# ECCC

## EUROPEAN CYBERSECURITY COMPETENCE CENTRE

### Digital Europe Programme Call

**4th ERA-ENISA Conference on Cybersecurity in Railways**

**Digital Europe Programme and Horizon Europe on Cybersecurity**

**Ivan SCANNAPIECORO**
*ECCC – Team Leader*
**03/10/2024**

#DigitalEU

# Agenda

1. The ECCC and its network;
2. Digital Europe Programme Call;
3. Horizon Europe Programme Call;
4. Q&A.

# The ECCC

*The ECCC is the engine for the implementation of Europe's strategy in research, innovation, and industrial policy in the area of cybersecurity.*

# The ECCC

- established with Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.

- The ECCC is financially autonomous since 24 September 2024.

- The ECCC premises are located at the **Polytechnic University in Bucharest - CAMPUS Centre**, and its operations have been carried out there **since 09.05.2023.**

- The permanent premises will be inaugurated on 30 October 2024.

- The ECCC will have soon 38 staff members as foreseen in the regulation.



**ECCC**
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

# The actors (1/3)



European Cybersecurity Competence Centre

Network of National Coordination Centres

Cybsersecurity Community

- *Strengthen EU leadership in cybersecurity by enhancing trust and security*

- *EU strategic autonomy and global competitiveness*

- *Support network and information system resilience and reliability*

- *Contributing to a strong European cybersecurity ecosystem and bringing stakeholders together*



**Mission**

Objectives

Implementation

**ECCC**
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE
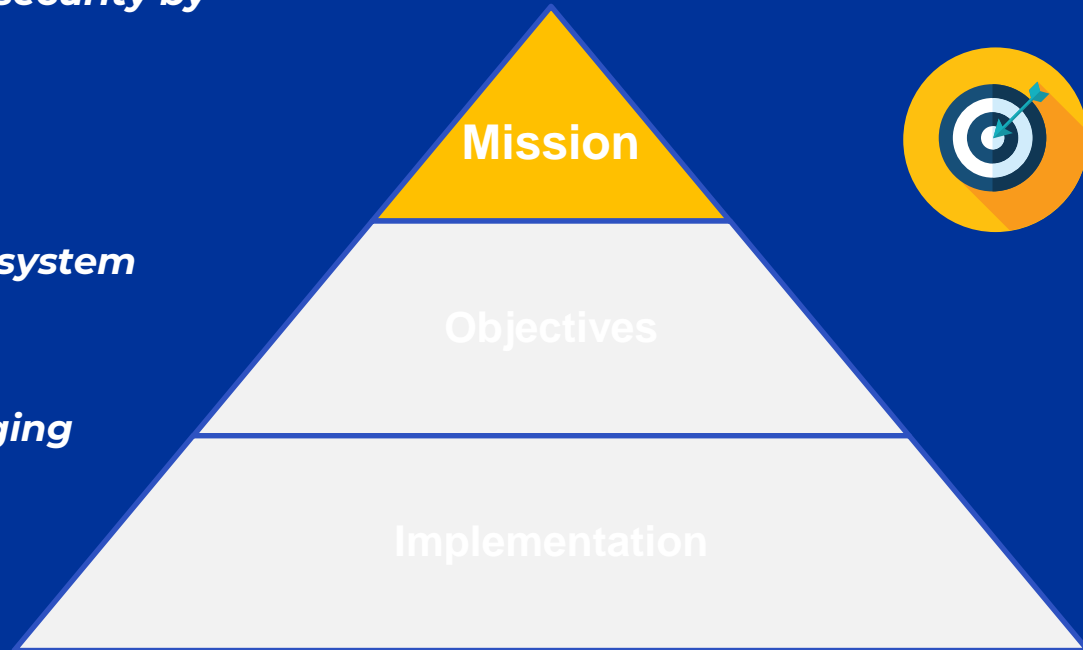
- *Facilitate the Network and Community to drive the cybersecurity technology agenda, building an inclusive and resilient stakeholder ecosystem*

- *Promoting research, innovation, deployment*

- *Enhancing cybersecurity capacities, capabilities, knowledge and infrastructures*



Mission

Objectives

Implementation

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE
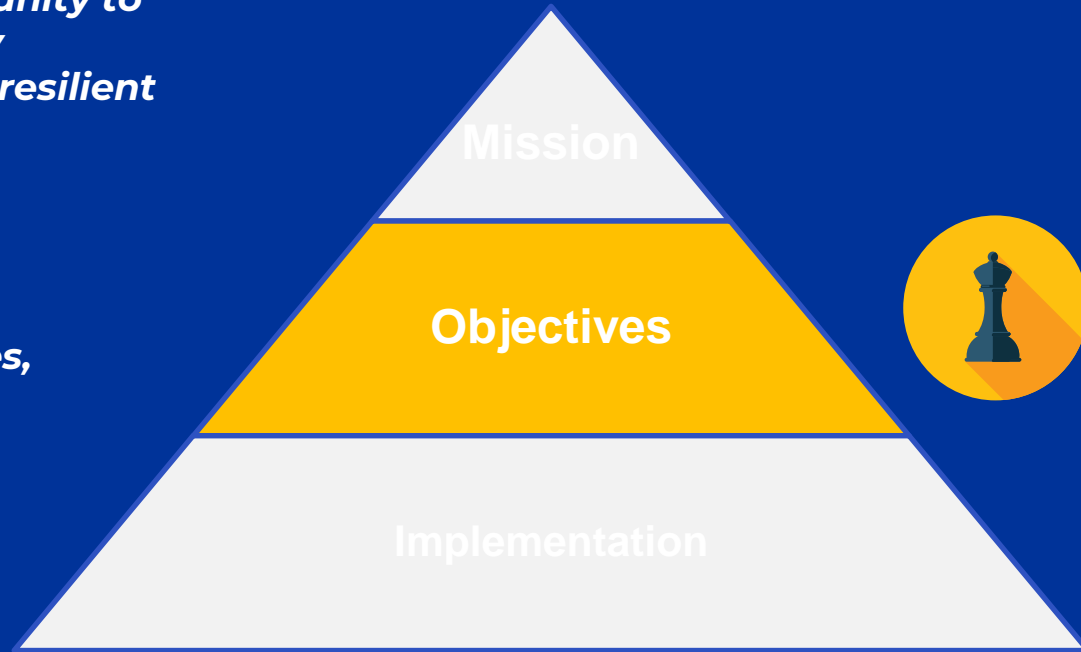
# ECCC – Overview (3/3)

