Principal Security Operations Centre Analyst

Background

As part of the Becrypt Managed Services strategy, we are looking to recruit a Principal SOC Analyst to work in our new Security Operations Centre.

This is a chance for an individual to be in 'at the ground up' at the start of the development of the SOC and will play a leading role in the day to day activity of the SOC, as well as leadership of the team and influence of the SOC on an operational, technical and strategic level.

Location

This role will be based in the Becrypt Head Office in Victoria, London.

Key Responsibilities:

First and foremost you will lead the SOC team on a day to day basis managing the security improvements process to the best of your ability, along with incident management and implementation of security standards.

On top of this, you will work with the team to provide our clients with the best possible service around.

Other Responsibilities:

- Point of escalation on an on-call rota basis with the potential of a future 24/7 operations rota
- Training and supervision of analysts
- Managing threat intelligence and actor profiling
- Assisting in the generation of new signatures / rules
- Assisting in the definition of analysis procedures and protocols
- Responsible for the completeness and timeliness of all security incident related reporting against contract constraints and SLAs
- Building and developing capability across the teams, with particular focus on succession planning, and manage & capability to cover absence or operational delivery
- Seek and create opportunities to understand, contribute and support strategic SOC related initiatives
- Act as front door for incoming requests into the SOC
- Oversee and oversight monthly reports before being released to clients
- Coordinate or participate in individual or team projects
- Manage all documentation from support design, implementation and maintenance, Sopra Steria Risk & Security policies, procedures and standards in line with the customer's and the business requirements
- Manage and oversea any management meetings with senior managers
- Attendance of internal SOC weekly briefing

Essential Skills:

- Previous leadership experience is essential
- Full understanding of SIEM systems – IBM QRadar, Log Rhythm, Alien Vault etc
- IT Security Management, Policies, Procedures, Standards and Guidelines
- Risk Assessment
- Privacy and Compliance
- Conversant with security best practices (including ISO27001) and relevant security legislation
- Security Operations and Incident Handling

- IT Security Architecture
- Preferably with Security certification (e.g. CISSP, GIAH, GIAC)

Security clearance:

You must at least hold SC Clearance for this role or be willing to go through SC Clearance