Position: Information Technology (IT) Security System Administrator	**Employment Regime:** Seconded/Contracted	**Post Category:** Assistant Level AL-1
Ref. number: 184	**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 Information Technology (IT) Security System Administrator reports to the System Network Engineer.

Main Tasks and Responsibilities:

- To verify and ensure the security posture of IT systems;
- To perform routine security monitoring of the Information and Communication Technologies (ICT) network and look into anomalies, IT events and incidents on the network and IT infrastructure;
- To detect and investigate anomalies, IT events and incidents on the internal and external networks, and IT infrastructure;
- To participate in IT security and forensic investigations, and recommend/implement remedial measures;
- To ensure the working and effectiveness of the Security information and event management (SIEM) and other security tooling in place;
- Perform IT security administration;
- To assist in the design, implementation, maintenance and continuous improvement of a secure networking and IT infrastructure environment;
- To monitor, administer, troubleshoot, augment & patch IT infrastructure components to ensure uninterrupted and secure service;
- To identifying and flag problems arising from recurring systematic or procedural defects concerning the network and IT infrastructure, and subsequently initiating action to resolve them;
- To liaise and cooperate with the IT/Information Security Officer on IT Security issues, also with external cyber security providers for threat intelligence, incident support and assessments/tests;
- To undertake any other related tasks as requested by the Line Managers.

Essential Qualifications and Experience:

- Level of secondary education attested by a diploma

AND

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

Specification of Education and Experience

- At least eight (8) years of experience with IT operations in an IT environment with 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;
- At least four (4) years of experience in the use of Splunk;
- Knowledge of Wireshark, Python or PowerShell, and building use cases;
- Knowledge of network protocols, firewalling, log analysis and Windows technology;

- Ability to perform routine administration tasks to patch systems, change firewall rules and adapt technical policies;
- 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.

Desirable

- Certifications in Splunk, incident response, penetration testing, SOC analysis, Windows server, VMware, or Cisco networking;
- Experience in the use of Splunk or other and SIEM technology;
- International experience, particularly in an international organization or a hybrid court system;
- Affinity with streaming & broadcasting environments.