Digital Europe Programme

Cybersecurity

Research to Reality - Brussels

06/02/2024

F
r
a

Francesco Barbato
Head of Sector
DG CNECT H1
European Commission

#DigitalEuropeProgramme

the Cybersecurity Work programme

Focus of this presentation:

- Amended DEP Cybersecurity Work Programme 2023-2024
- The Open Call
- Outlook on future DEP and Horizon Europe Calls

DIGITAL EUROPE PROGRAMME CYBERSECURITY INFO DAY

- Info Day, Bucharest 22nd February

https://cybersecurity-centre.europa.eu

DIGITAL-ECCC-2024-DEPLOY-CYBER-06, currently open

TOPIC	Title	Type of Action	Open Date	Deadline	Budget
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH	Novel applications of AI and Other Enabling Technologies for Security Operation Centres	Simple grant	16/01/2024	26/03/2024	30 M EUR
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA	Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations	Grant for Support to Third Parties	16/01/2024	26/03/2024	22 M EUR
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA	Tools for compliance with CRA requirements and obligations	SME support action grants	16/01/2024	26/03/2024	8 M EUR
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY	Deployment of Post Quantum Cryptography in systems in industrial sectors	Simple grants	16/01/2024	26/03/2024	22.25 M EUR
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC	Standardisation and awareness of the European transition to postquantum cryptography	Coordination and support action grant	16/01/2024	26/03/2024	1 M EUR
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-TRANSITIONEUPQC	Roadmap for the transition of European public administrations to a post-quantum cryptography era	Coordination and support action grant	16/01/2024	26/03/2024	0.75 M EUR

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH - Novel applications of AI and Other Enabling Technologies for Security Operation Centres (1/4)

Objectives:

- Deployment of Artificial Intelligence and Advanced Key Technologies as enablers for SOCs
- Tools for creation, analysis and processing of CTI that allow for faster and more scalable SOC operations
- Original European CTI feeds or services

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH - Novel applications of AI and Other Enabling Technologies for Security Operation Centres (2/4)

Scope

Activities should include at least one of the following:

- Continuous detection of patterns and identification of anomalies that indicate potential threats, recognising new attack vectors and enabling advanced detection in an evolving threat landscape.
- Creation of CTI based on novel threat detection capabilities.
- Enhancing speed of incident response through real-time monitoring of networks to identify security incidents and generating alerts or triggering automated responses.
- Mitigating malware threats by analysing code behaviour, network traffic, and file characteristics, reducing the window of opportunity for attackers to exploit malware.
- Identification and management of vulnerabilities.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH - Novel applications of AI and Other Enabling Technologies for Security Operation Centres (3/4)

Scope II

- Recovery from incidents through self-healing capacities.
- Reducing the chances of attacks and pre-emptively identifying weaknesses through automated vulnerability scanning and penetration testing.
- Protecting sensitive data through the analysis of access patterns and detection of abnormal behaviour.
- Enabling organisations to leverage and share CTI and other actionable information for analysis and insights without compromising data security and privacy, through anonymisation and de-identification. Tool and service providers are welcome to apply to this topic, also when in a consortium with National SOCs. Links with stakeholders in the area of High-Performance Computing should be made where appropriate, as well as activities to foster networking with such stakeholders.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH - Novel applications of AI and Other Enabling Technologies for Security Operation Centres (4/4)

Indicative duration of the action:	3 Years
Indicative budget:	EUR 30 MEUR
Type of Action:	Simple Grant
Type of Beneficiaries:	Technology providers, operators of SOCs, and other relevant stakeholders

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA - Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations (1/4)

Objectives:

- Support micro and small SMEs and other stakeholders for CRA compliance.
- Deliver an openly available platform with CRA-related resources (such as guidelines and supporting documents), providing supporting community building and upskilling
- Workshops, events, networking and exchange of experience of stakeholders
- Contributions to CRA standardisation

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA - Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations (2/4)

Scope

The proposed project should include actions addressing the following:

- Awareness raising, dissemination and other stakeholder engagement actions with the focus on the cascade financing to European SMEs, with a focus on micro and small enterprises.
- Managing an open call process to distribute cascade funding, including impartial evaluation of proposals and monitoring the implementation of grants.
- Establish an openly available platform providing links to CRA-related resources that the proposed project itself would collect or develop or which would be available from external sources and supporting community building and upskilling. This includes for example a dedicated central repository website to allow easy finding of internal and external resources, step-by-step guidelines, compliance tools, training materials, free and open-source code implementations, and other relevant resources to achieve CRA compliance. This should include, amongst others, tools procured for this purpose under this work programme.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA - Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations (3/4)

Scope Part II

- In close coordination with the EU Cybersecurity Skills Academy, perform trainings and upskilling of stakeholders to achieve CRA compliance, i.e. organise workshops, training sessions, and events, draft guidelines, supporting actions to facilitate interaction among European SMEs, including drafting reports or other material discussing the implementation of CRA compliance requirements and promoting awareness, including by contributing to relevant deliverables of standardisation bodies e.g. through a sectoral perspective and informed by the needs of companies on the ground.
- Facilitate and share CRA compliance best-practices and use-cases.
- Contribute to standardisation efforts, as appropriate, considering the activities of European and international standardisation that are directly relevant to the CRA implementation.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA - Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations (4/4)

● Indicative duration of the action:	36 Months
● Indicative budget:	EUR 22 MEUR
● Type of Action:	Grant for Support to Third Parties
● Type of Beneficiaries:	All stakeholders

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA - Tools for compliance with CRA requirements and obligations (1/3)

Objectives:

- Tools to simplify and automate CRA compliance, with particular focus towards automated compliance tools that would ensure alignment with the CRA cybersecurity essential requirements.
- Tools to simplify and automate CRA compliance documentation obligations.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA - Tools for compliance with CRA requirements and obligations (2/3)

Scope:

CRA compliance solutions are foreseen based either on technical specifications, training modules, and/or other relevant material. Tools for penetration testing, testing facilities and other cybersecurity practices, aligning with CRA requirements, are also in the scope.

