EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Digital Forensics and Incident Response Analyst

Vacancy: Contractual Agent FGIV
Where: DIGIT/CERT-EU, Brussels
Publication: from 23/11/2020 to 15/12/2020 until 12.00 hours noon Brussels time

We are

CERT-EU's mission is to support the European Institutions 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 CERT-EU's activities covers prevention, detection, response and recovery.

We propose

The Digital Forensics and Incident Response (DFIR) Team has the responsibility for monitoring available information sources for indications of compromise of CERT-EU constituents, triaging the incoming information, and – if necessary – investigating and coordinating the incidents.
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:

- 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;
- Excellent communication skills in English, both orally and in writing.

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:

- 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; 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 application 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 a CAST EPSO exams relevant to the function group.

Due to the large volume of applications received only candidates selected for interviews will be notified

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 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, (see the following link http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20110101:EN:PDF chapter IV, p. 215).
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 are 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. https://ec.europa.eu/dpo-register/detail/DPR-EC-01029