FORCES CYBER PATHWAYS
TRANSFORMING CYBER SECURITY

SENIOR CYBER SECURITY SPECIALIST

FULL TIME – MANCHESTER

Forces Cyber Pathways Ltd (FCP)

FORCES CYBER PATHWAYS
TRANSFORMING CYBER SECURITY

SENIOR CYBER SECURITY SPECIALIST

SALARY: Competitive

ROLE OVERVIEW

The Senior Cyber Security Specialist role is part of the Cyber Security Operations Centre (CSOC) and sits within the Cyber Services Department.

The candidate will be the technical lead within the Cyber Security Operations Centre (CSOC) for all SIEM and security platforms by managing and improving each to meet the requirements of the business. You are expected to think beyond a conventional SIEM approach and seek to enhance the security suite to a comprehensive automation and orchestration capability.

This is a hands-on technical role and requires a high level of technical ability and understanding across a variety of security systems, particularly within Microsoft. Although the focus is on Cyber Security, a broad knowledge and/or experience of modern IT systems and infrastructure is necessary to assist with the development and continuous improvement of the security platforms within customers' environments.

KEY CAPABILITIES

- You will be the technical lead / SME for the CSOC and SIEM service offering by managing and improving the platforms to meet the requirements of the business and/or client.
- Configure and develop SIEM tooling, and associated tool sets, to deliver effective and efficient SOC services through automation and orchestration, and to increase MTTD whilst reducing false positives and negatives.
- Ensure all security platforms are optimised to detect and prevent security threats across all on-prem and cloud environments to meet business objectives and regulatory requirements
- Provide technical oversight and support for the identification, triage and response to events or incidents of a suspicious or malicious nature, and apparent security breaches.
- You will work collaboratively with architects, infrastructure teams and key stakeholders inside and out of the business ensuring security and monitoring requirements are determined and implemented through onboarding or continuous improvement activities
- Actively support the onboarding of new clients throughout the transition to service delivery lifecycle.
- Conduct project activities including planning and execution of Changes, documentation, training / skills / knowledge transfer to the team and clients.
- Maintain a continuous understanding of the threat landscape with in-depth knowledge around threat actors, TTPs and vulnerabilities
- Be a technical mentor to the CSOC Specialists and Analysts, providing technical knowledge and training to the team.

Essential Skills

- Excellent soft-skills in the form of team working, problem solving and communication.
- You are a self-starter, keen to develop new services and can collaborate effectively.
- Technical experience in a Security Operations Centre, Incident Response Team or similar environment.
- Experience with a variety of SIEM platforms and monitoring tools, configuration management tools, host virtualisation, containerisation, vulnerability scanners, proxies, WAFs.
- An in-depth knowledge of log formats, log transports and log analysis as well as automating log ingestion and normalisation in a SOC environment.
- The ability to perform analysis of log files from a variety of sources (e.g. individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
- Strong technical skills with experience in intrusion analysis and investigation using a variety of security tools (SIEM, EDR, DLP, AV, Snort, Wireshark, TCPdump etc.).
- A thorough understanding of internet communications protocols and in-depth packet analysis, including knowledge of how these protocols are commonly secured.
- Strong awareness of cyber attack techniques and how protective monitoring systems can be used for detection, mitigation, remediation and protection.
- Awareness of risk management and the ability to contextualise technical issues into business risk relevant to the business and clients.
- One or more of the following industry certifications: CEH, GCIA, GCIH, GSEC, Security+, GCTI

Desired Skills

- Having achieved at least a BSc or MSc in Cyber Security incorporating Ethical Hacking, Digital Forensics or Information Security; or
- One of more of the following industry certifications: GCFE, GCFA, GNFA, GREM
- Formal experience in Digital Forensics or experience using EnCase, FTK Imager or similar
- Experience using Volatility (or equivalent) for memory analysis.
- Experience with static malware analysis
- Experience in secured cloud architectures (Azure, AWS) and engineering solutions
- An ability to undertake coding tasks using various languages (Assembler, C, C++. Java, Javascript, Perl, Python) and evidence of having done so either professionally or as a hobby or extra-curricular interest.
- An understanding of multiple operating systems and their programming interfaces such as UNIX Shell and PowerShell.
- An awareness of cyber security related standards and regulations, for example, NIST, CIS, ISO 27001 and PCI DSS

WHY WORK WITH FCP AND OUR PARTNERS

Forces Cyber Pathways Ltd (FCP) looks for candidates that wish to be supported throughout their careers after leaving the military. We standby the personnel we work with, continuing to develop them and place them into new roles as their careers progress.

We work with some of the largest companies in the UK (and Europe) and have forged solid partnership for the long term, offering different type of support, which translates into a diverse job range available with FCP.

We are the partners that our clients and candidates can rely on. We're looking forward to hearing from you.

info@focespathways.com

Tel: +44 (0) 207 971 1175

www.ForcesPathways.com