Senior Cyber Technical Security Consultant

Introduction

Net Consulting seek an experienced, technical hands-on Cyber Security Consultant to join a growing Cyber team delivering a range of services including the following:

- Penetration testing (external, internal, web app, etc) experience is essential.
- Advanced Vulnerability Assessments
- Live threat analysis and forensic investigation
- Cloud and end-point protection
- Next Generation Firewall configuration

The successful candidate will be a self-starter, able to support a project from pre-sales through to completion & reporting. The role can be worked remotely depending on location, with UK travel required to attend customer and supplier meetings.

Key Accountabilities:

- Providing Cyber Security services to external customers, involving:
- Offering accurate, independent & up to date consultancy & advice relating to the Cyber Security field
- Proficient use of required tooling (hardware & software)
- Technical delivery of solutions
- Technical quality assurance
- Undertaking Cyber Security deployments and / or projects, and seeing them through to completion within agreed timescales
- Providing technical authority for the Cyber team
- Maintaining high standards of personal professionalism and integrity
- Adhering to all Net Consulting and relevant customer policies, processes and procedures
- Proactive identification and communication of risks and issues affecting service or project delivery and supporting continuous service improvement
- Identifying opportunities for personal and professional growth, working with Line Manager to develop a Personal Development Plan
- Keeping Net Consulting managed service Cyber tooling functional and up to date

Responsibilities and Duties

- Attend pre-sales meetings with customers to provide technical expertise and support requirements gathering.
- Provide subject matter expertise in the field of Cyber Security for:
    - Pre-sales and cyber security consultancy at customer meetings
    - Technical consultancy in relation to the specific tools used to deliver Cyber Services.
    - Input into Bids, Proposals and Business Development
    - Industry awareness & best practices
    - Provide technical input to development of Cyber Security services
    - Service innovation and Continuous Service Improvement (CSI)
    - Input into Marketing literature

- Assist with the provision of technical recommendations and resource estimates to support the production of commercial proposals for the delivery of Cyber Security services to customers
- Mentor junior Cyber team members

- Monitor trustworthy data sources on an ongoing basis to identify trends and hot topics in the Cyber Security industry, providing internal briefings to inform business strategy and marketing campaigns
- Identify technologies and methodologies which could contribute to NCL's Cyber Security offering, proposing R&D projects to line management for consideration.
- Assist with development of approved R&D projects to develop NCL's portfolio of Cyber Security expertise
- Contribute to the continuous improvement of NCL's Cyber Security services, including identifying and implementing efficiency and quality improvements.
- Maintain relevant Cyber credentials/ certifications
- Carry out peer reviews of other Cyber Team member reports
- Contribute to the resource allocation process by providing up to date skillset information
- Provide input into the ongoing ISO27001 Information Security auditing
- Provide input into the information security management system (ISMS)
- Implement processes in accordance with ISO27001
- Maintain a weekly record of time spent against each project or cost code
- Provide subject matter expertise in the field of Cyber Security for:
    - Pre-sales and cyber security consultancy at customer meetings
    - Technical consultancy in relation to the specific tools used to deliver Cyber Services
    - Input into Bids, Proposals and Business Development
    - Industry awareness & best practices
    - Provide technical input to development of Cyber Security services
    - Service innovation and Continuous Service Improvement (CSI)
    - Input into Marketing literature

Person Specification

- Strong academic record, to degree level or equivalent industry experience
- CHECK or CISSP or CREST certification
- Strong attention to detail
- Maintaining high standards of personal professionalism and integrity
- Customer focused attitude
- Self-starter able to research and experiment to find a solution unaided
- Good written and verbal skills
- Strong technical skills in several of the following technology areas:
- Cyber threat analysis tools (e.g. RedSeal)
- Strong understanding of broad Cyber Security principles
- Basic appreciation of Enterprise architectures (e.g. servers / networks / firewalls)
- SIEM management tooling (e.g. Splunk / LogRhythm)
- End-Point Protection (e.g. Sophos / Palo Alto TRAPS)
- Border protection technologies (e.g. Cisco ASA / Palo Alto)
- Penetration testing techniques
- Web Application penetration testing tools (e.g. NetSpark/ Metasploit)
- Vulnerability scanning tools (e.g. Qualys / Nessus)
- Intrusion detection tools (e.g. Perception / DarkTrace)

Company Benefits

- Annual performance bonus & Company Performance Bonus
- 25 days holiday per annum (pro rata, excluding Bank Holidays)
- Benefit options (Contributory pension scheme, Private Medical Insurance, Life Assurance, Health & Wellbeing)
- Critical Illness Cover
- Brilliant opportunities to take on more responsibility and long-term career prospects