

**VACANCY NOTICE**

**SECONDED NATIONAL EXPERT TO THE EUROPEAN COMMISSION**

|  |  |
| --- | --- |
| **Post identification:**  (DG-DIR-UNIT) | **DIGIT-CERT-EU** |
| **Head of Unit:**  **Email address:**  **Telephone:**  **Number of available posts:**  **Suggested taking up duty:**  **Suggested initial duration:**  **Place of secondment:** | **Saâd KADHI**  [**saad.kadhi@ec.europa.eu**](mailto:saad.kadhi@ec.europa.eu)  **+32 2 29 85134**  **1**  **4th quarter 2021 [[1]](#footnote-1)**  **2 years1**  ☒ **Brussels** □ **Luxemburg** □ **Other: ……………..** |
|  | ☒**With allowances** □  **Cost-free** |
| **This vacancy notice is also open to**  **□    the following EFTA countries :  □ Iceland □ Liechtenstein □ Norway □ Switzerland  □ EFTA-EEA In-Kind agreement (Iceland, Liechtenstein, Norway) □    the following third countries: □    the following intergovernmental organisations:** | |

**1. Nature of the tasks**

The seconded national expert will work in one of the five cybersecurity domains listed below under A-E, and perform the tasks listed for that domain.

A. Digital Forensics and Incident Response Analyst

1) Monitor incoming communication (functional mailbox, emergency phone, various chats and alerts in TheHive);

2) Handle communications with constituents and with CERT-EU Peers and Partners, including organisations such as EGC, CNW, FIRST, TF-CSIRC, etc.;

3) Triage alerts and notifications related to incidents, vulnerabilities, or other threats;

4) Verify vulnerability reports;

5) Perform alert and incident analysis using the available data (logs, infrastructure information, etc.) and open sources;

6) Perform digital forensic and artefact analysis.

B. Cyber Threat Intelligence Analyst

1) Monitor threat information sources (open sources, partners, constituents, commercial sources);

2) Analyse threat reports;

3) Control technical threat data workflow (IOCs, detection rules in MISP, OpenCTI);

4) Operate threat intelligence platforms (MISP, OpenCTI);

5) Track top threat actors and top techniques, tactics and procedures (TTPs) activity;

6) Feed CERT-EU’s cyber threat intelligence knowledge base;

7) Produce informative and actionable threat assessments: memos, alerts, cyber security briefs, threat landscape reports.

C. Penetration Tester

1) Perform web application penetration testing;

2) Work on research and development in the context of offensive security assessments;

3) Contribute to toolset maintenance.

D. Red Teamer

1) Perform red team exercises. The main activities include, but are not limited to: payload design, delivery and execution, post-exploitation activities and reporting;

2) Formulate recommendations for hardening systems and protecting infrastructures on the basis of testing outcomes;

3) Work on research and development in the context of offensive security assessments.

E. Cooperation and Policy Officer

1) Support policy development in the elaboration, structuring and implementation of CERT-EU activities:

* Provide expert assessment and participate in the development of the operational cooperation with relevant stakeholders;
* Support the efficient and effective relationships, communication and knowledge-sharing with constituents, stakeholders, and external partners;
* Support CERT-EU’s activities in the structured cooperation with ENISA;
* Contribute to the development of the cyber crisis response plan and capacity building;

2) Manage security incidents through information collection and analysis:

* Conduct investigation and coordination of a subset of security incidents;
* Support planning and participation in cyber-exercises;
* Contribute in knowledge and best practices dissemination through presentations and trainings.

**2. Main qualifications**

**a) Eligibility criteria**

The following eligibility criteria must be fulfilled by the candidate in order to be seconded to the Commission. Consequently, the candidate who does not fulfil all of these criteria will be automatically eliminated from the selection process.

• Professional experience: at least three years of professional experience in administrative, legal, scientific, technical, advisory or supervisory functions which are equivalent to those of function group AD;

• Seniority: candidates must have at least one year seniority with their employer, that means having worked for an eligible employer as described in Art. 1 of the SNE decision on a permanent or contract basis for at least one year before the secondment;

• Linguistic skills: thorough knowledge of one of the EU languages and a satisfactory knowledge of another EU language to the extent necessary for the performance of the duties. SNE from a third country must produce evidence of a thorough knowledge of one EU language necessary for the performance of his duties.

**b) Selection criteria**

Diploma

- university degree or

- professional training or professional experience of an equivalent level

in the field(s) : related to one of the five cybersecurity domains listed above under “Nature of the tasks”.

