Role Title	Cyber Defence 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 Analyst will conduct analysis of security related events to include validation, escalation, and reporting upon any indicators of compromise based upon the guidelines and monitoring platforms provided to them. The Analyst will be responsible for handling all such events of interest and will make sure that they are continuously monitored and reviewed providing appropriate updates to customers and stakeholders.

Associated British Foods plc | Business Technology Services

Key accountabilities:

- To ensure completion, reporting and resolution/escalation of any scheduled task
- Responding to security cases and incidents in a timely manner
- Monitoring and analysis of security relevant logs, alerts and events, handling incidents submitted via tickets, email, or telephone
- Execution of standard operating procedures in response to any security relevant logs, alerts, events, and investigations
- Contribute to the progressiveness of the SOC by participating in proactive activities and operational improvements.
- Services monitored will include, but are not limited to SOAR, SIEM, IDS/IPS, Firewalls, AntiVirus/Anti-Malware, XDR, Vulnerability Analysis, Identity & Access Management toolsets, Azure, and Email Security Platforms
- Working with the Incident Response team to help perform and document root cause analysis of formal security incidents
- Working closely with other IT teams or customers on technical matters building strong relationships
- Conducting vulnerability management assessments and risk analysis on assets

Essential skills, knowledge & experience:

- Ability to effectively prioritize and execute tasks in a high-pressure environment
- Any Experience with a range of core security related technologies in an enterprise environment including SOAR, SIEM, XDR, IDS/IPS, Firewalls, Anti-Virus/Anti-Malware, Vulnerability Analysis, Identity & Access Management toolsets, Azure, and Email Security Gateways
- Knowledge of computer networks and firewall systems
- Ability to remain calm when under pressure
- Excellent analytical, attention to detail and problem-solving skills
- Have excellent written and verbal communication skills in English
- Possess the ability to adjust and adapt to changing priorities in a dynamic environment
- Be able to multi-task and be pro-active in addressing issues and requests
- Experience with technical writing and process documentation
- Possess technical acumen and the ability to understand and interpret technical specifications
- A genuine interest in Cyber Security, intrusion prevention and appetite to remain current on the latest cyber threats and best practices in information security.

Desirable skills, knowledge & experience:

- CompTIA Security + or other relevant security qualifications
- CompTIA Security + or other relevant security qualifications
- Bachelor's degree in Computer Science, Information Security, Computer Engineering, Mathematics, or related field
- Security Operations Centre (SOC) experience or experience of working as a Security Analyst, overseeing the review of security log events and console level alerts/information
- Possess an understanding of security standards and risk management frameworks
- Any experience in Malware Analysis, Cyber Threat Intelligence or Threat Hunting

Other requirements of the role:

- The SOC operates on a 24/7/365 basis 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 – Visits to Peterborough Head Office about once a quarter for team meetings.
- Willing to travel to other locations - suppliers/vendors, etc., when necessary.