- *Funds manager for cybersecurity in Digital Europe and Horizon Europe*

- *Strategic Agenda for research, innovation, deployment*

- *Support joint investment by the EU, Member States and industry*

- *Facilitating joint investment*

- *Voluntary national contributions*



Mission

Objectives

Implementation

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE
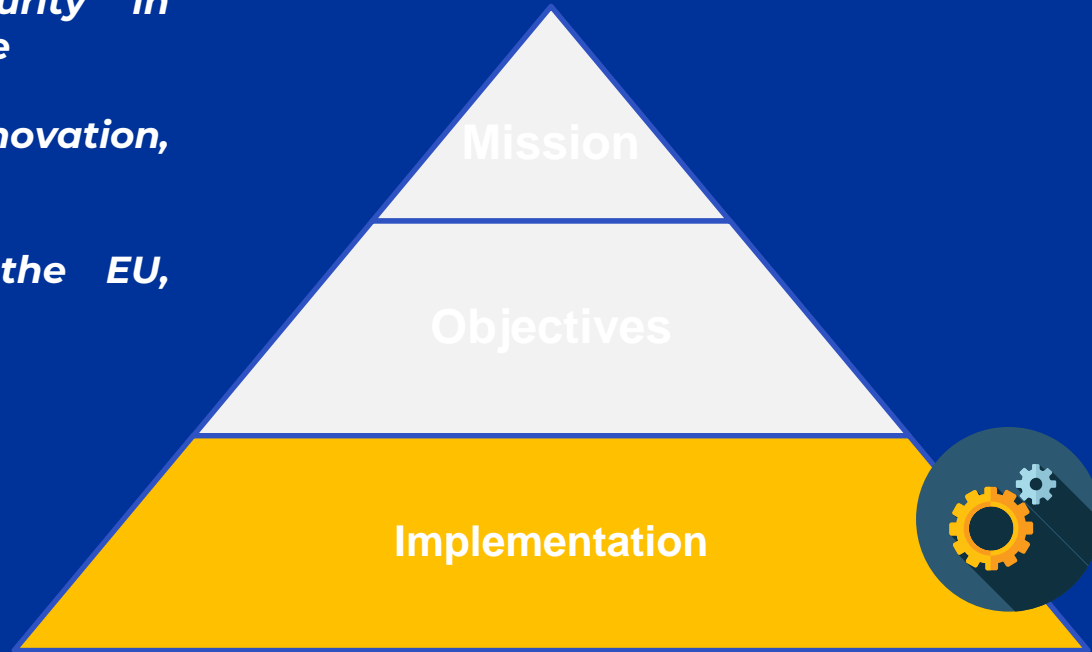
# ECCC – Strategic Agenda (2023 – 2027)

**The Agenda's goal is to create a unified and common vision to the EU investment in cybersecurity:**

Priorities and actions that are deemed of strategic importance in boosting cybersecurity innovation in Europe, while contributing to achieving the mission of ECCC:

| Support and grow the professional workforce | Strengthen R&D and innovation expertise | Support SMEs to develop and use strategic cybersecurity solutions |
|---|---|---|
| • Development of cybersecurity skills: education and professional training<br><br>• Cybersecurity skills framework and competence assessment | • Promoting post-quantum cryptography standardisation and adoption<br>• Support for EU Cybersec. Certification<br>• Promoting info-sharing | • Processes and tools for managing cybersecurity information and risk management<br>• Secure and resilient hardware and software systems |

**ECCC**
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

# The actors (2/3)

# National Coordination Centres (NCCs)

Nominated by Member States as the national contact point, and notified to the Commission (One NCC per Member State)

National capacity building: NCCs can effectively engage and coordinate with industry, academia and research community, citizens, and the public sector and authorities under NIS

NCCs may receive funding, may pass on financial support

- *Provides technical assistance*

- *Coordinates the national, regional and local levels*

- *Promotes cybersecurity educational programmes*

- *Advocates involvement of relevant entities*

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

List of confirmed NCCs available on-line : National Cybersecurity Coordination Centres (europa.eu)

# The Cybersecurity Competence Community

A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors.

