Role Title	Cyber Defence Principal Analyst
Reports to	Cyber Defence Team Leader
Directly Supervises	0
Total team size	12

Role Purpose

Reporting to the Cyber Defence Team Leader, the Cyber Defence Principal Analyst is the lead technical role within the Cyber Defence team. Supporting the Cyber Defence Team Leader and inspiring a shared vision to uphold the security of BTS and the businesses we support.

Associated British Foods plc | Business Technology Services

Key accountabilities:

- Providing a point of escalation for security investigations.
- Deputising for the Cyber Defence Team Leader when required.
- Development of processes to enhance our defensive capabilities and to remain current within a changing threat landscape and technologies.
- Create, publish and maintain support documentation and knowledge articles to ensure the team operates effectively.
- Ensure that the team is operating to the highest standards, and within Service Level Agreements (SLA)s, to protect Associated British Foods (ABF) information and information systems.
- Driving improvement in the quality of investigations and technical proficiency within the Cyber Defence team through quality assurance reviews.
- Respond to end-user security incidents, as referred by the service desk, and to other sources of information which may provide indicators of compromise.
- Ensure completion, reporting and resolution/escalation of any scheduled shift tasks.
- Monitoring and analysis of security relevant logs, alerts and events; handling incidents submitted to the Security Operations Centre (SOC).
- Execution of standard operating procedures (SOPs) in response to any security relevant logs, alerts, and events.
- Working with the Cyber Response Team, as part of a wider Incident Response team, to help determine root cause analysis for events which constitute formal security incidents.

Essential skills, knowledge & experience:

- Display a business enabling mindset, whilst collaborating with relevant teams to secure data and systems.
- Excellent communication skills with a variety of stakeholders.
- Coaching and leadership of team members.
- Demonstrable ability to prioritise and pragmatically investigate events and incidents, providing relevant reporting and communication to stakeholders.
- Excellent analytical and problem-solving skills, with an attention to detail.
- An investigative mindset with the ability to think laterally.
- Experience with technical and reporting writing.
- Possess an understanding of security standards, controls and risk management.
- Possess the ability to adjust and adapt to changing priorities in a dynamic environment.
- Be able to prioritise tasks, whilst being pro-active in addressing issues and requests.
- Possess technical acumen and the ability to understand and interpret technical specifications.
- Understanding of a range of core security related technologies deployed in a complex enterprise environment including:
    - EDR/XDR
    - SIEM/SOAR
    - IDS/IPS & Firewalls
    - Anti-Virus/Anti-Malware
    - Vulnerability Analysis
    - Identity & Access Management toolsets
    - Threat Intelligence Platforms
- Willingness to enhance individual capabilities through training.

Desirable skills, knowledge & experience:

- Bachelor's degree in computer science, Engineering/Information Security/related field, or comparable experience in industry.
- Experience in computer science, computer engineering, mathematics, or related field.
- Security Operations Centre (SOC) experience overseeing the review of security log events and console level alerts/information.
- CompTIA CYSA + or other relevant , security, networking or software engineering certifications would be preferable.
- Willingness to mentor junior colleagues.

Other requirements of the role:

- The SOC operates 24/7/365 and the role requires the ability to operate on a shift basis, working 12-hour shifts, equating to an average 42 hours per week.
- UK Remote Working – Occasional visits to the Peterborough Head Office as required.
- Willing to travel to other locations - suppliers/vendors, etc., when necessary.