# JOB DESCRIPTION

| 1. JOB SPECIFICS | |
|---|---|
| Job Title: | Security Operations Centre Analyst |
| Reports to: | Security Operations Manager |
| Location: | Leeds (Brown Lane West) |
| Department: | IT |

| 2. ABOUT THE ROLE | |
|---|---|
| What you'll be doing? | Working in the Security Operations Centre, you will monitor, identify and respond to security events spanning the organisation, multiple systems and locations. You will work with, maintain and leverage key security technologies including SIEM, IDS and Endpoint. |
| Key Responsibilities | Monitor, analyse and investigate alerts, log data and network traffic using SIEM/EndPoint platforms and Internet resources to identify cyber-attacks/security incidents<br>Report suspicious activity and identified incidents to the relevant IT or business team<br>Escalate suspected major security incidents/complex investigations where support is required<br>Conduct security assessments to identify vulnerabilities and performing risk analysis.<br>Define monitoring use cases and develop prototype rules e.g. in response to intelligence or gaps in defences<br>Advise and implement necessary changes required to counter attacks or improvise security standards/services<br>Generate reports for IT administrators, business managers, and security leaders to support management and security evaluation of systems/services<br>Ensure services are operated in line with agreed service definitions and measures<br>Contribute to the development of the services through process, people and technology where appropriate<br>Build a comprehensive knowledge of QA IT systems to support monitoring activities and tailor remediation recommendations to individual systems |
| Key Working Relationships | IT and senior business managers across all areas of QA.<br>3rd party software/service providers. |

| 3. ABOUT YOU | |
|---|---|
| Skills & Abilities | Excellent analytical, technical and communications skills<br>A positive, "can do" attitude and the drive and enthusiasm to |

| | |
|---|---|
| | persevere and deliver, both individually and as part of a team<br><br>Highly motivated with the ability to work autonomously to complete a range of tasks to time and quality with the minimum of supervision and as part of as a team<br><br>Ability to juggle priorities and balance long-term and short-term demands<br><br>Excellent oral and written communication skills with the confidence to interact with internal/external stakeholders at all levels, present complex analyses and influence decision makers |
| Your Experience & Knowledge | Experience of working in an information security, cyber security environment or Security Operations Centre<br><br>Strong technical background with excellent knowledge of cyber security, computer networks and operating systems including firewalls, IDS/IPS, Active Directory, endpoint protection, Windows Server, networks and cloud services<br><br>Comprehensive knowledge or experience of information security principles, including risk assessment, intrusion detection, Security Incident and Event Management (SIEM) tools, threat and vulnerability management<br><br>Detailed knowledge or experience of application or network based penetration testing tools and methodologies<br><br>Experience of incident response and/or security incident event management solutions, SOAR, UEBA<br><br>Analytical background with the ability to analyse and interpret large and complex data sets and articulate observations, conclusions and recommendations<br><br>Experience or knowledge of system integration using scripts to facilitate automation of commons tasks |
| Your Qualifications | No specific qualifications are required |
| What you'll bring to QA | Working as part of a team safeguarding QA IT infrastructure against cyber threats through the use of SIEM and analytical tools and application of threat, technical and business knowledge. |

| 4. ABOUT QA | |
|---|---|
| About us | We shape the next generation of technologists, leaders and innovators.<br>By powering potential – the potential of over a quarter of a million learners a year. We empower them to push boundaries and thrive in the workplace.<br>**Why we do learning**<br>For over 30 years, we've worked in technology – where the impact of great learning is changing the world.<br>A bold statement, but hear us out. We are right at the centre of a technological revolution. Devices are not just connecting people, cities and countries – they are connecting to each other, collecting data and using it to learn and make themselves better. Soon we will have cars that can drive themselves, fridges that make sure we never run out of milk and computers that can learn from their own mistakes.<br>Driving this revolution? People.<br>And this is where we come in.<br>People advancing their knowledge in technology – to enrich society – build a new culture – better how we live our lives, and how we work together.<br>People are learning to use technology to drive phenomenal change. This is our passion – powering their potential. |
| We promise to be | **Bold**<br>○ Ambition is great. We set ambitious targets – holding ourselves and others to ever-higher standards.<br>○ We contribute (insightfully) to the debate inside and outside QA.<br>○ We move. Quickly. We respond to your needs – fast.<br>**Collaborative**<br>○ We spend time getting to know you – our learners and our customers – to earn your trust.<br>○ We connect a solution to your problem – we have tonnes of different services to help you.<br>○ We're the positive person who actively gets stuck in to solving problems.<br>**Progressive**<br>○ We embrace change – and support it.<br>○ We challenge ourselves to use the latest technologies and methods – no matter how out there.<br>○ We're curious – about what you do, about what the person next to you does, about our customers and our learners. |

| | |
|---|---|
| What's on offer? | Learning is not just a service we provide, it's a way of life at QA, and we try to ensure that everyone has the opportunity to take advantage of our huge and varied range of learning and development options, so everyone is eligible for 3 **Training Days** every year, to focus on subjects they're interested in.<br><br>We also know that many people like to "give back" and so we offer 2 paid **Charity Days** each year to support your chosen charity in whatever way you choose. And if you get involved in charity fundraising, QA will also double any sponsorship money raised, up to £250. This is over and above the charitable activities that we encourage through our annual QA fundraising drives – you can get involved with this as much or as little as you like. We see it as a great way to foster team building too.<br><br>We all need to take time out to recharge our batteries from time to time and enjoy some down time, so we provide a fairly generous 25 days' holiday per annum (rising to 28 days after 5 years) – with the option to buy more if you wish.<br><br>It's important, too, to plan for the future and ensure we are able to maintain the lifestyle we have worked so hard to achieve, once we retire from the hurly burly and slow down to enjoy our later years, so we offer a defined contribution pension plan and will match your contributions up to a maximum of 4% of your basic salary.<br><br>Then there are two of our core benefit offerings, not the most exciting, but we consider it important to ensure everyone has the peace of mind provided by Life Assurance (4x your basic salary) and Permanent Health Insurance (after a qualifying period) in the event that ill health, or worse, disrupts our plans.<br><br>And finally, a few fringe benefits to assist with travel and lifestyle choices:<br><br>○ Season ticket loan<br>○ Corporate gym membership<br>○ Cycle to work scheme |