✓ The Centre, Network and Community should help to advance and disseminate the latest cybersecurity products and services

✓ Provides input to the activities of the competence centre to the multiannual work programme and to the annual work programme

✓ Splits up into working groups for regular dialogue

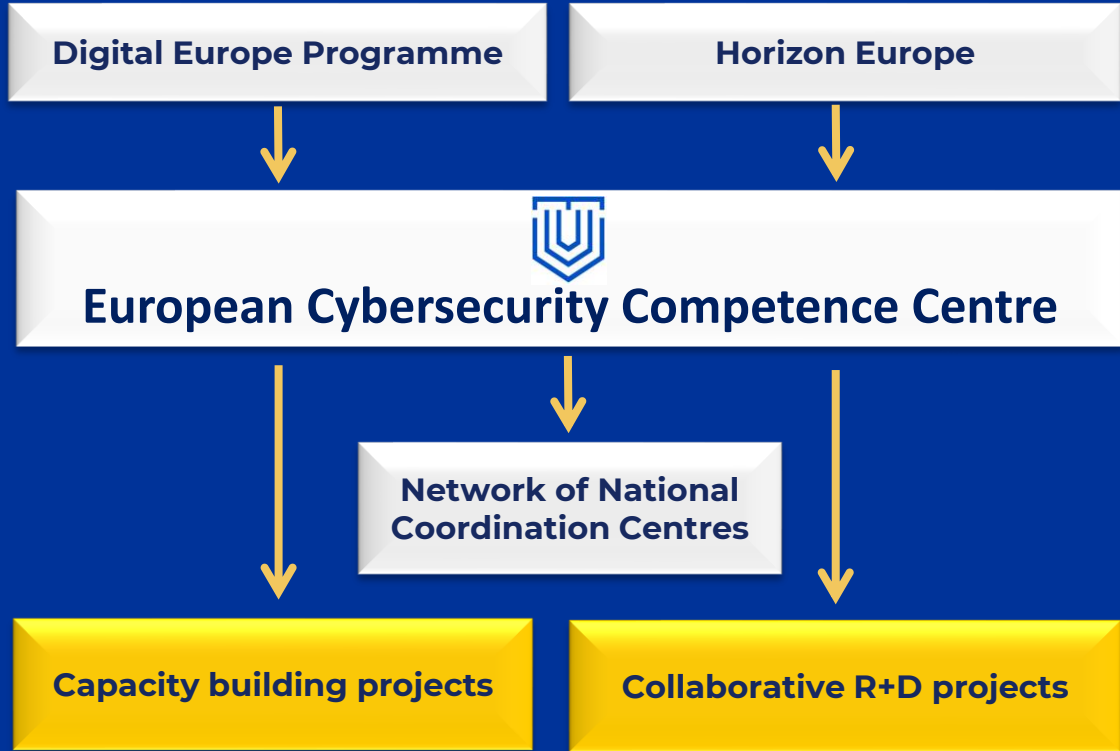✓ Supports stakeholders at their request, public-private coordination

# Proposed EU cybersecurity funding sources (2021-2027)

**Digital Europe Programme**

**Horizon Europe**

**European Cybersecurity Competence Centre**

Co-investment by industry on project basis

Subsidiary EFTA Contribution

Co-investment by Member States (voluntary)

**Network of National Coordination Centres**

**Capacity building projects**

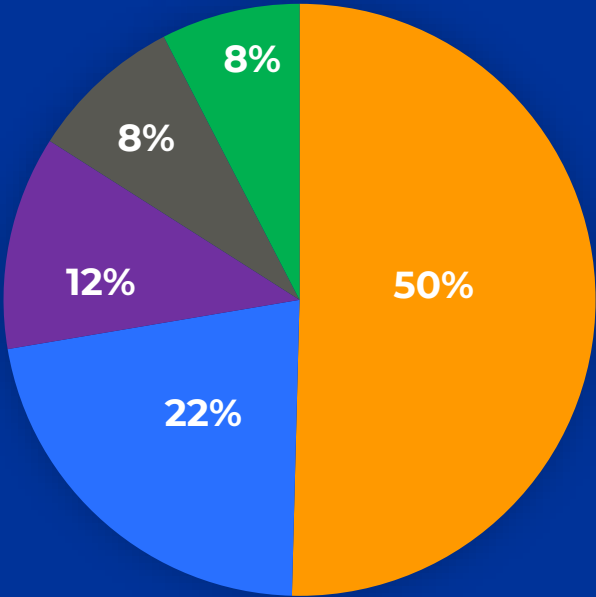**Collaborative R+D projects**

# Overall overview ECCC portfolio for DEP calls Cyber 02, 03, 03b, 04, 06: beneficiaries geographical distributions (coordinators and participants)
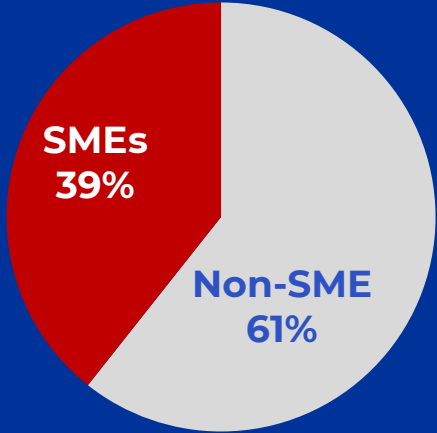


| Country | #Coordinators | #Partners | Total Beneficiaries |
|---|---|---|---|
| AT | 3 | 14 | 16 |
| BE | 6 | 46 | 52 |
| BG | 2 | 6 | 7 |
| CY | 6 | 51 | 56 |
| CZ | 5 | 9 | 13 |
| DE | 10 | 25 | 35 |
| DK | 2 | 2 | 3 |
| EL | 11 | 94 | 105 |
| ES | 14 | 23 | 27 |
| EE | 2 | 10 | 11 |
| FI | 3 | 4 | 5 |
| FR | 10 | 23 | 31 |
| HR | 6 | 11 | 14 |
| HU | 0 | 4 | 4 |
| IE | 6 | 8 | 14 |
| IS | 2 | 11 | 13 |
| IT | 10 | 34 | 44 |
| LT | 5 | 11 | 14 |
| LU | 9 | 13 | 17 |
| LV | 2 | 3 | 4 |
| MT | 2 | 3 | 4 |
| NL | 5 | 10 | 15 |
| NO | 5 | 9 | 13 |
| PL | 6 | 16 | 22 |
| PT | 6 | 14 | 17 |
| RO | 14 | 62 | 76 |
| SE | 4 | 7 | 11 |
| SI | 2 | 22 | 24 |
| SK | 15 | 6 | 21 |
| **Grand Total** | **136** | **550** | **686** |

