, well-documented findings. Assist in security incident response activities, including communicating with end-users or IT teams during incidents to gather information and implement immediate mitigation steps, documenting actions taken, and participating in post-incident reviews to capture lessons learned. <p>Vulnerability & Threat Management Support</p>

	<ul style="list-style-type: none"> • Support the vulnerability management process by running automated vulnerability scans on networks and systems, identifying vulnerabilities from scanner outputs, and performing an initial assessment of severity and impact. • Work with resolving teams to track remediation of vulnerabilities, following up with system owners and verifying that critical vulnerabilities are resolved within expected time frames. • Assist senior analysts in gathering and processing threat intelligence, such as monitoring threat feeds or advisories for emerging risks. Then using this information to help update internal security controls or alerting mechanisms, such as verifying that known malicious IPs or indicators of compromise are integrated into protective monitoring systems, and sharing relevant insights with the team and other stakeholders when needed. • Provide support for identity-related security tasks such as account audits, password resets for privileged accounts, monitoring for unauthorised access attempts, or verifying that access control changes follow correct processes. <p>Operational Support & Service Improvement</p> <ul style="list-style-type: none"> • Respond to cyber security service requests and incidents logged in IT service management (ITSM) tools, ensure that tickets are appropriately categorised, prioritised, and actioned in line with agreed service levels (SLAs). • Work closely with colleagues when dealing with complex issues, taking ownership through to resolution, and ensuring that escalated incidents or support requests include all necessary information for efficient resolution. • Identify opportunities to streamline security operations and reduce repetitive workload through “shift-left” initiatives. • Help maintain up-to-date security documentation and contributing to the team knowledge base so that similar issues can be resolved more quickly in the future. <p>Professional Development</p> <ul style="list-style-type: none"> • Engage proactively in on-the-job training and development, recognising that this is an entry-level role with a steep learning curve. • Show curiosity and initiative in learning new tools and techniques, including exploring relevant self-study materials. • Participate actively in team meetings, stand-ups, and incident debriefs, listening and contributing your perspective.
<p>Know-How</p> <p>[s] is used to denote the minimum shortlisting criteria.</p>	<p>Essential</p> <ul style="list-style-type: none"> • Proactive and curious, with a desire to improve processes and eager to learn from each situation. • Strong analytical mindset with attention to detail, able to approach problems systematically, gather relevant data, and assist in troubleshooting technical issues under guidance. • Methodical approach to following procedures, handling multiple tasks, and meeting agreed deadlines or response time targets.

	<ul style="list-style-type: none"> Tackling challenges that required attention to detail, persistence, and collaboration. Working as part of a team, cooperating with others, following processes, and contributing to shared outcomes. Capable of organising and prioritising workload in a busy operational environment. Basic understanding of IT and cyber security fundamentals, such as knowledge of how computers, networks, and operating systems work, and an awareness of common cyber security concepts, such as malware, phishing, firewalls, multi-factor authentication. <p>Desirable</p> <ul style="list-style-type: none"> General awareness of one or more cyber security domains, such as threat monitoring, incident response processes, vulnerability scanning, or access management, whether gained via formal education, personal study, or hands-on practice in a lab or internship environment. Practical experience or voluntary involvement in security and/or IT projects. Knowledge of IT support or technical service desk procedures and roles, whether gained through internships, volunteering, or part-time work, where responsibilities included handling technical requests or troubleshooting issues for end users. Awareness of best-practice frameworks for IT and/or cyber security. An active interest or engagement in cyber security beyond formal education and/or employment is highly valued.
Additional Requirements	None

Pre Engagement Checks Highlight bold as required	
DBS- England & Wales	None
PVG- Scotland	None
Access NI- Northern Ireland	None
Driver Check	No
<u>International Roles Only</u>	
International Police Check	No
International Driving Licence for manual cars	No

Role Reference		Review Date	
-----------------------	--	--------------------	--



We guarantee an interview to disabled candidates (as defined in the 2010 Equality Act), who meet the minimum shortlisting criteria in the advertised person specification and apply under the disability confident scheme.