Role Title	**SOC Lead Analyst**				
Job Family	**Security**	**Sub Category**	**Cyber Security**	**Grade**	**TPB5**
Behaviours	• Seeing the Big Picture • Making Effective Decisions • Communicating and Influencing • Leadership Charter				
Purpose	Identify and investigate security threat, incidents, anomalies or unexpected activities within the IT system of FCDO Services and its customers; provide and interface between FCDO IT and Security Service Desk teams to resolve security incidents.				

FCDO Services

Key Accountabilities

- Monitor, triage and investigate Security Alerts on the protective monitoring platforms to identify Security Incidents
- Understand and interpret a variety of system logs and reports for potential intrusions, security threats or breaches of policy; write Security Incident reports and report to senior stakeholders and customers
- Lead team on approaches used to investigate incidents and decide required response; implement and/or oversee implementation of resolutions
- Analyse Security Event Data / Security Alerts to support Customers in their response to Security Incidents
- In rotation with other Lead Analysts, represent the CSOC at meetings, provide advice to other areas of the business on new services and assess impact of proposed work
- Maintain current knowledge of IT based threats and vulnerabilities in order to identify and report real time attacks and vulnerabilities on the FCDO Services network
- Mentor, train and manage task delivery of Practitioner Analyst ensuring terms of the Service Level Agreement (SLA) are met

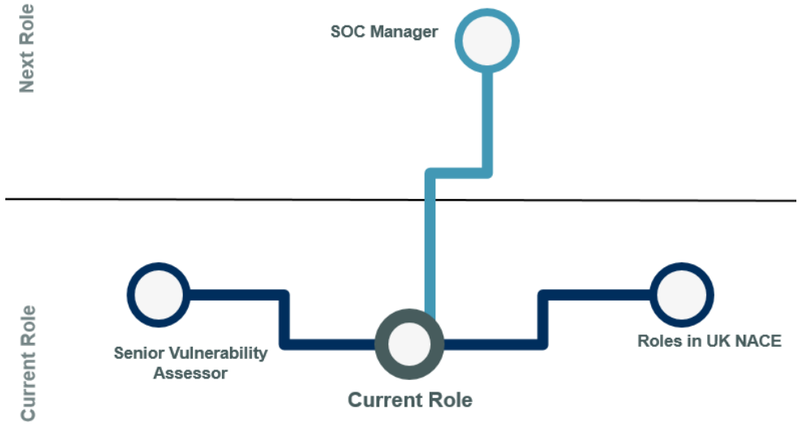
Authority and Scope

- Delivery of monitoring to Customers within agreed processes
- Security Incidents analysed and resolved according to procedures; major incidents escalated to Security Incident Management team
- Composite KPI compliance for internal and external customers
- Manage task delivery of Practitioner Analyst ensuring SLA terms are met

Internal and External Communications

- Operation leads and operation team members to analyse and coordinate incident responses, work collaboratively to remediate incidents
- Wider security team to analyse issues, and understand how different types of attack might manifest in the network
- Service Delivery Managers to report issues related to their Customers

Potential Next Career Moves



Skills

- Governance
- Analyse, interrogate and evaluate data
- Intrusion detection and analysis
- Cyber security operations
- Incident management, investigation and response
- Secure operations management
- Threat intelligence and threat assessment
- Threat understanding
- Bridge technical and non-technical

Qualifications, Knowledge and Experience

Essential

- Formal Cyber Security qualification
- BTEC, NVQ level or equivalent in IT, Cyber Security or related subject
- Advanced IT skills and experience in IT Security
- Strong interpersonal skills to work effectively in a team
- Able to manipulate and interpret data using a variety of tools

Desirable

- Membership of relevant professional body
- Deep knowledge of Networks, specifically Firewalls and other security devices