Position: Cyber/IT Security Assistant	**Employment Regime:** Seconded/Contracted	**Post Category:** Assistant Level AL-1
Ref. number: 195	**Location:** The Hague, the Netherlands	**Availability:** ASAP
Component/Department/Unit: Kosovo Specialist Chambers/ Division of Administration/ Information Technology Services Unit	**Security Clearance Level:** EU SECRET or equivalent	**Open to Contributing Third States:** Yes

Reporting Line:

The IT Security Assistant reports to the Cyber/IT Security Officer.

Main Tasks and Responsibilities:

- To perform 1st level routine security monitoring of the ICT network and to verify periodically the security posture of IT systems;
- To detect and investigate anomalies, IT events and incidents on the internal and external networks, and IT infrastructure;
- To participate in implementing security measures and hygiene measures such as updates and patches to cloud and on-premise environments;
- To participate in IT security and forensic investigations, and recommend/implement remedial measures;
- To ensure the effectiveness and comprehensiveness of the SIEM and other security tooling in place in a hybrid environment;
- To support the design, implementation, maintenance and continuous improvement of a secure networking and IT infrastructure environment;
- To support, identify and flag problems arising from recurring, systematic or procedural defects concerning the IT infrastructure, and subsequently initiating action to resolve them;
- To support in vulnerability & risk assessments on applications, technologies and services;
- To support the implementation of IT Security control measures to mitigate IT Security-related risks;
- To undertake any other related tasks as requested by the Line Managers.

Essential Qualifications and Experience:

- A level of secondary education attested by a diploma

AND

- A minimum of ten (10) years of relevant professional experience, after having fulfilled the education requirements.

Specification of Education and Experience

- At least five (5) years of experience with IT security or security operations in an IT environment using a broad range of IT technologies, including virtualization, switching, storage, optimization, management systems, security systems;
- Technical training in Network security and/or IT security, including application security testing;
- At least four (4) years of experience in the use of SIEMs;
- Experience working in Azure and Office365 and related services (MDM, Intune, Defender, etc..)
- Material knowledge of Wireshark, Python and/or PowerShell;
- Knowledge of network protocols, firewalling, log analysis and Windows technology;
- Ability to work productively in a fast-paced, team-oriented environment and produce accurate work under pressure and in difficult circumstances;

- Ability to establish and maintain effective and constructive working relationships with people of different national and/or cultural backgrounds with respect for diversity;
- Demonstrated gender awareness and sensitivity, ability to promote an inclusive working environment and integrate a gender perspective into tasks and responsibilities.

Desirable

- Ability to perform routine administration tasks to patch systems, change firewall rules and adapt technical policies;
- Information Security Certification e.g. Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM) or Certified Information System Auditor (CISA);
- Certifications in Splunk, incident response, penetration testing, SOC analysis, Cloud technologies, Windows server, VMware, or Cisco networking;
- Affinity with streaming & broadcasting environments;
- Prior working experience in a national and/or international criminal or hybrid court;
- Knowledge of the functioning of the EU and in particular CSDP Missions;
- Understanding of the political, cultural, and security situation of the Balkans, in particular Kosovo.