Professional experience

1. Applicants should have at least 3 years’ experience in one of the five cybersecurity domains listed above under “Nature of the tasks”.

II. Practical experience in the following areas is a clear advantage:

* Work experience in a complex public sector environment;
* General security certifications (e.g., CISSP);
* Certification in a Project Management methodology (e.g. PMI, Prince2) and/or in service management (e.g. ITIL);
* Experience in delivering trainings and public presentations;
* Experience with scripting and editing existing code and programming using one or more of the following: Python,bash,.NET, or C#;
* At least one year’s experience in a Governmental/National CSIRT or equivalent authority;
* At least one year’s experience in cyber exercises;
* Experience in an EU Member States' CERT.

III. Applicants should have or be willing to undergo a screening for a national security clearance at SECRET UE/EU SECRET level. Such clearance shall be obtained by the candidates from their relevant national authorities. Once obtained, this certificate must be valid for the remaining period of the secondment. If not or in the event of not being able to obtain a clearance, the General Secretariat reserves the right to refuse the secondment as national expert.

IV Applicants should have the following knowledge and skills:

* Analytic sharpness in thinking like a threat actor or attacker;
* Ability to translate complex findings into interpretable and simple output;
* High level of customer-orientation;
* Strong analytical and problem solving skills including the ability deal with large amount of information in a limited time;
* Ability to establish and maintain effective working relations with co-workers in an international and multi-disciplinary work environment;
* High degree of commitment and flexibility;
* Good communication skills in English, both orally and in writing.

Language(s) necessary for the performance of duties

Have a thorough knowledge of one of the official languages of the EU and an adequate knowledge of another of these official languages.

**3. Submission of applications and selection procedure**

Candidates should send their application according to the **Europass CV format** (<http://europass.cedefop.europa.eu/en/documents/curriculum-vitae>) in English, French or German **only to the Permanent Representation / Diplomatic Mission to the EU of their country**, which will forward it to the competent services of the Commission within the deadline fixed by the latter.The CV must mention the date of birth and the nationality of the candidate. **Not respecting this procedure or deadlines will automatically invalidate the application.**

Candidates are asked not to add any other documents(such as copy of passport, copy of degrees or certificate of professional experience, etc.). If necessary, these will be requested at a later stage.

Candidates will be informed of the follow-up of their application by the unit concerned.

**4. Conditions of the secondment**

The secondment will be governed by the **Commission Decision C(2008)6866 of 12/11/2008** laying down rules on the secondment to the Commission of national experts and national experts in professional training (SNE Decision).

The SNE will remain employed and remunerated by his/her employer during the secondment. He/she will equally remain covered by the national social security system.

Unless for cost-free SNE, allowances may be granted by the Commission to SNE fulfilling the conditions provided for in Art. 17 of the SNE decision.

During the secondment, SNE are subject to confidentiality, loyalty and absence of conflict of interest obligations, as provided for in Art. 6 and 7 of the SNE Decision.

If any document is inexact, incomplete or missing, the application may be cancelled.

Staff posted in a **European Union Delegation** are required to have a security clearance (up to SECRET UE/EU SECRET level according to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015, OJ L 72, 17.03.2015, p. 53).

The selected candidate has the obligation to launch the vetting procedure before getting the secondment confirmation.

**5. Processing of personal data**

The selection, secondment and termination of the secondment of a national expert requires the Commission (the competent services of DG HR, DG BUDG, PMO and the DG concerned) to process personal data concerning the person to be seconded, under the responsibility of the Head of Unit of DG HR.DDG.B4. The data processing is subject to the SNE Decision as well as the Regulation (EU) 2018/1725.

Data is kept by the competent services for 10 years after the secondment (2 years for not selected or not seconded experts).

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given below.

**Contact information**

* **The Data Controller**

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, HR.DDG.B.4, [HR-MAIL-B4@ec.europa.eu](mailto:HR-MAIL-B4@ec.europa.eu).

* **The Data Protection Officer (DPO) of the Commission**

You may contact the Data Protection Officer ([DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:DATA-PROTECTION-OFFICER@ec.europa.eu)) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

* **The European Data Protection Supervisor (EDPS)**

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

To the attention of candidates from third countries: your personal data can be used for necessary checks.

1. These mentions are given on an indicative basis only (Art.4 of the SNE Decision). [↑](#footnote-ref-1)