EUROPEAN COMMISSION

DIRECTORATE-GENERAL INFORMATICS

Digital Forensics and Incident Response Analyst

Vacancy: Contractual Agent (3b) FGIV
Where: DIGIT CERT EU, Brussels
Publication: from 15/05/2023 to 31/05/2023 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 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 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 people are 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 will be busy testing the defences of our constituents, while our cyber threat intelligence colleagues monitor and report on the latest threats and trends out there. And that's just a small part of the picture!
On any other day, the automation experts will be developing solutions for all sorts of upcoming software vulnerabilities, while the engineering and IT operations colleagues screen the networks and stand ready to sound warning calls in case of anomalies; the security consultation staff members suggest tailor-made solutions and help the constituents to improving their cybersecurity posture; and the cooperation team engages with the stakeholders and sets the grounds for fruitful working ties.

CERT-EU is proud of its team spirit; 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 a challenging and rewarding environment in the heart of cybersecurity in a truly collaborative and supportive atmosphere.

We propose

The Digital Forensics and Incident Response (DFIR) Team has the responsibility for monitoring available information sources for indications of compromise of the EU institutions, bodies and agencies, our constituents. Analysts in the team triage the incoming information, and, if necessary, investigate incidents and coordinate the full response process.

The selected candidate will work in a team of security experts, each one predominantly focused in the specific security domain for which they are most competent, but all closely cooperating as a team, coordinated by the DFIR Team Leader, who reports to the Head of CERT-EU.

The DFIR Analyst will be responsible for performing various roles in the DFIR team, depending on his or her specific experience and expertise. In particular the job will include security alerts triaging, log analysis, forensic analysis of disk and memory images, and reporting. Additional duties include improvements of tools and processes aiming at increasing efficiency and performance of the team. Additionally, DFIR Analyst will have the opportunity to improve his or her skills as well as learn new ones through comprehensive training program involving both internal and external trainings.

We look for

The successful candidate should have at least limited experience in IT Security with knowledge of some of the following domains:

- Vulnerability assessments and penetration testing;
- Knowledge of Windows, Linux, and MacOS operating systems;
- Log management tools for network log analysis (Splunk specifically is a plus);
- Tools for packet capture and analysis such as Wireshark or tcpdump;
- Web security including understanding of the underlying protocols;
- Static artefact analysis including debugging, code de-obfuscation, and reverse engineering basics
- Scripting experience with special interest in JavaScript, Python, and PowerShell;
- Using and configuring sandboxes such as Cuckoo, FireEye, etc.
- Memory forensics tools such as Volatility;
- Disk forensics tools, such as EnCase, FTK, the SleuthKit, or RegRipper, etc.;
- Cyber-threat intelligence sharing and in particular MISP sharing platform;
- Experience in incident management tools, such as TheHive.

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.

The candidate should show the following skills:

- A 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;
- A high degree of commitment and flexibility;
- Excellent communication skills in English, both orally and in writing;

- A focus on constant learning and improvement of technical and personal skills;
- Experience with a vast array of IT technologies and the ability to quickly master new ones.

The candidate must hold a security clearance at SECRET-EU 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:

Candidates will be eligible for this selection procedure if they fulfil the following formal criteria at the time of the application deadline:

- Be a national of a Member State of the European Union (EU) and enjoy his or her full rights as a citizen;
- Have fulfilled any obligations imposed by applicable laws concerning military service;
- Be physically fit to perform the duties linked to the post
- Produce the appropriate character references as to suitability for the performance of the duties
- Languages: Have a thorough knowledge of one of the official EU languages and a satisfactory knowledge of a second EU language to the extent necessary for the performance of his/her duties;
- Qualifications: Completed university studies of at least three years attested by a diploma.

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

Specific conditions - qualifications & professional experience

- A level of education which corresponds to completed university studies of at least three years attested by a diploma; or
- Where justified in the interest of the service, professional training of an equivalent level.

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 CV and motivation letter respecting the deadline of the vacancy to the following email address:

CERT EU Secretariat 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 exam 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 here.

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.