# DEP – Cyber 02, 03, 04 – type of beneficiaries



Pie chart (left):
- Private for-profit: 50%
- Public bodies: 22%
- Higher or Secondary Education: 12%
- Other: 8%
- Research and Technology: 8%

Pie chart (right):
- SMEs 39%
- Non-SME 61%

# DEP call CYBER-06: sector type distribution of participants

| Sector Type | Number | Rate |
|---|---|---|
| Higher or Secondary Education | 14 | 7,5% |
| Other | 13 | 7,0% |
| Private for Profit | 122 | 65% |
| Public Body | 24 | 12,8% |
| Research Organisation | 14 | 7,5% |



7% 8% 7%

13%

7%

65%



Other 38,5%

SME 61,5%
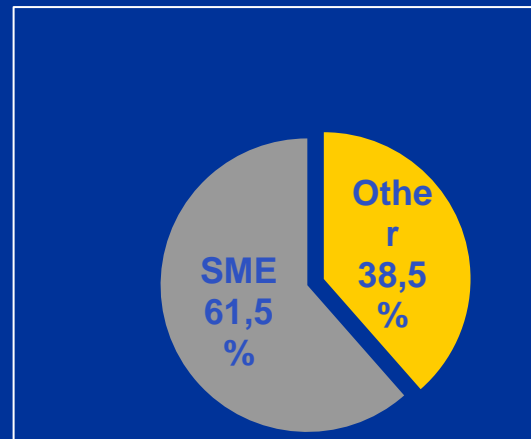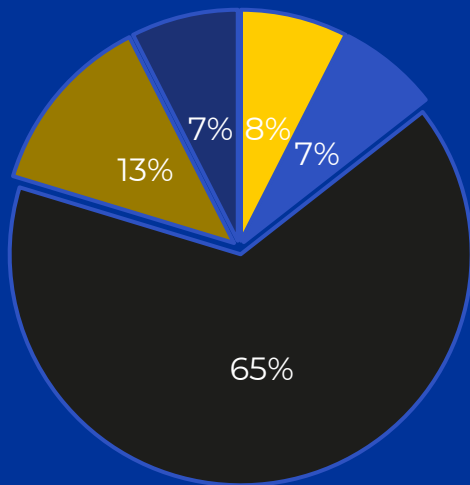
# Digital Europe Programme

The Digital Europe Programme will reinforce EU critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, governance and processing, the deployment of these technologies and their best use for critical sectors like energy, climate change and environment, manufacturing, agriculture and health.

The Digital Europe Programme is strategic in supporting the digital transformation of the EU industrial ecosystems

*(Digital Europe Work Programme 2021- 2022)*

# Topics call list

**DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC**

• National SOCs (Joint Procurement budget 15M€)

EUR 5.800.000

**DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT**

• Enlarging existing or Launching New Cross-Border SOC Platforms (Joint Procurement budget 17M€)

EUR 5.000.000

**DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS**

• Strengthening the SOC Ecosystem

EUR 2.000.000

**DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH**

• Development and Deployment of Advanced Key Technologies

EUR 35.000.000

**DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER**

• Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

EUR 35.000.000

**DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02**

• Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

EUR 20.000.000

# Timetable and deadlines

| | |
|---|---|
| **Call opening:** | **4 July 2024** |
| **Deadline for submission:** | **21 January 2025 –** <br> **17:00:00 CET (Brussels)** |
| **Evaluation:** | **February – March  2025** |
| **Information on evaluation results:** | **April – May 2025** |
| **GA signature:** | **October 2025** |

## National SOCs

### Objective:

- **Create or strengthen National SOCs**, in particular with state-of-the-art tools for monitoring, understanding and proactively managing cyber events, in close collaboration with relevant entities such as CSIRTs;

- **benefit from information and feeds from other SOCs in their countries and use the aggregated data and analysis to deliver early warnings to targeted critical infrastructures on a need-to-know basis**.

For this topics an expression of interest shall also be submitted no later than the 21 January 2025 at 17:00 Brussels time.
Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en.
Applications must be submitted in the correct form, duly completed and dated.

## Scope (1/2):

**The aim is capacity building for new or existing National SOCs.** This can include for example:

- automation, analysis and correlation tools and data feeds covering Cyber Threat Intelligence (CTI) at various levels ranging from field data to Security Information and Event Management (SIEM) data to higher level CTI;
- leverage state of the art technology such as artificial intelligence and dynamic learning of the threat landscape and context;
- use of shared cybersecurity information, to the extent possible based on existing taxonomies and/or ontologies, and hardware to ensure the secure exchange and storage of information;
- the operations should be built upon live network data. Where relevant, consideration should be given to SMEs as the ultimate recipients of cybersecurity operational information.

**Key elements:**
- ✓ translation of advanced AI/ML, data analytics and other relevant cybersecurity tools from research results to operational tools, and further testing and validating them in real conditions in combination with access to supercomputing facilities;
- ✓ knowledge transfer, such as training of cybersecurity analysis;
- ✓ National SOCs must share information with other stakeholders in a mutually beneficial exchange of information and commit to apply to participate in a cross-border SOC platform within the next 2 years, with a view to exchanging information with other National SOCs.

