Job Description:
Cyber Security Specialist

Function:	Service Operations / IS&T
Job:	
Position:	Cyber Security Specialist
Job holder:	Vacant
Date (in job since):	
Immediate manager (N+1 Job title and name):	Regional CISO
Additional reporting line to:	
Position location:	Salford DC / Homeworker

1. Purpose of the Job – State concisely the aim of the job.

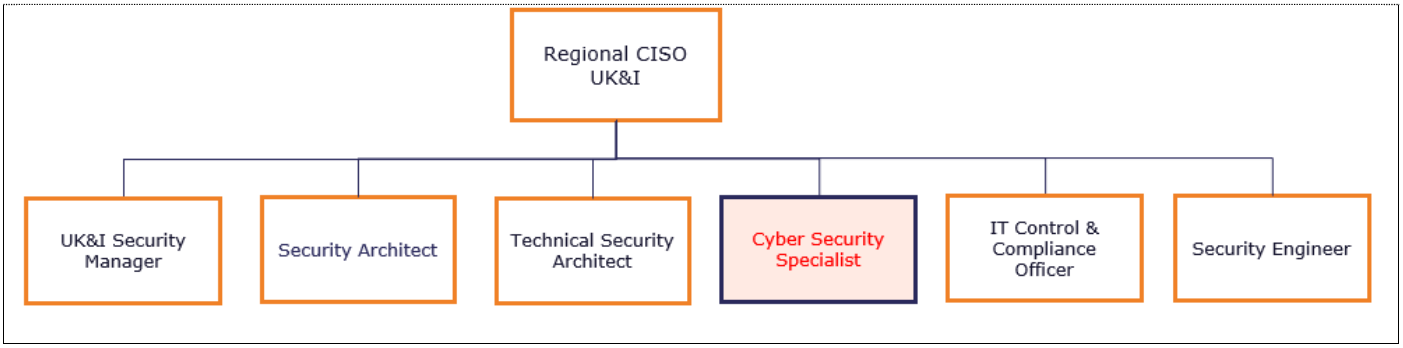
- Drive the reduction of vulnerabilities across Sodexo and its suppliers by developing and maintaining enterprise processes, procedures and tools
- Deploy and maintain security solutions (antimalware, EDR, MFA, etc.)
- Monitor the evolution of the threat landscape and propose countermeasures
- Increase operational security domain efficiency by automating ineffective processes

2. Dimensions – Point out the main figures / indicators to give some insight on the "volumes" managed by the position and/or the activity of the Department.

Characteristics

- Act as a subject matter expert on security solutions covering an estate comprising:
  - 13,000 users
  - 12,000 workstations
  - 8,000 mobile phones
  - 300 on premise servers
  - 2,000 interconnected sites and networks with varying security needs and connectivity
  - 100-200 of SaaS solutions accessed remotely
  - 100 technology suppliers providing support and maintenance to systems deployed on site
- Deal with hundreds of vulnerabilities

3. Organisation chart – Indicate schematically the position of the job within the organisation. It is sufficient to indicate one hierarchical level above (including possible functional boss) and, if applicable, one below the position. In the horizontal direction, the other jobs reporting to the same superior should be indicated.



4. Context and main issues – Describe the most difficult types of problems the jobholder has to face (internal or external to Sodexo) and/or the regulations, guidelines, practices that are to be adhered to.

- Interact with multiple stakeholders across IS&T (infrastructure, applications, PMO, security, etc.) and the wider business when needed
- Influence decisions and actions without direct authority
- Deal with resistance to change
- Develop an automate first approach in a very manual landscape
- Work with legacy environments and assets and find suitable workarounds to standard remediation procedures
- Work with external suppliers on their remediation activities without direct IT oversight

5. Main assignments – Indicate the main activities / duties to be conducted in the job.

- Vulnerability Management
  - Define and maintain a vulnerability testing programme across Sodexo and its suppliers to ensure vulnerabilities are timely identified and handled adequately
  - Monitor vulnerabilities for the whole estate covering on premise assets but also external SaaS and public Cloud assets as needed
  - Lead the penetration tests and technical security audits schedule (source code review, architecture review, etc.), report findings and lead the remediation program
  - Support business stakeholders, suppliers when needed, and the wider IS&T department in defining appropriate action plans
  - Prioritise vulnerability management remediation activities to ensure a sound approach to
  - Continuously improve the vulnerability management procedures and process
- Operational Security
  - Act as the Subject Matter Expert (level 3) on security solutions (antimalware, vulnerability scanner, EDR, MFA, etc.) and work as solution owner
  - Be the spokesperson and referent for the deployment of security solutions
  - Provide expertise and implement technical security protocols (encryption, DMARC, etc.)
  - Support activities in the security architecture domain to ensure security is adequately implemented in architecture design

- Assist with major security incidents as instructed by management
- Review change requests and provide technical recommendations as needed

- Continuous improvement
  - Contribute to pilots and proof of concepts to enhance IT & Cyber Security capabilities
  - Automate manual processes to gain in efficiency and reduce errors
  - Support the Operational Security domain in developing new processes, procedures, and tools
  - Stay up to date with evolving threats and mitigation techniques

6. Accountabilities – Give the 3 to 5 key outputs of the position vis-à-vis the organization; they should focus on end results, not duties or activities.

- Ensure vulnerabilities are identified and communicated to business stakeholders, and appropriate action plans are implemented to reduce risks
- Ensure security solutions are in place and operating as expected
- Provide technical security expertise for ad-hoc requests or projects for new security solutions
- Automate any security process possible

7. Person Specification – Indicate the skills, knowledge and experience that the job holder should require to conduct the role effectively

- Demonstrated experience of driving reduction of vulnerabilities within an enterprise
- Experience with risk-based vulnerability management
- Experience of establishing and maintaining operational security solutions management processes, procedures, and tools at enterprise level
- Hands-on experience of selecting, deploying and maintaining a variety of security solutions such as vulnerability appliances/agents, EDR, antimalware, MFA, etc.
- Hands-on experience in network/server and security operational roles
- Experience in automating manual processes in line with DevOps/DevSecOps
- Experience of leading penetration testing and technical security audit engagements
- Experience of communicating technical information to a non-technical audience to define relevant action plans with the business and IS&T
- Proficiency in core information security principles (access control, operating system security, vulnerability management, etc.)
- Solid understanding of exploitable vulnerabilities
- Knowledge of MITRE ATT&CK framework
- Knowledge of NIST framework and OWASP
- Knowledge of Microsoft Enterprise access model and AD tier model
- Knowledge of the Zero Trust concept
- Rigorous and organised
- Resilient
- Experience of penetration testing is a plus
- Experience of establishing and conducting proof of concepts with security solutions is a plus

8. Competencies – Indicate which of the Sodexo core competencies and any professional competencies that the role requires

▪ Rigorous management of results
▪ Innovation and Change
▪ Business Consulting

9. Management Approval – To be completed by document owner

Version	1.0	Date	17 January 2022
Document Owner	Regional CISO UK&I		