Role Title	Senior Vulnerability Assessor				
Job Family	Security	Sub Category	Cyber Security	Grade	TPB4
Behaviours	• Delivering at Pace	• Communicating and Influencing	• Developing Self and Others	• Making Effective Decisions	
Purpose	Identify and analyse potential security vulnerabilities and breaches in FCDO Services physical and virtual infrastructure and software applications.				

FCDO Services

Key Accountabilities

- Utilise, develop and design the most appropriate approaches and tools to identify, test and exploit security vulnerabilities of software systems and infrastructures of medium complexity within the FCDO Services, network, including applications, physical and virtual servers and storage, laptops etc.
- Conduct scheduled tests and checks to monitor user compliance with organisational information security policies and practices
- Analyse identified security breaches and recommend solutions to mitigate against similar incidents occurring in the future

- Communicate potential business impact of vulnerabilities and make implementable recommendations using language and medium appropriate to the audience
- Provide consultancy on security aspects of FCDO Services projects as required and promote security awareness across the organisation
- Coach associates and share knowledge with team colleagues
- Maintain own professional development and expertise in the latest technologies and best practice to support and grow the business
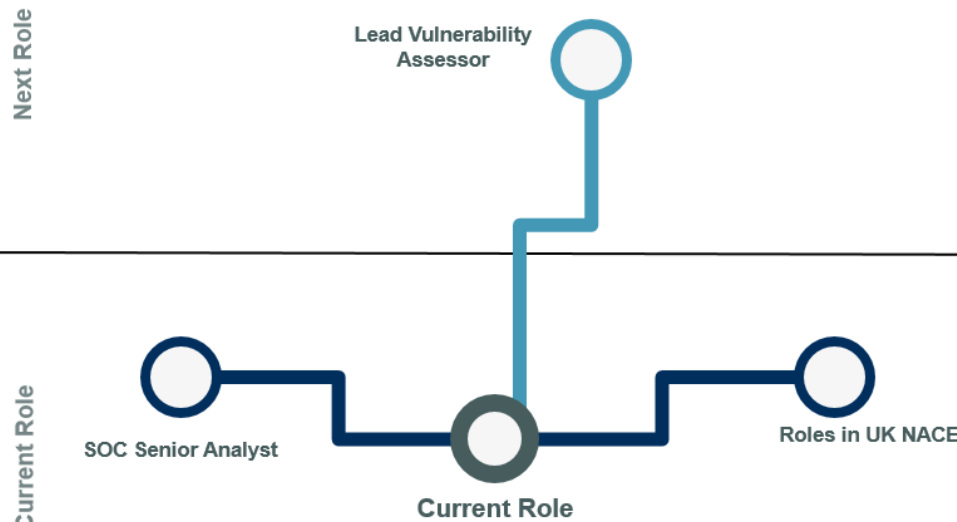
Authority and Scope

- Deliver scheduled and ad hoc tests and reports in agreed timeframes and to required standards
- Follow CREST guidelines and processes for Security Testing
- Assess potential impact of tests to be deployed and escalate / seek agreement from manager when risks are posed to live system performance
- May be responsible for performance management of 1 Practitioner Vulnerability Assessor ensuring they comply with guidelines and processes

Internal and External Communications

- Technical representatives of Customer's to communicate findings and recommendations
- Compliance and MI Manager, Head of Infrastructure, Project Managers and other internal contacts to advise on report findings relevant to their business areas
- Analysts, application developers and testers to provide information on security testing
- Wider security team to analyse issues, and understand how different types of attack might manifest in the network

Potential Next Career Moves

Skills

- Analyse, interrogate and evaluate data
- Bridge technical and non-technical
- Compliance monitoring and controls testing
- Incident management, investigation and response
- Information Risk Assessment and Risk Management
- Penetration testing
- Threat intelligence and threat assessment
- Threat understanding

Qualifications, Knowledge and Experience

Essential
- Working experience in IT resolving technical problems
- Experience in Vulnerability Management or Penetration Testing
- Strong interpersonal skills to work effectively in a team
- Able to manipulate and interpret data using a variety of tools
- Able to produce clear technical documentation

Desirable
- CREST Registered Penetration Tester, Offensive Security Certified Professional