## Scope (2/2):

To support the activities in scope of a National SOC, the following two work streams of activities are foreseen:

**a)      [Procurement]**

A Joint Procurement Action with the Member State where the national SOC is located: this will cover the procurement of the main equipment, tools and services needed to build up the National SOC.

**b) [Building up and running the National SOC]**
A grant will also be available to cover, among others, the preparatory activities for setting up the National SOC, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the National SOC, e.g., using the equipment, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

- Applications shall be made to both work streams.
- Applications to the Call for Expression of Interest (CfEI) will be object of evaluations procedures.
- Grants will only be awarded to applicants that have succeeded the CfEI evaluation.

# DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC

- Indicative duration of the action: 36 Months

- Type of Action: Simple Grant — 50% funding rate

- Grant amount: between 1 and 2 million EUR

- Type of Beneficiaries: public bodies acting as National SOCs

The target stakeholders under a) **[Procurement]** and b) **[Building up and running the National SOC]** are public bodies acting as National SOCs linked to a "call for expression of interest to deploy and operate National SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU".

Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

## Enlarging existing or Launching New Cross-Border SOC Platforms

## Objective:

This action **aims at new cross-border SOC platforms, as well as enlarging those that were already launched under the previous** DIGITAL work programme (2021-2022).

While the main focus of this action is on processes and tools for prevention, detection and analysis of emerging cyber-attacks, it also **foresees in particular the acquisition and/or adoption of common (automation) tools, processes and shared data infrastructures for the management and sharing of contextualised and actionable cybersecurity operational information across the EU.**

In case of enlargement of an ongoing cross-border grant, the new consortium should be composed by the coordinator of the ongoing grant plus the new entities that want to join the cross-border SOC.

The new grant will work in close cooperation with the ongoing one.

For this topics an expression of interest shall also be submitted no later than the 21 January 2025 at 17:00 Brussels time.
Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en.
Applications must be submitted in the correct form, duly completed and dated.

## Scope:

- Supporting the development of better performing data analytics, detection, and response tools, through the pooling of larger amounts of data, including new data generated internally;
- act as a central point allowing for broader pooling of relevant data and CTI, enable the spreading of threat information on a large scale and among a large and diverse set of actors;
- enhancing and consolidating collective situational awareness and capabilities in detection and CTI;
- support common situational awareness and effective crisis management and response by providing relevant information to networks and entities responsible for cybersecurity operational cooperation and crisis management.

**Key elements:**
- ✓ for cross-border SOC platforms, there is a crucial need for novel tools based on advanced Artificial Intelligence and machine learning (AI/ML), data analytics and other relevant cybersecurity relevant technologies, based on research results and further tested and validated in real conditions, in combination with access to supercomputing facilities (e.g., to boost the correlation and detection features of cross-border platforms).

## Scope:

To support the above activities of a Cross-Border SOC platform, the following two workstreams of activities are foreseen:

**a) [Procurement]**
A Joint Procurement Action with the Member State participating in the Cross-Border SOC platform: this will cover the procurement of the main equipment, tools and services needed to build up the Cross-Border SOC platform.

**b)** [**Building up and running the Cross-Border SOC platform**]
A grant will also be available to cover, among others, the preparatory activities for setting up the Cross-Border SOC platform, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Cross-Border SOC platform, e.g., using the equipment, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

- Applications shall be made to both work streams.
- Applications to the Call for Expression of Interest (CfEI) will be object of evaluations procedures.
- Grants will only be awarded to applicants that have succeeded the CfEI evaluation.

- Indicative duration of the action: 36 Months

- Type of Action: Simple Grant — 50% funding rate

- Grant amount: Between 2 and 3 million EUR

- Type of Beneficiaries: Public bodies acting as National SOCs

The target stakeholders under a) **[Procurement]** and **b)** [**Building up and running the Cross-Border SOC platform**] above are public bodies acting as National SOCs linked to a "call for expression of interest to deploy and operate Cross-border SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU".

Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

## Scope:

**Applicants to the call for expressions of interest should describe:**

- the aims and objectives of the National/Cross-Border SOC platform,

- its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders,

- the detailed planning of the activities and tasks of the National/Cross-Border SOC platform,

- the services it will offer,

- the way they will operate and be operationalised,

- the duration of the activity as well as the main milestones and deliverables.

**They should also specify what equipment, tools and services need to be jointly procured and integrated to build up the National/Cross-Border SOC platform, its services and its infrastructure.**

## Strengthening the SOC Ecosystem

### Objective:

- It will **empower SOCs which are linked to National SOCs, and to a stronger collaboration between local SOCs, National SOCs and Cross-Border SOC platforms**, leading to an increased data sharing and better detection capability for cyber threats.

- **Foster interoperability**, identifying what data can be shared, how this is shared and in what format, requirements and sharing agreements, and ways to enable better exchange.

- **Increased engagement**, including from the private sector, and to a better collaboration towards a common EU cyber threat knowledge base and technological independence.

- **Develop a comprehensive governance framework, with for example enrolment conditions and vetting procedures**. The aim is to foster discussion between such platforms, sharing best practices and identifying opportunities for collaboration.

✓ Links to the actions funded under the Cybersecurity Skills Academy (in the main Digital Europe work programme) can also be envisaged.

✓ One Coordination and support action will be selected, bringing together the largest possible network of National and Cross-Border SOC platforms.

