littlefish
managed IT services

www.littlefish.co.uk

Job Title	Cyber Security Analyst - Tier 2
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 as a tier 2 member of the team, to monitor customer infrastructure for potential threats and act as a escalation point for tier 1 analyst queries and customer requests. Undertaking timely investigation of, and response to, security alerts to identify verified security incidents and take action to appropriately contain and eradicate active threats to our clients infrastructure. As a Tier 2 Cyber Security Analyst you are a security professional, knowledgeable about information security alerting, incident response, threat trends, security event triage, intrusion analysis, malware, and anomalous behaviour. Working hours within the 24/7 SOC will consist of a shift pattern working 12-hour shifts on a 4 days on and 4 days off 4 nights on and 4 nights off rotation. 20% shift allowance payable when on the shift rotations.

Main duties & responsibilities	**To include:** • Monitoring of Security incidents via ITSM Platform • Conduct analysis using an array of security solutions, resulting in the investigation, triage and potential initial response actions to the security alerts produced. • In the event that a verified incident is identified, work with our incident responders to establish root cause of the incident and recommend/initiate corrective action • Act as escalation point for Tier 1 analysts, providing knowledge and mentoring experience to queries and issues that they may face • Ensuring the integrity of customer IT infrastructure and data through the use of layered security controls ranging from EDR and email security to conditional access policies and robust user authentication methods • Ensuring security assessments are carried out in areas such as privilege account , endpoint, email and cloud infrastructure security posture, with results documented and recommendations provided. • To be able to communicate with customers regarding security related incidents and translate technical information into an understandable format fit for a larger audience. • Carry out analysis of emerging threat landscapes utilising CTI based TTP's and knowledge articles to then advise on how such threats can best be mitigated using the security tooling at our disposal. • Assist in the creation and enhancement of alert 'playbooks', documenting the processes and procedures necessary to respond to threats based on client requirements.

littlefish
managed IT services
www.littlefish.co.uk

Main duties & responsibilities (continued)	• To enhance the SIEM platform to identify customer security incidents and provide remediation advice.
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 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 Skills / Knowledge Education/Qualifications • Microsoft SC-200 Certification • CompTIA Security+ 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 & execution and reconnaissance activity. • Understanding of the everchanging emerging threat landscape and how to interpret these threats to	Education/Qualifications • Either SC-300 or AZ-500 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

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 2
Author	Darren Murphy
Status	Live
Classification	Private
Location	HR Hub

Version Control

Version	Author	Change	Date
1.1	Darren Murphy	Update to working hours & desirable qualifications	13th January 2025

Job Levels

Career Framework	Front Line Teams
Definition	Brings fundamental knowledge in own area of specialism and works in a customer facing environment
Contribution to Success	Works autonomously to deliver their own output or service based on specific standard or guidelines within their set department
Communication	These roles ensure that our services are provided to our customers / internal stakeholders
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 direct supervision from their departmental line manager, usually a Team Manager or Manager
Values Statement	Demonstrates excellent behaviours in line with our values. Is encouraging and optimistic with colleagues and consistently strives to be a great team contributor

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