littlefish
managed IT services
www.littlefish.co.uk

Job Title	Cyber Security Analyst - Tier 3
Department	Cyber Security
Location	Nottingham, Sheffield
Reports to	Cyber Security Operations Centre Manager
Staff Responsibility	N/A
General Overview of position	Working within the Cyber Security Operations Centre to monitor customer infrastructure for potential threats. Undertaking timely investigation of and response to security alerts to identify security incidents and act to appropriately contain threats. Supporting, as required, the CSOC Manager in the day-to-day running of the Cyber Security Operations Centre (CSOC) operations team. Acting as an initial point of escalation for the Cyber Security Analysts the role has responsibility for coaching and mentoring the analysts on a day-to-day basis. Provide out of hours technical escalation support to shift analysts
Main duties & responsibilities	**To include:** • Developing SIEM detection rules and tuning alerts across our client estates. • Conduct proactive threat intelligence research and carry out threat hunting across client estates • Lead the training of analysts and developing training resources and materials • Act as a point of escalation for the Security Analysts • Ensuring appropriate detection and responses to security threats • Analysing security breaches to identify the root cause. • Compile and present CSOC monthly reporting and provide guidance around improving security posture • Provide technical support within client service reviews along with attending any other meetings at the CSOC Managers discretion • Articulation of security risk to customers in a language that can be understood by business representatives • Responsible for continual service improvement activities within the CSOC • Ensuring the integrity of client IT infrastructures • Protecting information systems residing upon them from external and internal attack/ compromise • Conducting privilege account reviews • Conducting security assessments through vulnerability testing and risk analysis

	• Maintaining high quality security incident resolution and performance within the CSOC

littlefish
managed IT services
www.littlefish.co.uk

Other duties	**ISO Accreditations:** Littlefish are ISO9001 and ISO27001 certified it is expected that all employees adhere to the Quality Management and Information Security systems, policies and procedures. **Equality, Diversity and Inclusion:** It is expected that you will actively promote and embed Equality, Diversity and Inclusion (EDI) Any other responsibilities at the line managers discretion

littlefish
managed IT services

www.littlefish.co.uk

Person Specification

Essential	Desirable
Experience • 2-4 years' experience in Security Operations or similar role • Experience in investigating and responding to cyber security threats within strict SLA's. • Experience with, SIEM, EDR and Email Security toolsets and how to leverage these tools to provide robust Detect & Respond services. • Experience working in a Microsoft XDR SOC • KQL (Kusto Query Language) experience • Experience in mentoring and assisting analysts of varying levels of skill. • Must have been a UK resident for a minimum of 5 years prior to application Education/Qualifications • Microsoft SC-200 Certification • CompTIA CySA+ or equivalent Skills / Knowledge • Sound technical understanding of security threats and compromise methods • Understanding of server, client and network technologies. • Understanding of security attack vectors and techniques utilised, including areas such as Business Email & user account Compromise, malicious payload installation &	Education/Qualifications • Either AZ-500, SC-300 or SC-100 certifications • SANS: GSOC, GCED, GCDA Experience • Previous experience working in a security operations environment • Experience in responding to cyber security threats • Experience in the use of anti-virus technologies • Experience in vulnerability assessments • Experience as an incident responder Skills / Knowledge • Vulnerability Awareness/Understanding • Delivery of the appropriate balance between business need, technical perfection and security standards. **Other job requirements** • Willing to undertake further training to fulfil the requirements of the role, with this training resulting in industry recognised certification for the individual and the potential to increase their salary through the completion of awards within our training academy

execution and reconnaissance activity. • Understanding of the everchanging emerging threat landscape and how to interpret these threats to create initiate mitigation actions across a client's security estate. • Willingness to learn, adapt, and innovate • Critical thinking and analytical skills • Excellent written and oral communications skills • Great interpersonal and teamwork skills Aptitudes and Attributes • Strong analytical skills, clear logical thinking and good judgement • Excellent communication skills both written and verbal • Service delivery mentality and experience. • Time management and expectation management. • Curiosity and tenacity. • Passion for Cyber Security. • Self-motivated proactive individual. • Ability to work under pressure with competing priorities. • Ability to work independently and prioritise own work to meet tight deadlines.	

littlefish
managed IT services
www.littlefish.co.uk

Document Control

File Name	Cyber Security Analyst - Tier 3
Author	Darren Murphy
Status	Live
Classification	Private
Location	HR Hub

Version Control

Version	Author	Change	Date
1.1	Darren Murphy	Amended role specification and qualifications	22nd January 2025

Job Levels

Career Framework	Technical
Definition	Technical subject matter expert working in a customer-facing capacity and able to support/implement typical technology requirements
Contribution to Success	Supports and facilitates others in the implementation of short term plans or works to achieve agreed goals. Performs a range of mainly straightforward assignments. Will manage cost on a day to day basis, looking for opportunities to generate efficiencies
Communication	To act as a technical escalation point for internal teams and customers. Provide input and guidance for technology roadmaps, projects and transitions
Expertise	Will follow well established work routines with skills gained through job related training and considerable work experience within specific department. May start to develop skills within a professional qualification
Leadership	Will receive guidance from their line manager and won't usually manage a team
Values Statement	Displays consistent and positive behaviours in line with the values. Acts with integrity and professionalism within own team and across the organisation

littlefish
managed IT services
www.littlefish.co.uk

HR@littlefish.co.uk

0344 848 4441

Littlefish UK, Price House, 37 Stoney Street, Nottingham NG1 1LS

@Littlefishuk Littlefish (UK) Ltd @Littlefishuk @Littlefish_UK