SOC and Vulnerability Analyst

Logiq Consulting is a fantastic place to work. Our ethos is based on our core values of innovation, collaboration, and quality delivery which has created a genuine "Yes" culture. Being a fast growing SME working alongside some of most prestigious clients in the UK we can offer not only a varied and interesting workload, but we can nurture your inquisitive nature and help you create change in the workplace - making it better for all.

Logiq Consulting are Cyber Security and Information Assurance experts. We specialise in providing leading edge consultancy to high-threat clients, as well as delivering a range of security services and products throughout the Private and

The Role:

An increase in clients across our Managed Services, along with the maturing of our service offering as driven the requirement for this new role, SOC and Vulnerability Analyst. The role will be reporting to our Information Security Lead and sit within our Information Security Team. The ideal candidate will have current or recent experience working in a SOC environment and/or have a strong focus on vulnerability management.

Key Responsibilities:

As SOC and Vulnerability Analyst you will work within a close-knit team and be responsible for:

- Monitoring the company IT infrastructure. Monitoring Logiq IT security systems, applications and networks for irregularities and alerts which may indicate incidents, breaches and events.
- Investigation of alerts and incidents to ascertain the criticality and prioritisation of security incidents and vulnerabilities. Collaborate with other team members to further investigate incidents and propose responses and solutions.
- Report any new knowledge gained about existing cyber threats or vulnerabilities within their network so that future incidents can be prevented.
- Promote and evolve the company Security Operations Centre (SOC), make recommendations for playbooks, processes and procedures, and assist in further integrating monitoring capabilities to enhance our SOC function.
- Utilise threat intelligence feeds and software vulnerability management tools to identify and respond to emerging threats and vulnerabilities in company IT systems.
- Review configuration dashboards, identifying deployment issues and misconfigurations that may lead to vulnerabilities to Logiq platforms.
- Collaborate with other InfoSec team members to ensure that the company has the correct procedures in place to continue to operate safely and securely.
- Conduct the daily and weekly checks to identify vulnerabilities, providing reports and returns to ensure any issues are remediated with Systems Engineers.
- Provide recommendations on identified risks regarding further potential treatment/ mitigation options.

Essential Skills:

Experience in operating SIEM tools and vulnerability management software and being able to interpret and prioritise alerts, incidents and threat intelligence.

Desirable Skills:

To support the requirements of this role an awareness of national and international standards including the ISO27000 family, along with familiarity with recent NCSC guidance would be helpful.

Familiar with the following tools:

- Microsoft Sentinel
- Qualys VMDR
- Tenable VM
- MITRE ATT&CK Framework

Desirable Certifications, Qualifications Experience:

- Computer Security
- Security Blue Team 1 or higher
- CompTIA Cyber Security Analyst
- SC-200 Microsoft Security Operations Analyst

Company benefits include:

- Hybrid working from your choice of Chippenham and / or Bristol 1 or 2 days a week, home based otherwise
- Discretionary 10% bonus
- Discretionary 2k annual training fund per employee
- Very competitive pension scheme
- Virtual GP
- Annual Eye Test