

<b>Job Title</b>	<b>Cyber Security Analyst 2nd/3rd line</b>
<b>Reports to</b>	<b>Service Operations Manager</b>
<b>Location</b>	<b>Cardiff, CF15 7NE</b>
<b>Package</b>	<b>Highly Competitive with Company benefits</b>

## About Net Consulting

Net Consulting is a leading IT consultancy specialising in Performance Management, Cyber Security and Managed Services. We have built a solid track record of delivering benefit driven capabilities across a diverse range of sectors.

## About the Role of Cyber Security Analyst

Intermediate and experienced Cyber Analysts are required to join a new and dynamic Service Operations team in our purpose-built Service Operations Centre (SOC). This exciting new team carries out a broad range of activities ranging from proactively monitoring customer estates using Security Incident Event Management (SIEM) tools, Infrastructure and Application performance and availability monitoring, as well as actively threat hunting for Cyber Security issues on customer networks utilising state of the art tools.

The Analyst needs to have previous experience of SIEM tool operation, be proactive and possess good analytical skills. They should be able to take events of interest and perform complex analysis, recommending and performing remediation steps when appropriate.

The candidate should have a broad knowledge of the Cyber Security field and maintain up to date knowledge. The candidate should also be keen to document any such knowledge or Incident learnings in the ITSM tool Knowledge Base.

The Analyst should be a self-starter, able to research & investigate the routes to a solution with minimal direction. The role will involve an element of mentoring junior members to build up the overall skillset of the team.

## Roles & Responsibilities

- Have a solid grounding in using SIEM tools to provide an excellent Managed Service solution to a range of customers
- Be able to log and perform initial triage of any events and alerts highlighted. Utilising the SIEM tools and any other tooling available to the Net Consulting Service Operations Centre
- The ability to follow up on any such events by performing a complex and detailed analysis, which may result in the Analyst offering remediation advice to the customer to rectify the situation. This may also extend to the Analyst carrying out the remediation in line with all existing Net Consulting processes and Knowledge articles
- Ensure that any Incidents are updated in a detailed manner, outlining investigative actions performed and any resolution or remediation efforts. Ensuring all levels of the Service Operations team are kept up to date on the progress of the Incident, whilst providing the level of detail required for any subsequent Incident Report.
- Have excellent ticket management and prioritisation skills to ensure that all Incidents and Requests are actioned in a timely manner, making all efforts to preserve relevant SLA's and OLA's
- Ensure that after the resolution of each Incident, appropriate Knowledge Base articles are created in the ITSM tool
- An understanding of Incident, Change and Problem management activities

- Be extremely customer focused
- Have excellent written and verbal communications skills
- Be willing to assist and mentor junior members of the team
- Actively seek ways of improving all processes as part of a Continual Service Improvement initiative

### Qualifications

- 2+ years Cyber security experience
- Experience in working for several Enterprise clients
- A degree in an IT-related subject (desirable)
- Networking experience and good understanding of TCP/IP
  
- Experience of multiple Operating Systems, UNIX/Linux/Windows (desirable)
- Professional certifications in Information Security (CRISC, CISSP, CISA) (desirable but not essential)
- Experience in threat hunting, such as log analysis (highly desirable)
- ITIL foundation (highly desirable)