Position: Cyber/IT Security Officer	**Employment Regime:** Seconded/Contracted	**Post Category:** Management Level ML-2
Ref. number: 194*	**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 Cyber/IT Security Officer reports to the Head of Information Technology Services Unit.

Main Tasks and Responsibilities:

- To perform 2nd 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 IT security and forensic investigations, and recommend/implement remedial measures;
- To compile reports in relation to reported breaches of Cyber security and proposed remediation;
- To ensure the effectiveness of the SIEM [Splunk] and other security tooling & services in place;
- To ensure the design, implementation, maintenance and continuous improvement of a secure networking and IT infrastructure environment;
- Creating and maintaining detection rules;
- To identify and flag problems arising from recurring, systematic or procedural defects concerning the networks and IT infrastructure, and subsequently initiating action to resolve them;
- To conduct vulnerability & risk assessments on applications, technologies and services;
- To review contracts and organizational policies for the procurement of IT Security services, or where services related to IT are being procured;
- To coordinate and support the KSC's daily routines by providing advice on IT Security related matters;
- To recommend and develop the implementation of IT Security control measures to mitigate IT Security-related risks;
- To liaise with the KSC's external Information Security Officer & cyber security providers for threat intelligence, incident support and assessments/tests;
- To supervise staff and related Cyber/IT activities as required;
- To undertake any other related tasks as requested by the Line Managers.

Essential Qualifications and Experience:

- Successful completion of University studies of at least three (3) years attested by a diploma OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework OR a qualification of the first cycle under the framework of qualifications of the European Higher Education Area e.g. Bachelor's degree.

AND

- A minimum of seven (7) years of relevant professional experience, after having fulfilled the education requirements.

Specification of Education and Experience

- The above mentioned University degree must be in at least one of the following fields of expertise: Information Security, Computer Science, Business & Information Technology or other related university studies;
- At least four (4) years of experience with IT 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;
- Knowledge of Wireshark, Python and/or PowerShell;
- Material 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;
- Knowledge of NIST and ISO2700x, implementing/recommending security controls and knowledge of the NIST phases;
- 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

- Information Security Certification e.g. Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM) or Certified Information System Auditor (CISA);
- Working experience in the use of Splunk;
- Certifications in Splunk, incident response, penetration testing, SOC analysis, Windows server, VMware, or Cisco networking;
- International experience, particularly in an international organization or a hybrid court system;
- Affinity with streaming & broadcasting environments.
- Knowledge and experience in deploying honeypots;
- 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.

Additional information

*This post is exceptionally approved within the limits of the current budget of the Kosovo Specialist Chambers and Specialist Prosecutor's Office. The continuation of this post into the next budgetary period is subject to final confirmation.