European Commission

## Scope:

Actions should address one or more of the following actions:

- **foster the collaboration and interconnection** between Cross-Border SOC platforms and National SOCs, as well as fostering the link between National SOCs and other SOCs at national level;
- support the **cooperation and coordination of Cross-Border SOC platforms**, both between different Cross-Border SOC platforms, and with relation to national SOCs and other SOCs;
- foster links between public sector and industry, and stimulate **mutually beneficial exchange of information, tools and data as well as exchange of knowledge and training opportunities;**
- **foster links between SOCs and industrial stakeholders in artificial intelligence** and in other enabling technologies, fostering the adoption of such technologies;
- **engage stakeholders from the HPC stakeholder community and practitioners of breakthrough AI technologies, to develop a blueprint for the requirements of AI models that necessitate access to large or smaller HPC facilities**.

ENISA is tasked to develop guidelines on the **interoperability** of Cross-Border Cyber Hubs.
Therefore, the selected proposal shall be required to collaborate with ENISA on the aspect of the interoperability.

# DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS

- Indicative duration of the action:          36 Months

- Type of Action:          Coordination and Support Actions — 100% funding rate

- Grant amount:          #1 proposal for up to 2 million EUR

- Type of Beneficiaries:          National SOCs, Cross-Border SOC Platforms and other relevant stakeholders

## Development and Deployment of Advanced Key Technologies

## Objective:

- The objective is to enable European cybersecurity actors to **take advantage of new breakthroughs in *key digital technologies*** *(such as Artificial Intelligence Big Data Analytics, Quantum, Blockchain Technology, High Performance Computing and Software-Defined Networking)* **improving detection and prevention capabilities, efficiency, scalability, and facilitating data sharing and regulatory compliance.**

- In particular innovative technologies should allow for the **processing of larger amounts of data, automating real-time pattern recognition, log analysis, vulnerability scanning,** while enabling security professionals to focus on **higher level interpretation of data and response decisions**.

A priority is to create and strengthen capacity for original Cyber Threat Information (CTI), e.g., in the form of CTI feeds or services.

European Commission

## Scope:

Activities should fortify cybersecurity capabilities using breakthrough technologies, encompassing various aspects of cybersecurity. In one or more of the following topics should be addressed:

- **Real-time Monitoring and Incident Response**

- **Malware Defence and Analysis**

- **Proactive Vulnerability Management**

- **Data Protection and Anomaly Detection**

- **Incident investigation**

- **Data Utilisation with Privacy**

✓ The systems, tools and services developed under this topic, where relevant, will be made available for licencing to National and/or Cross-Border SOC platforms under favourable market conditions.

✓ The deployment of such technologies must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.

European Commission

- Indicative duration of the action: 36 Months

- Type of Action: SME Support Actions — 50% and 75% (for SMEs) funding rate

- Grant amount: Between 3 and 5 million

- Type of Beneficiaries:

  - ✓ Technology companies, especially SMEs, working to provide and support other private and public organisations with cyber threat detection and CTI feeds.

  - ✓ Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

## Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

## Objective:

- Complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, in particular for large industrial installations and infrastructures, by assisting Member States in their efforts to **improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise;**

- creation of platforms that serve as a reference point and provide services such as penetration testing and threat assessments for providers of essential services and critical infrastructures, as well as other actors.

- Preparedness actions should benefit entities in sectors indicated as critical infrastructure sectors in NIS2
- This involves data and operational measure regarding cybersecurity, including penetration tests and exploitable vulnerabilities

## Scope:

The provision of preparedness support services (ex-ante) shall include activities reported below, addressing for example large industrial installations or infrastructures, operators of essential services, digital service providers and governmental entities:

**Support for testing for potential vulnerabilities:**

- Development of penetration testing scenarios.
- Support for conducting testing of EE operating CI for potential vulnerabilities.
- Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises Evaluation and/or testing of MS cybersecurity capabilities.
- Consulting services.

**Support for threat assessment and risk assessment:**

- Threat Assessment process implementation and life cycle.

- Customised risk scenarios analysis.

**Risk monitoring service:**

- Specific continuous risk monitoring such as attack surface monitoring, risk.
- Monitoring of assets and vulnerabilities.

# DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- Indicative duration of the action:       36 Months

- Type of Action:                                    Grants for Financial Support — 100% funding rate

- Grant amount:                                      Between 3 and 5 million EUR

- Type of Beneficiaries:
  - ✓ This topic targets in particular industrial players, national cybersecurity authorities, national cybersecurity competence centres, National Coordination Centres (as defined in Regulation (EU) 2021/887), private entities and any other relevant stakeholders with the capacity to aggregate demand from end beneficiaries, to launch tenders for procurement in the cybersecurity market space and to run downstream calls for allocating Financial Support to Third Parties.
  - ✓ Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

## Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

## Objective:

Proposals should contribute to achieving at least one of these objectives:

- Development of trust and confidence between Member States.

- Supporting market surveillance authorities/notifying authorities/national accreditation bodies to **implement the CRA.**

- **Effective operational cooperation** of organisations entrusted with EU or Member State's national level cybersecurity, in particular cooperation of CSIRTs, or cooperation of OSE including public authorities.

- **Better security and notification processes** and means for Essential and Important Entities in the EU, including cross-border (automated) incident notification systems.

- **Better reporting of cyber-attacks to law enforcement authorities** in line with the Directive on attacks against information systems.

- Improved security of network and information systems in the EU.

- **More alignment of Member States' implementations of NIS2**.

- **Support cybersecurity certification in line with the amended Cybersecurity Act.**

**Scope:** The action will focus on the support of at least one of the following priorities:

- Implementation, validation, piloting and **deployment of technologies**, tools and IT-based solutions, processes and methods **for monitoring and handling cybersecurity incidents.**

- **Increasing capacity** for market surveillance authorities/notifying authorities/national accreditation bodies in view of tasks as provided by the **CRA**.

