MAKE A DIFFERENCE – JOIN THE EUROPEAN COMMISSION

Do you want to help shape the future of the European Union? Make the planet greener, promote a fairer society, or support businesses and innovation across the EU? Then come and work for the European Commission where you can really make a difference!

Commission staff are a diverse group of people, who are motivated to help make Europe – and the world – a better place. They come from the 27 Member States of the European Union. Different nationalities, backgrounds, languages and cultures make the Commission a vibrant and inclusive place to work.

WE OFFER GREAT JOBS AND GREAT WORKING CONDITIONS:

- Interesting and challenging jobs with plenty of opportunities for training and acquiring new skills and competencies throughout your whole career
- Opportunities to move between different policy areas throughout your career
- A package of flexible working conditions including the possibility of teleworking – we care about your work-life balance
- A competitive financial package, including comprehensive healthcare, accident and pension schemes
- A multilingual, multicultural workplace where personal and career development are strongly promoted
- Multilingual schools for your children

We recruit from a wide range of backgrounds and actively promote diversity and inclusion:

We do not only recruit political scientists and lawyers but are also looking for all kinds of profiles, including scientists, linguists, IT experts, data analysts and economists, as well as drivers and engineers.

We are committed to equal opportunities and to fostering a rich, diverse and inclusive working environment. We aim for our workforce to be representative of European society and strongly welcome applications from all qualified candidates. We actively seek to create a workplace where each staff member feels valued and respected, can give their best and can develop to their full potential.

To promote diversity and establish a geographically balanced pool of candidates, we strongly encourage applicants from Member States which are currently underrepresented in the European Commission workforce to apply. These Member States are currently Austria, Cyprus, the Czech Republic, Denmark, the Netherlands, Estonia, Finland, Germany, Ireland, Luxembourg, Malta, Poland, Portugal, Slovakia and Sweden[1]. Recruitment will however remain strictly based on the merits of all applicants and no positions will be reserved for nationals of any specific Member State.

For more information ec.europa.eu/work-with-us

STAFF RECRUITED ON CONTRACTS

In addition to permanent officials, the European Commission offers non-permanent positions. There are two categories of non-permanent staff:

- **temporary agents** are recruited to fill vacant positions for a set amount of time or to perform highly specialised tasks.
- **contract agents** may provide additional capacity in specialised fields where an insufficient number of officials is available or carry out a number of administrative or manual tasks. They are generally recruited for fixed-term contracts (maximum 6 years in any EU Institution), but in some cases they can be offered contracts for an indefinite duration (in offices, agencies, delegations or representations).

For more information on different staff categories

[1] Please note that the list of underrepresented Member States may be subject to future amendment based on potential data changes over time.

IT Security Officer

Digital Forensics & Incident Response analyst

Directorate-General for Digital Services CERT-EU of the European Commission

Selection reference: DIGIT/COM/2025/1193
Domain: Information and Communication Technologies
Where: DIGIT CERT-EU, Brussels
Staff category and Function Group: Temporary agent 2b/2d – Administrator
Grade range: AD5-7
Publication deadline: 17.10.2025 - 12.00 (Brussels time)

WE ARE

DIGIT is the Directorate-General for Digital Services whose aim is to deliver digital services to enable EU policies and to support the Commission's internal administration. CERT-EU is the Cybersecurity Service for the European Union institutions, bodies, offices and agencies (Union entities). CERT-EU is administratively attached to DIGIT.

Established in 2011 to shore up the ICT security for the Union entities, we have been steadily expanding our IT security operations over the years and currently serve over 90 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.

