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 –

Threat Detection Engineering Architect

Directorate-General for Digital Services (DG DIGIT) of the European Commission

Selection reference: DIGIT/COM/2026/553
Domain: Cybersecurity
Where: Unit DIGIT.S.2 "Cybersecurity Operations Centre", Luxembourg
Staff category and Function Group: Temporary agent 2b/2d – Administrator
Grade range: AD5-7
Publication deadline: 15.04.2026 - 12.00 (Brussels time)

WE ARE

The Cybersecurity Operations Centre Unit (DIGIT.S.2) is responsible for providing the principal operational cybersecurity incident response capability within the European Commission and the Executive Agencies.

The unit is a modern Cybersecurity Operations Centre (CSOC) with enhanced ability to detect, analyse and respond to cyber threats, in a scalable and sustainable way. It protects the users, the data sets and the IT assets of the Digital Commission through continuous analysis of the threat landscape, monitoring, detection and real-time investigation of potential intrusions, response to confirmed incidents and reinforced situational awareness.

The mission of the unit is to strengthen the cybersecurity posture of the organisation by providing state of the art monitoring, detection and response services and solutions and, more specifically by:

- Preventing IT security incidents through proactive measures, including continuous analysis of the threat landscape and deploying coordinated mitigation controls.
- Monitoring, detection, and analysis of potential intrusions in real time and through adversary hunting, utilizing a variety of IT security-relevant data sources.
- Responding to confirmed cybersecurity incidents, by coordinating resources and directing use of timely and appropriate mitigation measures.
- Providing situational awareness and reporting on cybersecurity threat landscape, incidents, and trends in adversary behaviour.
- Engineering and operating CSOC technologies, such as host sensors, network sensors, log collection, and various analysis systems.

DIGIT.S.2 satisfies the constituency's cybersecurity incident management needs by providing the following capabilities:

- Cybersecurity Operations Coordination and Enablement (SOCET).
- Malware Analysis, Research and Threat Intelligence (MARTI).
- Cybersecurity Incident Response Capability (CSIRC).
- Cybersecurity Analytics, Trending, Correlations and Hunting (CATCH).
- Cybersecurity capability Engineering and Management (CEM).

WE PROPOSE

We seek an **IT Security Officer - Threat Detection Engineering Architect** to join our **Cybersecurity Analytics, Trending, Correlations and Hunting (CATCH)** team (Sector DIGIT.S.2.004). You will define and oversee **threat-informed detection and visibility architecture** for **network security services**, supporting the CSOC's security operations.

Key Responsibilities:

- Design and recommend security controls and visibility requirements applicable to network security services.
- Ensure that appropriate logging, telemetry and network traffic inspection mechanisms are in place for high-quality visibility into pan-european network service.
- Embed zero-trust principles into detection architecture by designing use cases that validate continuous authentication, least-privilege enforcement, and micro-segmentation, leveraging identity-aware logs and behavioural analytics to detect trust violations in real time.
- Design and recommend detection in streamed data/log collection pipeline before ingestion into the SIEM when applicable
- Use, and help operationalise, the OpenTIDE framework for threat-informed detection, translating threat intelligence and adversary techniques into detection requirements and detection-as-code artefacts.
- Support Threat Hunting activities by ensuring that the necessary network telemetry and logs are available to implement automated threat hunting campaigns and detections on indicators of compromise and adversary techniques.

Collaboration:

- Work with network/infrastructure teams, log collection teams, and CSIRC/MARTI for threat hunting and detection.
- Liaise with multiple units inside and outside the Directorate-General for Digital Services.

Profile:

- Strong background in threat detection, SIEM, network security, and zero-trust architectures.
- Experience with detection engineering, and automated threat hunting.
- Ability to translate threat intelligence into actionable detection rules.

Join us to enhance cybersecurity resilience through innovative detection engineering!

WE LOOK FOR

We are looking for a Threat Detection Engineering Architect.
The ideal profile for the job combines the following professional experience and skills.

Professional experience:

IT Security / Threat Detection (essential)

At least 3 years of experience in the domain of IT security, with specific background in one or more of the following areas:

- Network security architecture, design or engineering (e.g. firewalling, IDS/IPS, proxies, VPN, DNS security, web gateways, WAF, network segmentation).
- IT security monitoring and detection, including SIEM use cases, correlation rules and detection engineering.
- Threat-informed defence (e.g. MITRE ATT&CK, kill chain) and applying threat intelligence to detection use cases.
- Threat hunting or supporting threat hunting through visibility enablement and log source design.
- Practical understanding of zero-trust architectures (ZTA) and how to translate them into detection requirement.

IT Service Management / Governance (desirable)

At least 2 years of experience in IT Service Management, covering:

- Experience in developing and/or operating an IT service in a large organisation.
- Practical experience in systems/solutions design including supporting processes and procedures.
- Familiarity with ITIL-based processes (incident, problem, change and configuration management) or equivalent frameworks.

Practical experience considered a clear advantage:

- Experience implementing zero-trust detection frameworks on network security architectures or integrating zero-trust signals into threat detection.
- Designing or reviewing network and security system engineering documentation, concepts of operations, security operations procedures and configuration specifications, to derive and validate detection and visibility requirements.
- Designing or validating logging and telemetry requirements for network security components and integrating them into a SIEM or similar analytical platform in a large environment.
- Working with threat-informed detection frameworks such as OpenTIDE, including mapping threats and adversary techniques to concrete detection and logging requirements.
- Familiarity with modern log pipelines and data platforms (e.g. Kafka, Fluentd/Fluent Bit, Logstash, data lakes) and the concept of detection in log collection pipelines.
- Implementing open source projects or EU-based solutions related to cybersecurity (e.g. MISP, Suricata, OpenVPN, Strongswan).
- Supporting the design of SOC processes and case management for handling alerts originating from network security services.
- Integrating security capabilities with automation and orchestration (e.g. SOAR, automated enrichment, detection-as-code pipelines).

Holding security certifications in the field of IT security, network security, or IT service management is an asset.

Skills:

- Ability to lead working groups and drive consensus on architectural decisions across multiple technical and non-technical stakeholders.
- Ability to work effectively with team members and with customers, including network operations, infrastructure, application owners and CSOC analysts.
- Self-motivated, with ability to manage and follow up on multiple tasks simultaneously.
- Ability to manage parallel tasks and cope with pressure, in particular in crisis situations or during major incident handling.
- Demonstrated organisational and scheduling skills for planning roadmaps, log onboarding and visibility improvement programmes.
- Strong analytical skills, with the ability to approach problems from multiple angles and translate threats into technical requirements.
- Effective verbal and written communication skills, including the ability to communicate technical and architectural topics clearly and concisely.

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 DIGIT-S2@ec.europa.eu indicating the selection reference DIGIT/COM/2026/553 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.

For temporary agents under Article 2(a) of the Conditions of Employment of Other Servants, the post is published directly on the EPSO website, without mandatory prior internal publication.

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.

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 **Luxembourg**.

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, AST or AST/SC.**

[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.