- **Collaboration, communication, awareness-raising, knowledge exchange and training, on the implementation of NIS2.**

- **Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies for** effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.

- Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs.

- Ensure that manufacturers improve the security of products with digital elements and enhance **the transparency of security properties** of products with digital elements. **Facilitate compliance for hardware and software producers.**

- Enable **businesses across all sectors and consumers to use products with digital elements securely.**

- **Support to Cybersecurity certification.**

- Indicative duration of the action:       36 Months

- Type of Action:       Simple Grants — 50% funding rate

- Grant amount:        Between 2 and 4 million

- Type of Beneficiaries:

  - ✓ This topic targets relevant industrial stakeholders, including SMEs and start-ups in the scope of the upcoming CRA, concerned by the NIS2 Directive or that may benefit from the European cybersecurity certification schemes. It refers also to Member State competent authorities, which play a central role in the implementation of the NIS2 Directive, CSIRTs - including sectorial CSIRTs, SOC, OES, DSP, ISACs, actors that play a role in the implementation of the Cyber Resilience Act (including certification bodies), and any other actors within the scope of the legislations mentioned above.

  - ✓ Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

# Specific topics conditions

**All topics are subject to the provisions of article 12(5) of the Digital Europe Programme Regulation.**

- For the topics:
  - ✓ SOC - National SOC
  - ✓ SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms
  - ✓ KEYTECH - Development and Deployment of Advanced Key Technologies
  - ✓ LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

**following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment** *(see section 10).*

- For the topics:
  - ✓ SOCSYS - Strengthening the SOC Ecosystem
  - ✓ CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

**following reimbursement option for equipment costs applies: depreciation only** *(see section 10)*

# Awards criteria

**Relevance**
- Alignment with the objectives and activities
- Contribution to long-term policy and strategic objectives
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*

**Implementation**
- Maturity of the proposed action
- Soundness and efficiency of the implementation plan
- Capacity of the applicants or consortium to carry out the proposed work

**Impact**
- Achievement of the expected outcomes and deliverables, as well as communication and dissemination
- Competitiveness strengthen and contribution to society

*<u>Not applicable for topics:</u>  NATIONAL SOCs, SOCPLAT, SOCSYS.
*<u>Applicable only for the topics:</u>  KEYTECH, LARGEOPER, CYBERSEC-02

A. Personnel costs - average personnel costs (unit cost according to usual cost accounting practices)

- A.1 Employees
- A.2 Natural persons under direct contract
- A.3 Seconded persons
- A.4 SME owner/natural person unit cost

B. Subcontracting costs - restrictions due to security:

- <u>Subcontracting should constitute only a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities)</u>
- Subcontracted work must be performed in the eligible countries
- Only costs for activities carried out in eligible countries are eligible

C. Purchase costs

- C.1 Travel and subsistence (only actual costs)
- C.2 Equipment (depreciation)
- C.3 Other goods, works and services

D. Other cost categories

- D.1 Financial Support to Third Parties:
  - ***compulsory only for topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER*** *; (max. 60k, at least 50% project budget and co-financed 50%)*
  - *not allowed for the other topics.*
- D.2 Internally invoiced goods and services

# References

**Digital Europe Programme website** : https://digital-strategy.ec.europa.eu/en/activities/digital-programme

**Digital Europe Programme Regulation:** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1621344635377

**Funding & tender opportunities portal:** https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital

**Call document:** call-fiche_digital-eccc-2024-deploy-cyber-07_en.pdf (europa.eu)

DIGITAL
EUROPE
PROGRAMME

European
Commission

# Cluster 3: Civil Security for Society

Destination
"Increased cybersecurity and a more secure online environment"

CALL "INCREASED CYBERSECURITY" (CS)

HORIZON-CL3-2024-CS-01

# Destination "Increased cybersecurity and a more secure online environment (CS)"

➢ **Expected impact of the Horizon Europe Strategic Plan 2021-2024:**

- *Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats.*

➢ **Specific impacts:**

- **Generate knowledge and value** in cross-cutting matters in order to avoid sector-specific bias and to **break silos** that impede the proliferation of common security solutions;

- **Strengthen key pillars** of the research and innovation cycle to increase the effectiveness and efficiency of its contribution to the development of security capabilities;

- **Support innovation uptake and go-to-market strategies** with the aim of paving the way towards an increased industrialisation, commercialisation, adoption and deployment of successful outcomes of security research, thus contributing to reinforce the competitiveness of EU security industry and safeguard the security of supply of EU products in key security areas.

European Commission

# Destination "Increased cybersecurity and a more secure online environment (CS)"

- **CL3 Increased Cybersecurity:**
  - Will support the implementation of the **EU Cybersecurity Strategy.**
  - Will support the Regulation of the European Parliament and of the Council establishing the **European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)** and the Network of **National Coordination Centre (NCC)** (COM 2018(630))
  - Supported by R&I, citizens, public authorities and companies, including SMEs, will be empowered to **protect their data and online activities**, via a resilient critical digital infrastructure, both private and public, that better protects the Digital Single Market and the digital life of citizens against malicious cyber activities.
  - Will strengthen European cybersecurity industrial capacities, supply chain security and increased open strategic autonomy vis-à-vis foreign technologies.
  - Will support the use of **innovative digital technologies**, including self-healing, artificial intelligence, cryptography, massively distributed computing and storage, as well as quantum technologies to increase data security and augment cybersecurity.
  - Will support innovations in secure hardware and software development and implementation and improve methods for cybersecurity testing and certification

# Destination "Increased cybersecurity and a more secure online environment (CS)"

➢ All these measures aim at **defending the integrity of the Digital Single Market** as well as the EU's high standards concerning rights to privacy, protection of personal data, and the protection of other fundamental rights in the digital age on the global stage.