WE PROPOSE

CERT-EU is looking to hire a truly motivated IT Security Officer - Digital Forensics & Incident Response analyst. This is a highly challenging and empowering job which provides many opportunities for one's competencies to shine in a very friendly, supportive, human and professional environment. The selected candidate will serve as a Digital Forensics and Incident Response (DFIR) analyst within CERT-EU, supporting the European Union institutions, bodies, offices and agencies (Union entities).
Your primary responsibility will be to investigate and respond to cybersecurity incidents, uncovering threats through forensic analysis of multiple evidence artifacts at scale, including disk, memory, and network data. The job holder will also lead the threat hunting exercises within the team, designing and refining threat detection logic, use cases, and response workflows to enhance CERT-

EU's ability to uncover and respond to threats effectively.
The position will consist of the following, amongst other tasks:

- Conducting in-depth investigations of cybersecurity incidents affecting Union entities, including forensic analysis of disk, memory, and network data.
- Analysing logs and digital artefacts across diverse platforms (Windows, Linux, macOS) to determine root cause and scope of incidents.
- Using specialised forensic tools (Thor, Dissect, Plaso, Velociraptor) to extract and interpret digital evidence.
- Leveraging log management platforms and SIEM/XDR solutions, such as Microsoft Sentinel and Microsoft XDR, to support detection and investigation workflows.
- Documenting findings in clear, structured incident reports and contributing to post-incident reviews and lessons learned.
- Collaborating with other DFIR team members and stakeholders to ensure a coordinated response to major incidents.
- Leading the implementation of threat hunting strategies by proposing them to the sector (FORCE) management and coordinating their implementation.
- Conducting threat hunting exercises within the customer's network and working in close collaboration with the customer's technical teams.
- Designing, implementing, and maintaining threat detection rules to identify malicious behaviours during threat hunting exercises.
- Continuously improving threat detection logic to reduce false positives and enhance findings fidelity.
- Working closely with SOC analysts, the CTI team, and the DFIR team to translate threat insights into actionable hunting campaigns.
- Monitoring threat landscape developments in close collaboration with CTI team and proactively adapting threat hunting capabilities accordingly.
- Developing and maintaining custom scripts and tools to support DFIR investigations and detection workflows.
- Automating repetitive or manual tasks to improve operational efficiency in forensic analysis and detection response.
- Ensuring the reliability and scalability of DFIR tools and platforms used by the team.
- Contributing to the development of internal tooling to facilitate analysis and evidence handling.
- Leveraging and sharing operational insights to help Union entities improve detection and response capabilities.
- Supporting training efforts within the team and actively engaging in knowledge transfer and mentoring.
- Providing feedback on CERT-EU services and capabilities based on operational experience to guide continuous improvement.

WE LOOK FOR

The selected candidate should also possess knowledge and experience in the following domains:

- Knowledge of Windows, Linux, and macOS operating systems.
- Practical experience with log management and analysis tools.
- Knowledge in forensics operations.
- Practical experience with forensics tools: Network, e.g., Wireshark, tcpdump / Disk, e.g., Plaso, Dissect, SleuthKit, Velociraptor / Memory, e.g., Volatility.

- Knowledge in web security including understanding of the underlying protocols.
- Experience in static artefact analysis including debugging, code de-obfuscation, and reverse engineering basics.
- Scripting/Development experience.
- Experience using SIEM and XDR platforms to support investigations, particularly Microsoft Sentinel and Microsoft XDR.
- Experience in Cyber-threat intelligence sharing, using MISP in particular.
- Experience in incident response, and incident management as well as threat hunting.

The candidate should also demonstrate the following skills:

- A high level of customer orientation.
- Strong analytical and problem-solving skills including the ability to deal with a 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.
- Excellent communication skills in English, both orally and in writing.
- High degree of commitment and flexibility, enthusiasm and motivation to work, with strong teamwork abilities.
- A focus on constant learning and improving technical and personal skillsets.
- Experience with a vast array of IT technologies and the ability to quickly master new technologies.

To make your application stand out, please consider that the ideal candidate will possess some, or all, of the following:

- A university-issued diploma or equivalent.
- At least 4 years of professional experience in Digital Forensics & Incident Response, including at least 1 year of experience in the threat hunting field.
- Experience with Threat-Detection-as-Code principles, particularly using Sigma, across multiple platforms.
- Work experience in a complex public sector environment.
- Experience in delivering trainings and public presentations.

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

HOW TO EXPRESS YOUR INTEREST?

