# Principal Analyst – Cyber Security

## Introduction

Do you enjoy the challenge of keeping up with the pace of technology, the ever-evolving tactics, techniques, and procedures from our adversaries, or the plethora of tools being developed to combat threats?

Net Consulting is looking for an exceptional hands-on person to join our cyber operations team in a key role to help define, direct and guide the team in the delivery of managed security services to our clients, leveraging state of the art security platforms and associated processes, training and education.

This is an exciting time where you can help build the team and shape the capabilities.

## Responsibilities

Lead a team of cyber security analysts, having overall responsibility for all analysis, detection and response activity performed by the team.

Provide knowledge and expertise is responding to and managing security incidents.

Identify suspicious and / or anomalous activities and taking appropriate action based on documented processes and procedures.

Provide situational security awareness to Clients by combining information from a variety of systems and normalizing / correlating the information.

Perform analysis of log files and security audit data.

Provide on the job mentoring, guidance and advice to cyber analysts and where necessary taking on the handling of incidents to ensure the best possible service is provided to the Customer.

Troubleshooting detection and response system issues.

Develop and maintain security Use Cases and Incident Playbooks and training and development content to enable quick upskilling of new starters to the team.

Help develop and maintain associated policies, controls and operational processes.

Continuously seeking to identify potential service / tool improvements which will enhance the delivered services.

Mentor and supervise staff to improve their cyber security awareness.

## Skills and Experience

Degree preferred or equivalent industry experience.

6+ years of experience in information/cyber security or related technology areas.

Experience of managing and/or supervising technical personnel.

Strong cyber security knowledge, with a focus on operational security such as security monitoring and alerting, vulnerability management and incident response including associated policies and processes.

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 cyberattack frameworks e.g. Cyber Kill Chain, MITRE ATT&CK matrix.

Understanding and practical application of cyber security standards and frameworks e.g. ISO27001, NIST, CIS, OWASP, SANS.

General well-rounded knowledge of IT, network and application security and architecture and business continuity management.

Specialist knowledge in one or more of the following is highly desirable:

- Digital Investigations
- Threat Intelligence
- Malware Engineering
- Major Incident Management
- Security Orchestration and Automated Response (SOAR)

Knowledgeable in use of one or more of RegEx, LUA, Python and PowerShell highly desirable.

Professional training in Incident Management would be good to have.

Professional training in Cyber Security Analysis and/or Threat Intelligence also good to have.

Qualifications such as CISSP, CEH, OSCP or from GIAC, CREST or equivalent are desirable.

## 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.

On-call/call-out allowance, where applicable.

Brilliant opportunities to take on more responsibility and long-term career prospects.

The health and safety of our employees and clients is a top priority for Net Consulting. We are adhering to government guidelines to COVID-19 and have implemented policies and processes to prevent the spread within our offices. During the current changing COVID threat levels and ensuing government guidelines, employees are either working remotely on a full-time basis, or attending the office on a rota system.

All interviews are currently being conducted remotely, with client visits also restricted to essential work and upon request.