|  |  |
| --- | --- |
| **Role Title:** | Principal Network Defence Analyst |
| **Report to (title):** | DevSecOps Manager |
| **Function/Department:** | Cyber Security |
| **Associated British Foods (ABF) Business Technology Services (BTS) Overview** | |
| Standard wording | |

|  |
| --- |
| **Role Summary** |
| The Principal Network Defence Analyst plays a key role in the Cyber Security team. Supporting the DevSecOps Team and the Security Operations Centre (SOC) in inspiring a shared vision, to transform BTS’ IT service provision, in line with the BTS vision and values.  The DevSecOps team are responsible for all components within the Security Products ensuring that these are managed including Lifecycle, Capacity, Monitoring, Cost & Licensing, Innovation, and Security. |

|  |
| --- |
| **Role Responsibilities/Accountabilities** |
| Act as a technical **networking subject matter expert** within Cyber Security. |
| **Proactively** triage and manage **the patching of network infrastructure** (switches, firewalls) in a timely manner, whilst limiting adverse business impact. **Automating** discovery and remediation processes, as appropriate. |
| Drive innovation and continuous improvements to existing security products/services as well as development of **new products/services**, particularly from a networking perspective (Network Detection and Response solutions, IPS, IDS, packet capture and analysis). |
| Producing Network Security Technical standards, best practices and delivering security functional briefings to BUs and BTS teams. |
| Development of networking skills and knowledge within the team and into the wider security teams. |

|  |
| --- |
| **Shift/Working Pattern** |
| * This role is a 37.5-hour week Monday – Friday * Speak with us about flexible working. We are happy to discuss flexible working patterns for this role. |

|  |  |
| --- | --- |
| **Experience, Knowledge, Skills & Attributes** | |
| **Essential** | **Desirable** |
| Good skills in technical environments and advising on security controls within large complex organisations | Industry recognised qualifications including but not limited to Cisco Certified Network Associate (CCNA), Check Point Certified Security Administrator (CCSA) |
| Good understanding of information security standards and best practice including ISO 27001 and the NIST Framework | Security industry standard certification(s) (CISSP, CISM, CCSP, CEH, Sec+, CySA+, CASP+) |
| Knowledge of current security trends and potential technical ramifications of changing environments on current and future technology solutions | Experience of running Penetration Testing engagements (scoping, supporting, tracking, and managing remediation activities) |
| Excellent analytical and problem-solving skills.  Experience managing multiple stakeholders, both internal and external (vendors, third parties) | Technical knowledge of Cisco, Avaya and Extreme products |
| Technical experience including:  • WAN technologies (SD-WAN and Fabric) Azure /  Other Cloud providers  • LAN technologies (Cisco/Extreme Appliances)  • Security appliances (Palo Alto, Checkpoint)  • System Management technologies; SolarWinds.  • Cloud base Internet proxy solutions (zScaler)  • Network Detection and Response (NDR) tooling | Demonstratable knowledge and experience of packet capture and analysis in a large complex organisation and familiarity with associated tooling (WireShark) |
| Maintain performance when under stress, and manage time effectively through the application of organisation and planning skills | An understanding of Cyber Threat Intelligence principles |
| Understanding of sound Security Architecture principles (e.g. cloud vs on-prem, interoperability between services and infrastructure) | Passionate about emerging technologies, such as machine learning and artificial intelligence, to facilitate workflows |

|  |
| --- |
| **Decision Making, Influence & Key stakeholders** |
| Ability to influence cross-functional teams without formal authority |
| Ability to present and articulate technically complex work clearly to stakeholders in a variety of formats to different technical levels and audience types |
| Self-motivated, self-disciplined, used to acting on own initiative and taking ownership |
| Strong team player with ability to collaboratively deliver results |
| Maintaining and developing relationships with security, platforms, client protect, change management and connectivity and all other BTS teams |

|  |
| --- |
| **Other Information** |
| This role is contracted to our Peterborough head office however we are looking for a remote working pattern. You will need to be flexible to travel to Peterborough as needed however majority of this role can be done remotely.  Applicants must be willing to travel to other locations/suppliers/vendors etc when necessary. |