Senior Technical Cyber Security Consultant

Introduction

Do you like meeting new organisations and discussing their concerns relating to cyber security? Can you define and implement solutions for clients to improve the security of their digital assets?

We're looking for people with good hands-on technical skills to join the team to provide consultancy advice and develop and implement cyber security solutions to address current and emerging concerns of our clients. You'll be part of a
team informing, defining and building solutions both for our clients and our managed security services group, leveraging a state of the art security platform.

You'll be expected to have a good understanding of UK cyber security practices and frameworks and stay up to date with the latest industry standards as well as best practice security guidance.

Responsibilities

- Deliver advice and guidance to internal or external customers on how to identify and minimise the impact of potential threats to assets and services.
- Liaise with potential or current partners and suppliers to evaluate the cyber security posture of their organisation or services.
- Contribute to the continuous improvement of NCL's Cyber Security services, including identifying and implementing efficiency and quality improvements.
- Undertake solution deployments and/or consulting projects and see them through to completion.
- Provide knowledge and expertise in responding to and remediating cyber security incidents.
- Help develop and maintain company IS27001 and Cyber Essentials certifications and associated policies and controls.
- Ensure controls implemented in solutions are operating as designed to mitigate identified risks
- Develop reports on the effectiveness of controls to internal and external stakeholders.
- Maintain awareness of current and possible future trends in information security landscape and the impact on the policies and standards in industry.
- Mentor and supervise junior staff to improve their cyber security awareness.

Skills & Experience

- Degree preferred or equivalent industry experience.
- 5+ years of experience in information/cyber security or related technology areas.
- CREST Registered Technical Security Architect or similar highly desirable.

- Certified Information Systems Security Professional (CISSP) or similar highly desirable.
- CREST Registered Penetration Tester or similar highly desirable.
- It would be great if you've strong skills in some of the following technical areas:
    - Cyber threat analysis tools.
    - Understanding of broad Cyber Security principles.
    - Appreciation of Enterprise architectures (e.g. servers/networks/storage/backup/apps/databases).
    - Security technologies (firewalls/proxies/IDPS/DLP/UTM).
    - SIEM and SOAR technologies.
    - End-Point Protection and Response tools.
    - Border protection technologies.
    - Vulnerability scanning/Penetration testing/Web Application penetration testing.
    - Firewalls and intrusion detection/prevention tools.
- Experience with industry compliance and one or more information security management frameworks is useful (e.g. IS027000, Cyber Essentials, COBIT, NIST 800, etc.).

Company Benefits & Perks

- Competitive Salary
- Workplace Benefits: Contributory Pension Scheme, Private Medical Insurance, Life Assurance, Critical Illness Cover, Health & Wellbeing
- 25 Days' Annual Leave (in addition to Bank Holidays)
- Performance Bonuses (Personal & Company)
- Excellent Career Progression Opportunities