NCL

Senior Analyst – Cyber Security

Introduction

We're looking for experienced cyber security people who are customer focused, love technology and like solving problems to join our team.

Working from our Digital Operations Centre near Cardiff, you'll be part of our team helping to deliver managed security services to our clients, leveraging state of the art security platforms and processes; Carrying out a broad range of activities from proactive cyber detection and response services, to infrastructure, end user experience and application performance and availability management.

This is an exciting time where you can be part of an energetic growing business and help build our dream, while learning and further developing your skills in cyber security and associated data networks and information technology.

Responsibilities

- Monitor the security, performance and availability of client networks and enacting associated detection and response activity.
- Perform initial triage/identification of 'Events of Interest' from our toolsets.
- Identify suspicious and / or anomalous activities and taking appropriate action based on documented processes and procedures.
- Ensure that events of interest, exceptions and incidents are responded to in accordance with established work processes, including remedial action/recommendations.
- Provide event and log analysis to support our operational services.
- Provide situational security awareness to Clients by combining information from a variety of systems and normalizing / correlating the information.
- Produce reports (as per templates) & trending analysis as required.
- Contribute to the continuous improvement of NCL's Cyber Security services, including identifying and implementing efficiency and quality improvements.
- Help develop and maintain company IS27001 and Cyber Essentials certifications and associated policies, controls and operational processes.
- Assist in the continual development of cyber security Use Cases and Incident Playbooks and training and development content to enable quick upskilling of new starters to the team.
- Potential for staff supervision.

Skills & Experience

- Degree preferred or equivalent industry experience.

- 3+ years of experience in information/cyber security or related technology areas.
- Experience of supervising technical personnel is useful but not essential.
- Good cyber security knowledge, with a focus on one or more of the following operational security areas; Security monitoring and alerting, detection and response, vulnerability management or incident response.
- Hands on experience with security tooling such as SIEM and EDR solutions (monitoring, Use Case development and content creation, upgrades and troubleshooting).
- Knowledge, understanding and application of cyber-attack frameworks e.g. Cyber Kill Chain, MITRE ATT&CK.
- Some understanding and practical application of cyber security standards and frameworks would be useful e.g. ISO27001, NIST, CIS, OWASP, SANS.
- Knowledge in one or more of the following is desirable:
    - Digital Investigations
    - Threat Intelligence
    - Malware Engineering
    - Incident Response/Incident Management
    - Security Orchestration and Automated Response (SOAR)
- Proficient in RegEx, SQL/KQL and should be able to demonstrate use cases.
- Knowledgeable in the use of one or more of RegEx, LUA, Python and PowerShell is desirable.
- Professional training in IT, networking and/or cyber security is highly desirable.
- Qualifications such as CISSP, CEH, OSCP or from GIAC, CREST, CompTIA or equivalent are desirable.
- Most important is the desire to learn and develop your skills while helping our customers be secure, performant and resilient, we can provide the training and education.

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