You should send your documents in a **single pdf** in the following order:

1. your CV 2. completed application form.

Please send these documents by the publication deadline to *secretariat@cert.europa.eu* indicating the selection reference **DIGIT/COM/2025/1193** in the subject.

No applications will be accepted after the publication deadline.

ANNEX

1. *Selection*

➢ Am I eligible to apply?

<u>You must meet the following eligibility criteria when you validate your application</u>:

Our rules provide that you can only be recruited as a temporary agent at the European Commission if you:

General criteria:

- Are a citizen of a Member State of the EU and enjoy full rights as a citizen
- Have fulfilled any obligations imposed by applicable laws concerning military service
- Are physically fit to perform the duties linked to the post
- Produce the appropriate character references as to suitability for the performance of the duties.

Qualifications:

In order to be recruited for this position, you must have at least a level of education which corresponds to completed university studies of at least 3 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 the eligibility criteria (diplomas, certificates and other supporting documents).

Languages:

- have a thorough knowledge (minimum level C1) of one of the 24 official languages of the EU[2]
- AND a satisfactory knowledge (minimum level B2) of a second official language of the EU, to the extent necessary for the performance of the duties.

➢ What about the selection steps?

The post was published internally within the Commission, inter-institutionally, and brought to the attention of competition laureates.

[2] 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 (Croatian), HU (Hungarian), IT (Italian), LT (Lithuanian), LV (Latvian), MT (Maltese), NL (Dutch), PL (Polish), PT (Portuguese), RO (Romanian), SK (Slovak), SL (Slovenian), SV (Swedish).

In accordance with Article 29 of the Staff Regulations, applications from Commission officials, officials from other Institutions, and laureates of competitions have priority[3]. If these candidates do not best fit the requirements for the position, the Commission can recruit a temporary agent.

A selection panel will choose a limited number of candidates for interview, based on the CV and application form that they submitted. Due to the large volume of applications, we may receive, **only candidates selected for the next step of the selection phase will be notified.**

For operational reasons and in order to complete the selection procedure as quickly as possible in the interest of the candidates and of the institution, the selection procedure will be carried out in English and possibly in another language.

2. Recruitment

The candidate selected for recruitment will be requested to supply documentary evidence in support of the statements made in their application.

The successful candidate will be required to undergo a mandatory pre-recruitment medical check-up, carried out by the Commission. Candidates are required to undergo a security vetting that is conducted with the national administration of the Member State.

➢ Type of contract and working conditions

The place of employment will be **Brussels.**

In case the successful candidate is not an official or a competition laureate, they will be recruited as a **temporary agent under Article 2(b)/2(d) of the** Conditions of Employment of Other Servants**, in function groups AD.**

[3] Officials from the Commission or other Institutions are invited to use the standard channels (Sysper or inter-institutional vacancy portal).

➢ Grade

The recruitment grade, as well as the step in that grade, will be determined in accordance with Commission Decision C(2025)4716 on policies for the engagement and use of temporary agents and with Commission Decision C(2013)8970 laying down the criteria applicable to classification in step on engagement.

The recruitment grade will be calculated based on the qualifications and the number of years of professional experience, according to Art. 13 of the Commission Decision C(2025)4716. Higher grades may be granted exceptionally.

The duration of the **1st contract will be up to 4 years.** The contract might then be extended only once for a maximum of 2 years and in the interest of service, in accordance with Commission Decision C(2025)4716 on policies for the engagement and use of temporary agents.

All new staff have to successfully complete a 9-month probationary period.

The pay of staff members consists of a basic salary supplemented with specific allowances, including, where applicable, expatriation and family allowances. The provisions guiding the calculation of these allowances can be consulted in the Conditions of Employment of Other Servants. As a member of staff of the European institutions, your pay is subject to a tax raised by those institutions.

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

Should you need further information on working conditions, please refer to Working conditions and benefits of EU Careers.

For information related to Data Protection, please see the Specific Privacy Statement under "7. Information to data subjects on their rights", to find your rights and how to exercise them in addition to the privacy statement, which summarises the processing of your data.