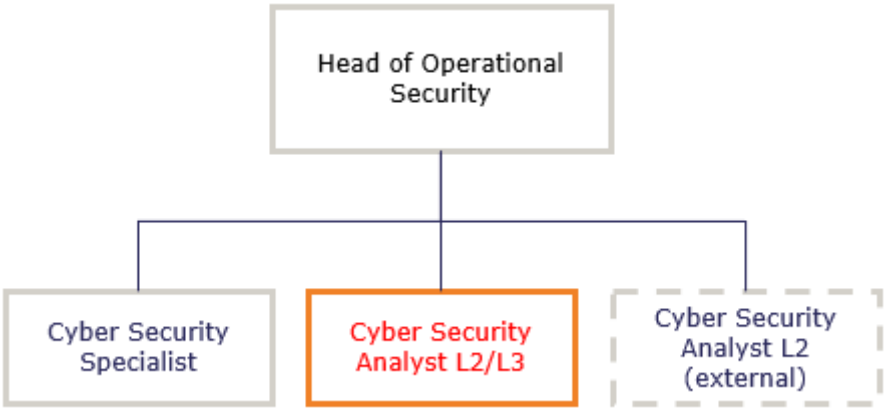
Job Description:
Cyber Security Analyst L2/L3

Function:	IS&T
Job:	[Enter generic job title] Refer to Invent Position Title Guidance
Position:	Cyber Security Analyst L2/L3
Job holder:	Vacant
Date (in job since):	N/A
Immediate manager (N+1 Job title and name):	Head of Operational Security
Additional reporting line to:	N/A
Position location:	Flexible

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

- Monitor networks and systems, detect security threats ('events'), analyse and assess alerts
- Report on threats, intrusion attempts and false alarms, either resolving them or escalating them, depending on the severity
- Contribute to the definition and revision of the security data collection strategy
- Provide support to infrastructure administrators in the deployment of detection systems
- Feed internal knowledge bases for capitalising on threats and vulnerabilities
- Ensure the continuous improvement of service processes

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.

- This role may be expanded with requirements relating to internal control, risk management and preventive cybersecurity
- The increase of security requirements due to implementation of new regulatory requirements for compliance with standards and practices
- The increase, diversity and multiplication of threats further underline the importance of security-related technology watching

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

- Take full ownership of incidents escalated by Analyst level 1 or the SOC and control quality of actions performed
- Investigate and analyse cybersecurity incidents and follow up action plans
- Assist the modelling of new attack scenarios
- Coordinate regional cyber response activities with IT and business stakeholders, and contribute to global cyber response activities as needed
- Build response instructions and execute level 2 containment measures, document processing of incident within the incident orchestration solution (SOAR)
- Monitor APT (threat detection, reporting, contextualisation)
- Perform 'hunting' activities based on information collected by the Analysts and the Cyber Threat Intelligence
- Complete cyber forensics activities when required (threat scenarios, malware analysis, etc.)
- Perform technological watch (collect information about the most recent attack techniques and threats, identify potential data leak, etc.)
- Continuously update processes and documentation to improve detection rules, as well as containment and remediation playbooks
- Contribute to the development of the global security operations centre maturity and processes
- Develop and expand tools supporting day to day to SOC analyst roles (sandbox, lab, etc.)
- Share regularly appropriate knowledge with level 1 support to improve overall competencies in handling cyber security incidents

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.

- Coordinate cybersecurity response activities to contain threats and remediate gaps
- Ensure operational processes and procedures are fit for purpose to deal with current and emerging cyber threats
- Ensure that cyber security incidents are treated timely and with quality to mitigate the cyber risk
- Ensure that significant/potential cyber security incidents are timely escalated when needed to ensure appropriate focus from management and minimise adverse impact to the information system

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

- Learn through experimentation when tackling new problems, using both successes and failures as learning fodder
- Rebound from setbacks and adversity when facing difficult situations. Experience of dealing with stressful contexts and situations when facing cyber crisis
- Experience of working and partnering with other technology teams to resolve cyber security incidents
- Experience of communicating effectively technical information to a technical audience without expertise

- Experience of communicating effectively technical information and articulate risks to non-technical audience and senior management in crisis situations
- Experience of persuading technical individuals and teams who share different objectives and priorities to deliver the security activities expected from them
- Experience of performing threat hunting and digital forensic on computers, servers or network assets
- Experience of developing scripts (Python, REGEX, Powershell, Shell, etc.) quickly in reaction to incidents or for proof of concepts
- Demonstrated experience of strong knowledge in information security principles (security principles applied to architecture, network & systems, cyber forensic, security risk assessment, software development)
- Actionable knowledge of MITRE ATT&CK framework
- Knowledge of NIST framework and OWASP
- Solid understanding of exploitable vulnerabilities and remediation techniques
- Experience of penetration testing is a strong plus
- Experience in automating manual processes for responding to cyber security incidents is a strong plus
- Experience of Threat Intelligence and CERT/CSIRT activities is preferred

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	16 February 2022
Document Owner	Regional CISO UK&I		