➢ The Destination will pay particular attention to the **cybersecurity of the most vulnerable organisations and individuals**.

➢ In order to defend against cyber-threats, the architectural principles of **'security-by-design' and 'privacy-by-design' will be implemented in digital technologies and their applications**, such as 5G, industry 4.0, artificial intelligence, Internet of Things, block chain, quantum technologies, mobile devices and connected cooperative and autonomous mobility and energy.

➢ Complementary Instrument: **Digital Europe Programme** (which focuses more on the industry side).

➢ Related policy areas: Quantum research, Cryptography, Support for cyber capacities and deployment, European Cybersecurity Competence Centre, NIS2 Directive, 5G, AI, Cyber Resilience Act, Cybersecurity Act, Cyber Solidarity Act, Certification, EU Cybersecurity Skills Academy, CyberCommunity

# Overview

| Topic | Instrument | EUR (million) | Projects | Opening date | Deadline date |
|---|---|---|---|---|---|
| **Increased Cybersecurity (CS)** | | | | | |
| **CS01 - Approaches and tools for security in software and hardware development and assessment** | | | | | |
| HORIZON-CL3-2024-CS-01-01 | IA | 37,00 | 6 | 27/06/2024 | 20/11/2024 |
| **CS02 –Post-quantum cryptography transition** | | | | | |
| HORIZON-CL3-2024-CS-01-02 | RIA | 23,40 | 4 | 27/06/2024 | 20/11/2024 |

# Destination
# "Increased Cybersecurity (CS)"

## CALL TOPICS 2024

# HORIZON-CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment

➢ **Projects' results are expected to contribute to some or all of the following outcomes**:

- Improved hardware and software security engineering; resilient systems design;

- Improved access to testing of hardware and software in virtual, closed and secure environments;

- Systematic and, where possible, automated study of vulnerabilities, software analysis, vulnerability discovery, and dynamic security assessment;

- Trustworthy certifiable hardware and software;

- AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks.

European Commission

# HORIZON-CL3-2024-CS-01-02: Post-quantum cryptography transition

➢ **<u>Projects' results are expected to contribute to some or all of the following outcomes:</u>**

- Increasing the maturity of current post-quantum cryptographic algorithms and contribution to further standardisation;

- Easy-to-use tools for the large-scale implementation of post-quantum cryptographic algorithms, based on state-of-the-art standards;

- Secure and efficient transition from pre- to post-quantum encryption through tools implementing a hybrid approach combining recognised pre-quantum public key algorithms and additional post-quantum algorithms;

- Phase-in of post-quantum algorithms or protocols to new or existing applications;

- Demonstrators and good-practice implementations of post-quantum cryptographic algorithms on varied hardware and software platforms;

- Application-oriented recommendations for the widespread implementation of post-quantum cryptography across the EU.

# General conditions for call: Increased Cybersecurity 2023 (HORIZON-CL3-2023-CS-01)

**General conditions**

**1. Admissibility conditions:** described in Annex A and Annex E of the Horizon Europe Work Programme General Annexes

**2. Eligible countries:** described in Annex B of the Work Programme General Annexes

A number of non-EU/non-Associated Countries that are not automatically eligible for funding have made specific provisions for making funding available for their participants in Horizon Europe projects. See the information in the Horizon Europe Programme Guide.

**3. Other eligibility conditions:** described in Annex B of the Work Programme General Annexes

**4. Financial and operational capacity and exclusion:** described in Annex C of the Work Programme General Annexes

**5. Award criteria, scoring and thresholds** are described in Annex D of the Work Programme General Annexes

**6. Submission and evaluation processes** are described in Annex F of the Work Programme General Annexes and the Online Manual

**7. Indicative timeline for evaluation and grant agreement:** described in Annex F of the Work Programme General Annexes

**8. Legal and financial set-up of the grants:** described in Annex G of the Work Programme General Annexes

European Commission

# Additional documents

✓HE Main Work Programme 2023–2024 – 1. General Introduction

✓HE Main Work Programme 2023–2024 – 6. Civil Security for Society

✓HE Main Work Programme 2023–2024 – 13. General Annexes

✓ HE Programme Guide

✓HE Framework Programme and Rules for Participation Regulation 2021/695

✓HE Specific Programme Decision 2021/764

✓EU Financial Regulation

# 2024 Horizon Implementations Days

**(**remote only, no need to register**)**

**Grant Agreement Preparation in Horizon Europe**
**Date:** 16 October 2024, 09:30h to 12:45h (CEST, Brussels Time)
**Event Website:** [Horizon Implementation Day: Grant Agreement Preparation in Horizon Europe (16 October 2024) (europa.eu)](#) (remote only, no need to register)

**Lump Sum Funding in Horizon Europe: How does it work? How to write a proposal?**
**Date:** 17 October 2024, from 10:00h to 12:00h (CEST, Brussels time)
**Event website:** [Lump Sum Funding in Horizon Europe: How does it work? How to write a proposal? (17 October 2024) (europa.eu)](#) (remote only, no need to register)

**Grant Management in Horizon Europe**
**Date:** 05 November 2024, 09:30h to 13:00h (CEST, Brussels Time)
**Event Website:** [Horizon Implementation Day: Grant Management in Horizon Europe (05 November 2024) (europa.eu)](#)

European Commission

# Q&A

DEP questions: dep@eccc.europa.eu
HE questions: Research Enquiry Service

# Keep in touch

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

**Thank you!**

Europe digitally secured