littlefish
managed IT services
www.littlefish.co.uk

Job Title	Cyber Security Engineer
Department	Cyber Security
Location	Hybrid
Reports to	Cyber Services Director
Staff Responsibility	Mentoring / Coaching
General Overview of Position	Working within the Cyber Services Division this is role is dual focused. Firstly, a responsibility for the tooling within the Security Operations Centre (SOC), primarily the technical ownership, the implementation and ongoing maintenance of the SIEM platform; and secondly the delivery of Cyber Security engineering services and thought leadership for customers, through either a recurring advice and guidance capacity or the delivery of Cyber-led project engagements in either a standalone capacity or as part of a wider Professional Services-led engagement. More generally, the role would contribute to the definition of the future security tooling roadmap with the Cyber Services division as a whole and stay abreast of security controls and security-related technologies to become a thought leader in this space, providing advice and guidance for the wider-business and delivery teams.

littlefish
managed IT services
www.littlefish.co.uk

Main duties & responsibilities	• Technical ownership of the Security Operations Centre (SOC) tooling, most notably the SIEM platform but including other supporting tooling as required. • Responsible for the implementation of the SIEM platform in customer environments including the initial tuning of data feeds (from both a SIEM and source device perspective), and early life support of the implementation. • Required to work closely with the SOC post-implementation, to support and maintain the SIEM platform on behalf of the SOC, contributing to the ongoing development and maintenance of use cases and rulesets as required. • Provide chargeable technical Cyber thought leadership, advice and guidance for selected customers, including the technical implementation of product features when required. • Provide technical support and guidance in response to major security incidents across the customer landscape as and when required. • Undertake the chargeable delivery of Cyber-led project engagements, either on a standalone basis or contributing to broader Professional Services-led engagements. • Stay abreast of security controls and security-related technologies to become a thought leader in this space and provide advice and guidance for the wider-business and delivery teams. • Contribute to the definition of the future security tooling roadmap within the Cyber Services division as a whole.

Main duties & responsibilities (continued)	**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) in all your work and support and comply with all organisational initiatives, policies and procedures on EDI.

littlefish
managed IT services

www.littlefish.co.uk

Other duties	Other such reasonable duties within the general scope of the job role, at the line managers direction.

littlefish
managed IT services
www.littlefish.co.uk

Person Specification

Essential	Desirable
• Understanding of SIEM tools and concepts. • Technical experience of O365, M365 and Azure administration, with a particular focus on security controls and capabilities. • Experience in creating and maintaining scripts in PowerShell. • Understanding of the tactics, techniques and procedures (TTP) used by attackers. • Understanding and experience of implementing and managing security controls on network access control systems such as Firewall, IDS, WAF and network segmentation technology. • Understanding and experience of technologies and concepts including Windows, Networking, Identity and Access Management, Event Logging and Monitoring, Anti-virus and Zero-Touch Architecture. • Demonstrable communication skills with the ability to articulate technical security concepts, controls and technologies to both business and IT representatives in a customer facing capacity. • Ability to translate policy and regulatory requirements into sensible technical solutions. • Ability to write security focused architecture design documents and diagrams.	• Understanding and experience of Azure Sentinel and/or AlienVault USM Anywhere. • Understand the cloud service concepts and control capabilities on either Amazon Web Services (AWS), Google Cloud Platform (GCP). • Understanding and experience of technologies and concepts including Linux and Data Storage. • Experience in using scripting languages such as Python and Bash.

littlefish
managed IT services
www.littlefish.co.uk

Document Control

File Name	Cyber Security Engineer
Author	Richard Roome
Status	Live
Classification	Private
Location	HR Hub

Version Control

Version	Author	Change	Date
1.0	Keith Price	Template Change	February 2021
2.0	Richard Roome	Refinement	August 2021

Job Level

Career Framework	**Experienced Technical**
Definition	Industry/technology-experienced technical subject matter expert working in a senior capacity whether customer-facing or helping to develop professional colleagues. Able to assimilate complex/non-standard technology requirements and fulfil senior stakeholder engagement
Contribution to Success	Implements operational plans that contribute to the results of their department. Typically focused on timescales of 3-6 months. Will manage costs and will look for efficiencies with their area of responsibility
Communication	Influences others to make favourable decisions, mostly within their function but sometimes without
Expertise	Are the subject matter expert within their technical specialism and will have a basic knowledge of how their specialism impacts / links with other departments. Act as a senior escalation for their own team and across teams. Will usually have a professional qualification
Leadership	Will usually operate in a standalone position but acts as a key influencer across customers, contracts and / or projects. May manage a small team
Values Statement	Leads by example in displaying positive behaviours and instilling high performance within their teams, across the organisation and with customers

littlefish
managed IT services

www.littlefish.co.uk

0344 848 4441 HR@littlefish.co.uk

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

Littlefish (UK) Ltd @Littlefishuk @Littlefish_UK