Position Name: Visiting Expert on Cyber Security	**Employment Regime:** Seconded	
Ref. Number: MOL 222 (VE), MOL 223 (VE), MOL 224 (VE)	**Location:** Chisinau, Moldova	**Availability:** ASAP
Component/Department/Unit: Operations Department/ Hybrid Threats and Cyber security Component	**Security Clearance Level:** NOT REQUIRED	**Open to Contributing Third States:** Yes

1. Reporting Line

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

2. Main Tasks and Responsibilities

- To support Moldovan counterparts' in building their capacity to prevent, respond and resolve cyber security incidents and operations;
- To strengthen local partners capabilities in monitoring, analysing and communicating about cyber security and threats, vulnerabilities and incidents;
- To enhance the host country direct interlocutors' expertise in areas such as public-private cooperation, national and international collaboration and the role and praxis for supervising authorities;
- To advise on suitable cyber security equipment and related specialised services;
- To promote cyber security best practises and methodologies in line with international standards;
- To advise local counterparts on the practical application of regulations pertaining to cyber security.

3. General Tasks and Responsibilities

- To identify and report on best practices and lessons learned 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; **AND**
- A minimum of 4 years of relevant professional experience, after having fulfilled the education requirements.

5. Essential Knowledge, Skills and Abilities

- Knowledge and experience in one **OR** more of the following fields:
  - Security Operations Centre (SOC) operations, Computer Security Incident Response Team (CSIRT) operations, digital forensics, cyber threat analysis and/or hunting, Cyber Threat Intelligence (CTI), Open-Source Intelligence (OSINT), reporting, network engineering, IT infrastructure hardening, Critical National Infrastructure (CNI) protection, risk assessments, cyber governance, compliance activities, information sharing;

- Ability to communicate, present and report to relevant stakeholders;
- 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 in sensitive information sharing and secure communications between stakeholders;
- Experience in working with Security Information and Event Management (SIEM) platforms;
- Experience in working with different centralised endpoint detection and response platforms;
- Advanced knowledge of: Operating system (Microsoft Windows, Linux, etc);
- Knowledge of networking (flows, protocols, standards), databases, programming, cryptographic processes (certificates, public/private keys, digital signatures), virtualisation (tools, concepts and services);
- Basic to advanced knowledge on cloud infrastructure, services and security;
- Experience in identifying critical entities covered by the EU Directive on Measures for a High Common Level of Cybersecurity (NIS2), and in assessing cybersecurity levels as well as infrastructure and architecture resilience
- Knowledge of international security standards, such as the ISO 27000 series or equivalent frameworks
- Experience obtained in a governmental agency or equivalent;
- Experience in advising at a strategic level, both orally and in writing;
- Experience in drafting analytical reports and strategic recommendations;
- International experience, particularly in crisis areas with multi-national and international organisations.

7. Desirable Knowledge, Skills and Abilities

- Knowledge of cyber security exercises and education;
- Experience in building and facilitating stakeholder relationships for sensitive information sharing and trust-based cooperation;
- Knowledge of Romanian and Russian Language.