Job Description

Senior Cyber Security Consultant

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
- Penetration tests
- Next Generation Firewall configuration

The successful candidate will be a self-starter, able to support a project from pre-sales through to completion & reporting.

Short description of role
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 NCL's ISO27001 accreditation
- Maintaining high standards of personal professionalism and integrity
- Adhering to all Net Consulting and relevant customer policies, processes and procedures
- Maintaining knowledge of and applying industry best practise and standards
- Ensuring that security standards are always maintained
- Proactive identification and communication of risks and issues affecting service or project delivery and supporting continuous service improvement
- Maintaining existing relevant accreditations and certifications
- 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

- Cyber security consultancy at customer meetings
- Technical consultancy in relation to the specific tools used to deliver Cyber Services
- Subject matter & technical input into Bids & Proposals

Business Development

- Industry awareness & best practices
- Service innovation
- Continuous Service Improvement (CSI)

- Subject matter & technical 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
- Provide input into the technical descriptions of Cyber Security services for the purposes of marketing and framework applications
- Maintain relevant Cyber credentials
- Carry out penetration tests (web application and infrastructure) and Cyber Security risk assessments
- Carry out peer reviews of other Cyber Team member reports
- Contribute to the resource allocation process by providing up to date skillset information
- Support recruitment of technical roles by assisting with technical testing of interview candidates
- Provide input into the ongoing ISO27001 Information Security auditing
- Provide input into the information security management system (ISMS)
- Carry out ISO27001 internal audits
- Implement processes in accordance with ISO27001

Maintain a weekly record of time spent against each project or cost code

Person specification

- Strong academic record, to degree level or equivalent industry experience
- CHECK or CREST certification
- Strong attention to detail
- 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:
    a. Cyber threat analysis tools

b. Strong understanding of broad Cyber Security principles
c. Basic appreciation of Enterprise architectures (e.g. servers / networks / firewalls)
d. SIEM management tooling
e. End-Point Protection
f. Border protection technologies
g. Penetration testing techniques
h. Web Application penetration testing tools
i. Vulnerability scanning tools
j. Intrusion detection tools
k. Web Application penetration testing tools
l. Vulnerability scanning tools
m. Intrusion detection tools

Working environment

The role is primarily based in the Cardiff head-office, with occasional UK travel required to attend customer and supplier meetings.