Position Name: Visiting Expert on Cyber Security (technical)	**Employment Regime:** Seconded	
Ref. Number: MOL 205 (VE)	**Location:** Chisinau, Moldova	**Availability:** ASAP
Component/Department/Unit: Operations Department/ Hybrid Threats /Cyber security Component	**Security Clearance Level:** EU Secret	**Open to Contributing Third States:** No

1. **Reporting Line**

The Visiting Expert on Cyber Security reports to the Head of Hybrid Threats / Cyber security Component.

2. **Main Tasks and Responsibilities**
- Capacity building on the prevention, resolution and response to cyber incidents;
- Capacity building on the establishment and operationalisation of a Security Operations Center (SOC) and Cyber Incident Response Team (CSIRT), and supporting the constant improvement of the SOC and CSIRT functions;
- Support with updating and defining the list of equipment needs (hardware and software, incl. specifications and certification requirements) for the efficient conduct of SOC and CSIRT functions;
- Capacity building on the monitoring and analyses of cyber threats, vulnerabilities and cyber incidents;
- Support to the establishment of a incident reporting system (external) and ticketing system for incidents (internal);
- Capacity building on information dissemination (early warnings, alerts, announcements on threats, vulnerabilities and incidents);
- Provide training on international cooperation, especially cooperation and information exchange between CSIRTs (e.g. Trusted Introducer network, Malware Information Sharing Platform MISP) and on the integration of platforms with partner organisations of the EU;
- Evaluate the results of the capacity building activities and identify areas for improvement and follow-up actions and solutions.

3. **General Tasks and Responsibilities**
- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective area of responsibility;
- To take account of gender equality and human rights aspects in the execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s).

4. **Essential Qualifications and Experience**
- Successful completion of university studies of at least 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 OR equivalent and attested police and/or military education or training or an award of an equivalent rank;
- Minimum 4 years of relevant cybersecurity experience, preferably in a SOC or CSIRT, after having fulfilled the education requirements.

5. **Essential Knowledge, Skills and Abilities**
- Expert-knowledge of SOC operations, CSIRT operations, network, and/or digital forensics;
- Ability to work with diverse stakeholders, colleagues and counterparts;
- Ability to mentor and motivate local national counterparts, taking into account national

circumstances.

6. **Desirable Qualifications and Experience**
   - Experience on international security standards e.g. ISO27000 series or similar;
   - International recognised IT and/or cyber security certification(s), e.g. ISACA: CISM, CRISC, CISA or ISC2: CISSP, CCSP or similar;
   - Experience in cyber security incident management;
   - Experience in working with SIEM (Security Information and Event Management) platforms;
   - Experience in coordination and information sharing between governmental agencies and services nationally and internationally.
7. **Desirable Knowledge, Skills and Abilities**
   - Excellent interpersonal and teamwork skills;
   - Organisational, analytical and administrative skills;
   - Knowledge of Romanian Language.