EUROPEAN COMMISSION

DIRECTORATE-GENERAL INFORMATICS

OPERATIONAL COOPERATION OFFICER

Vacancy: Contractual Agent FGIV
Where: DIGIT/CERT-EU, Brussels
Publication: from 30/04/2021 to 30/05/2021 until 12.00 hours Brussels time

We are

DIGIT is the Directorate-General for Informatics whose aim is to deliver digital services to enable EU policies and to support the Commission's internal administration. CERT-EU is part of DIGIT.

CERT-EU is the Computer Emergency Response Team for the Institutions, Bodies and Agencies of the European Union. CERT-EU helps them to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of its activities covers prevention, detection, response and recovery.

CERT-EU is a world-renowned cybersecurity entity, working tirelessly to protect the data and systems of our constituents. Established in 2011 to shore up the ICT security of all the European Union Institutions, Bodies and Agencies, we have been steadily expanding our IT security operations over the years and currently serve over 80 such entities spread across the Continent and beyond. From our base in Brussels, we work with a range of peers, partners and researchers from all over the world to ensure we maintain our technological edge and have access to the best-in-class expertise.

Our team is a mix of technical and non-technical experts – diverse, talented, and all of them passionate. On any given day, the digital forensics and incident response team fights to prevent breaches from sophisticated adversaries, our offensive security experts assess the defences of our constituents, while our cyber threat intelligence colleagues, having a unique perspective on the threat landscape, monitor and report on the latest threats and trends out there. And that's just a small part of the overall picture!

Indeed, on any other day, our automation experts will be developing effective solutions to increase our collective efficiency, while our engineering and IT operations colleagues operate our vast network of detection sensors and log collection platforms, continuously refine our operational security and relentlessly work to sustain the services we provide to our constituents. The security consultation staff members suggest tailor-made solutions and help the organisations we protect improve their cybersecurity posture. Finally, our cooperation team engages with key stakeholders such as the CSIRTs Network, Europol EC3, ENISA and NATO and sets the grounds for fruitful working ties.

CERT-EU is proud of its team spirit. Our motto is "Think Constituent, Create Value". To achieve this, all of our professionals share a strong will to work and grow together. We offer a very dynamic and multicultural workplace, with a range of career opportunities for seasoned professionals, recent graduates or students alike. With us, you will find not only an environment designed to encourage open minds and attitudes but also a truly collaborative and congenial working atmosphere. To put it shortly, we are the closest you can get to a start-up in a public administration setup.

We propose

We wish to hire an Operational Cooperation Officer to join our élite Cooperation team, which operates as an interface between the technical and the operational cybersecurity community, ensuring the efficient cooperation of the various stakeholders, such as the European Commission, the European External Action Service, ENISA, Europol, the CSIRTs Network, NATO and other key cybersecurity players worldwide.

The Cooperation team has a key role in crisis response in the EU Institutions, Bodies and Agencies, CERT-EU's constituents. The team also provides recommendations to CERT-EU's upper management and supervises their implementation as regards capacity building and structured cooperation.

Under the guidance of the Cooperation leader, the selected candidate will:
- 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 its structured cooperation with ENISA.
- Contribute to the development of the cyber crisis response plan and capacity building.
- Support planning and participation in cyber-exercises.
- Organise and oversee CERT-EU's knowledge base.

This is a highly technical, challenging, and empowering job with enough room for all of one's competencies to shine in a very friendly, supportive, human and professional environment.

We look for

The successful candidate should have the following knowledge and skills:
- Relevant academic background in Information Security;
- Proven experience in IT security, particularly in the policy development, risk management, governance and compliance areas;
- Excellent drafting skills, experience in drafting policies, standards, and operational procedures; service delivery experience;
- Good understanding of European Institutions, Bodies and Agencies' decision-making and consultation processes and cross-functional project stakeholder coordination.
- Strong analytical and problem-solving skills including the ability deal with large amounts of information in a limited time;
- Ability to manage parallel tasks and cope with pressure, in particular in crisis situations;
- Very good command of English (written and spoken); knowledge of French is an advantage.

Any of the following elements represent an advantage:
- Work experience in a multi-layered and complex public sector environment;
- Knowledge of the EU Cybersecurity strategy, the NIS Directive, the Cybersecurity Act, the Cyber Blueprint and the Joint Cyber Unit;
- Work experience in a National/Governmental CSIRT;
- General cyber security certifications (e.g. CISSP);
- Certification in service management (e.g. ITIL) and/or security certifications in the field of risk management, maturity assessment or security management.

The candidate must hold a security clearance at EU SECRET level or be in a position to be security cleared.

Am I eligible to apply?

You must meet the following eligibility criteria when you validate your application:

General conditions:

- Enjoy full rights as a citizen of an EU Member State
- Meet any obligations under national laws on military service
- Meet the character requirements for the duties concerned
- The EU institutions apply an equal opportunities policy and accept applications without distinction on the grounds of gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

Specific conditions - Languages

Language 1: minimum level C1 in one of the 24 official EU languages
Language 2: minimum level B2 in English, French or German; must be different from language 1

The official languages of the European Union are: BG (Bulgarian), CS (Czech), DA (Danish), DE (German), EL (Greek), EN (English), ES (Spanish), ET (Estonian), FI (Finnish), FR (French), GA (Irish), HR (Croat), HU (Hungarian), IT (Italian), LT (Lithuanian), LV (Latvian), MT (Maltese), NL (Dutch), PL (Polish), PT (Portuguese), RO (Romanian), SK (Slovak), SL (Slovenian), SV (Swedish)

For details on language levels, please see the Common European Framework of Reference for Languages (https://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr)

Specific conditions - qualifications & professional experience

- A level of education which corresponds to completed university studies of at least three years attested by a diploma;

Only qualifications issued or recognised as equivalent by EU Member State authorities (e.g. by the Ministry of Education) will be accepted. Furthermore, before recruitment, you will be required to provide the documents that corroborate your eligibility and the information in your application form (diplomas, certificates and other supporting documents)

How to apply

The interested candidates should send their application respecting the deadline of the vacancy to the following email address:

secretariat@cert.europa.eu

Due to the large volume of applications received, only candidates selected for the interview will be notified.

Selection procedure

No applications will be accepted after the closing date of the vacancy.

Candidates selected for interviews will have to succeed in an EPSO CAST exam relevant to the function group.

The request to sit the EPSO CAST exams does not commit in any way the European Commission to invite candidates for a selection panel or offer a Contract Agent position, should they succeed the test.

During the recruitment process, candidates will be requested to supply documentary evidence, in original, in support of the statements made in the application.

For functional reasons and in order to complete the selection procedure as quickly as possible in the interest of the candidates as well as that of the institution, the selection procedure will be carried out in English and/or French only.

For more information on the Contract Agent positions please consult the following EPSO page.

Should a position be offered, candidates are required to undergo a mandatory medical analysis and physical check-up with our selected medical service.

The working conditions of contract staff are governed by the Staff Regulations of Officials and the Conditions of Employment of Other Servants, as described in chapter IV, p. 215 of the following document:
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20110101:EN:PDF
Contract agents carry out tasks under the supervision of officials or temporary staff members. Further details concerning the nature of tasks and type of duties can be found in ANNEX I.

Equal opportunities

The European Commission applies a policy of equal opportunities and non-discrimination in accordance with Article 1d of the Staff Regulations.

Data Protection

For information related to Data Protection, please see the Specific Privacy Statement.