**ROLE PROFILE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role Title** | Cyber Security Administrator | **Location** | Bristol or London |
| **Business Unit** | Technology | **Job Family** |  |
| **Reports to Role Title** |  | **Sub Family** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **PURPOSE** | | | |
| The purpose of this role is responsibility for delivering day-to-day information security assurance activities and to support cyber security operations. This includes, but is not limited to, supporting general testing activities, supporting security incident remediation and providing communication and awareness functions.  **Purpose**   * To support the Technology team in ensuring that corporate IT systems and controls are tested, assured, represented and reported accurately and appropriately * To engage, support and work closely with the business at all levels to ensure information security regulations, requirement and policies are understood, communicated, & implemented effectively across all business functions * Support security operations and cyber incident management * Create awareness and training material, drive user compliance activities and contribute to a culture of Information security management | | | |
| **CORE ACCOUNTABILITIES** | | | |
| The Cyber Security Administrator will:   * Assist in the research, selection and deployment of new technical security controls for use by C&C Group * Support the organisation’s safe advancement with new technology and ways of working by leading the design, creation and application of appropriate technical security policies * Advise on matters related to cyber security, such as in the support of procurement and project activity * Work closely with Technology Operations to ensure critical business assets are adequately protected from cyber-related threats through the use of appropriate technical controls * Document and raise non-conformities with the CISO * Produce regular reporting to demonstrate the effectiveness of technical security controls and identify gaps and recommendations where needed * Work closely with Procurement, Data Protection & Risk teams on supplier due diligence activity. * Support of cyber-related audits and certifications plus assisting in the remediation of any findings * Manage third-party security (supplier) relationships and assist in the development of existing relationships and the competitive selection of new suppliers * Assist with ongoing colleague education related to cyber security, helping with phishing simulations, awareness campaigns and ad-hoc queries that come into the team. * Support incident investigations * Help to develop strategies and roadmaps for cyber security technology, in step with the Technology Strategy and other business planning activity * Work with third-party security providers and network administrators to track down security vulnerabilities in the information sharing network to ensure that such weaknesses in the system are addressed and remedied efficiently * Research any vulnerabilities in security and ensure that they are incorporated into the patching schedules * Monitor the third-party management of AV solutions and ensure policies are implemented to the company standards * Work with the business users to ensure that we share information securely, by defining the security standards for sharing e.g. Microsoft SharePoint and work with the administrators to provide secure access * Monitors industry best practice web sites and standards and identifies change requirements to the organisations security policies and procedures | | | |
| **CONTACTS/ KEY RELATIONSHIPS & NATURE OF INFLUENCE** | | | |
| **Internal:**   * IT Support & Technical Teams * Senior Management   **External:**   * 3rd Party Service Providers | | | |
| **KNOWLEDGE/ EXPERIENCE/ SKILLS** | | | |
| A good understanding of the following:   * Endpoint security * SIEM platforms * Windows Server technologies, Active Directory and Entra ID * Networking concepts (DNS, IP, segregation techniques) * Cloud computing concepts and service models IaaS/PaaS/SaaS * Authentication concepts (Windows, Entra ID, Managed Identity) * Microsoft 365 security and compliance * MITRE ATT&CK Framework * Cyber Essentials/Essentials Plus, GDPR, ISO 27001 and other information security-related regulatory and compliance standards | | | |
| **PROFESSIONAL QUALIFICATIONS & EDUCATION** | | | |
| * A degree in Cyber Security, Information Technology, Computer Science, or a related field is preferred * Relevant certifications such as CISSP, CEH, GCIH, or equivalent are highly desirable | | | |
| **TECHNICAL/ BEHAVIOURAL/ PERSONAL COMPETENCIES** | | | |
| * To have a genuine passion for Cyber Security and its technology, and a drive to continually develop professional and personal knowledge in this fast-moving area * Be self-motivated and able to work to a high standard under own initiative * Able to pay and maintain close attention to detail * Have sound analytical skills; able to think laterally and challenge existing concepts * Be a good and confident communicator at all levels; an ability to assert and defend a point of view that can be balanced with pragmatism at times * Must be able to operate as a member of the wider Technology team, contributing to a wide range of Information Security risks and issues, to provide joint outcomes * Have the ability to understand technical complexities and issues, and be able to explain and translate these to a less technical audience * Have a good understanding of security threats, attack scenarios, intrusion detection techniques and incident management * Awareness of information risk, assurance and information security strategy programs, within large corporate environments is desirable * Awareness of information security principles (Confidentiality, Integrity, Availability) * Awareness of communication channels and methods of influence (Awareness, Behavior, Culture) * Awareness of web apps design, development and deployment across different platforms * Awareness of enterprise technologies including associated security vulnerabilities and exploits * Experience dealing with malware and attack vectors | | | |
| **BUSINESS SPECIFIC REQUIREMENTS (Optional Section)** | | | |
|  | | | |
| **OPERATING ENVIRONMENT & CONTEXT:**  **TRAVEL & OTHER REQUIREMENTS** | | | |
| **ROLE DIMENSIONS** | | | |
| No of Direct Reports | 0 | Financial Impact (Direct) |  |
| Total Team Size | 5 | Financial Impact (Indirect) |  |
| No of Locations |  | Other/ People Manager (yes/ no) |  |

Back Office Use only:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Job Code** |  | **Reward Level** |  | **TW Grade** |  |
| **Salary Survey Ref** |  | **Career Level** |  | **Date Created** |  |
| **Salary Min** |  | **Salary Mid** |  | **Salary Max** |  |