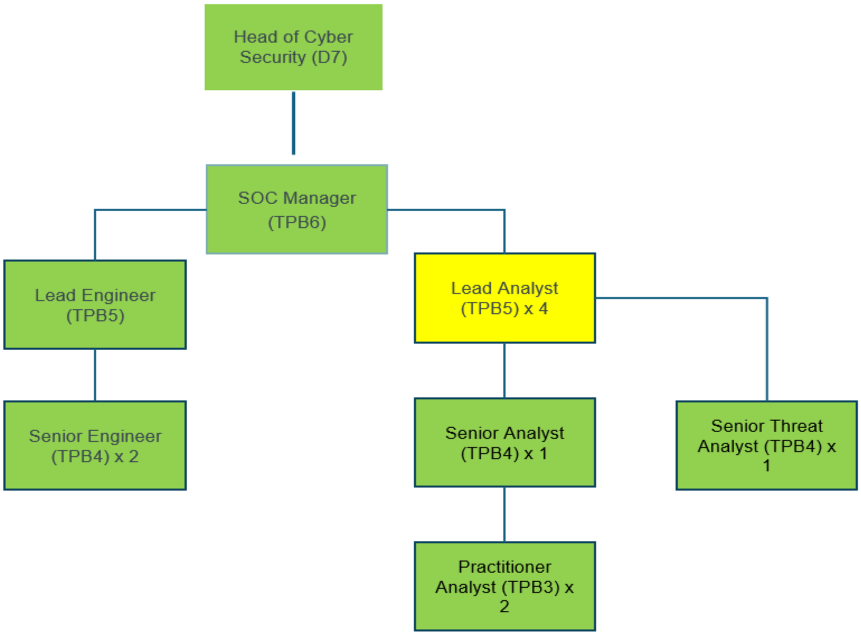
FCDO Services

Job Description

Role Title	**SOC Lead Analyst**		
Business group	T&O Cyber Security		
Job 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.		
Org Chart	 Head of Cyber Security (D7) SOC Manager (TPB6) Lead Engineer (TPB5) Lead Analyst (TPB5) x 4 Senior Engineer (TPB4) x 2 Senior Analyst (TPB4) x 1 Senior Threat Analyst (TPB4) x 1 Practitioner Analyst (TPB3) x 2		
Date Updated	18/12/2024	**Grade**	TPB5

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.
- In association with other colleagues provide an on-Call service to investigate and remedy security and technical issues in relation to the SOC service on a 24/7 basis
- Mentor, train and manage task delivery of Practitioner Analyst ensuring terms of the Service Level Agreement (SLA) are met.

QUALIFICATIONS, KNOWLEDGE & 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

CIVIL SERVICE BEHAVIOURS

Top three for job:

- Seeing the Big Picture
- Making Effective Decisions
- Communicating and Influencing

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

SUCCESS INDICATORS

Success measured and evidenced by:

- 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
-

Budget and Authority	N/A
Reports to: **(Role Title and Grade)**	SOC Manager TPB6
Direct Reports: **(Number and grades of staff)**	2 X TPB4

V 6.0. Dec. 2024