Tools should be tailored towards needs of European SMEs, with a focus on micro and small enterprises, though also usable by broader stakeholder categories, such as:

- Manufacturers of relevant product categories falling within the scope of the CRA, including software developers.
- Others, such as distributors, importers, open-source community, etc.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA - Tools for compliance with CRA requirements and obligations (3/3)

● Indicative duration of the action:	12-18 Months
● Indicative budget:	EUR 8 MEUR
● Type of Action:	SME support action grants
● Type of Beneficiaries:	Technology providers

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY - Deployment of Post Quantum Cryptography in systems in industrial sectors (1/3)

Objectives:

- The adoption of PQC in industrial sectors like automotive, automation, finance, control systems or energy.
- To seamlessly integrate PQC systems, equipment, components, protocols,
- Long-term protection of critical assets, long-term information security and operational continuity
- Migration checklists and plans for PQC in sectors where this has not yet taken place.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY - Deployment of Post Quantum Cryptography in systems in industrial sectors (2/3)

Scope:

Proposals should focus on the integration of a standardised PQC protocol into the digital security and communication networks in the automotive, automation, finance, or energy sector, while taking into account specific needs of the sector, such as necessary keys strength and keys management. Proposals should cover the development or adaptation of the required software/hardware and the validation of the solution in a large-scale demonstrator.

Successful consortia are expected to raise awareness on the need to transition to PQC and share their experience and best practice.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY - Deployment of Post Quantum Cryptography in systems in industrial sectors (3/3)

● Indicative duration of the action:	Up to 36 Months
● Indicative budget:	22.25 MEUR
● Type of Action:	Simple grants
● Type of Beneficiaries:	Industry actors and related stakeholders

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC -Standardisation and awareness of the European transition to post-quantum cryptography (1/3)

Objectives:

- Contributions to European and international standards and regulations in PQC.
- Workshops, white papers and other activities to support synergies between different sectors transition to PQC.
- A European PQC migration roadmap, which can be the basis for sector-specific roadmaps.
- Actions supporting the European PQC community.
- Development of standards for hybrid cryptographic systems (pre- and postquantum encryption systems) for encryption, key encapsulation mechanisms, digital signatures, etc. and for the PQC integration in the existing digital infrastructure.
- Support for participation of relevant European experts in European and international cross-topical standardisation bodies in order to integrate PQC whenever new cryptographic standards are developed or existing ones are updated especially for critical sectors like energy, transport, health, and finance.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC -Standardisation and awareness of the European transition to post-quantum cryptography (2/3)

Scope:

Proposals are expected to engage in concrete standardisation efforts within both European and international standardisation forums, where PQC will play a pivotal role in the near future and where progress in standardisation will augment existing cybersecurity capabilities and create a competitive edge upon Europe. Also, in alignment with projects resulting from the topic "Transition to QuantumResistant Cryptography" (call HORIZON-CL3-2022-CS-01-03) and the topic Deployment of PostQuantum Cryptography (PQC) systems in industrial sectors (in this work programme), the proposals will incorporate practical strategies to coordinate and synergise European research and innovation endeavours with PQC standardisation initiatives.

To this end, proposals should establish a proactive presence and take on leadership roles in orchestrating and shaping international standards and regulations for PQC. This can either be in existing standardisation activities and bodies or, where relevant, by contributing to creating new standardisation activities in existing groups and/or creation of new groups.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC -Standardisation and awareness of the European transition to post-quantum cryptography (3/3)

Indicative duration of the action:	Up to 36 Months
Indicative budget:	1 MEUR
Type of Action:	Coordination and support action grant
Type of Beneficiaries:	Stakeholders in the field of cryptography, PQC and/or standardisation

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-TRANSITIONEUPQC - Roadmap for the transition of European public administrations to a post-quantum cryptography era (1/3)

Expected Outcome

- Roadmap for the transition of European public administration for PQC
- Workshops, white papers and other activities to support synergies between national security agencies and public administrations.
- Collaborations between public administrations regarding the transition to PQC.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-TRANSITIONEUPQC - Roadmap for the transition of European public administrations to a post-quantum cryptography era (2/3)

Scope

Proposals should bring together national security agencies, relevant public administrations and related stakeholders including experts in the area of PQC. Activities should be foreseen to engage stakeholders to efficiently coordinate their efforts at national and European level in order to achieve impactful outcomes leading to the adoption of PQC in European public administrations.

The roadmap should identify what encryption systems need to be replaced, what algorithms should be adopted, priorities for defending against quantum attacks across the spectrum of public administrations, and legal and technical aspects of the transition to PQC. It should foster collaborations and exchange of best practice.

This action aims at the transition of public administration towards a new paradigm that is set to be a game changer in encryption, which directly involves national security as it relates to information that must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk.

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-TRANSITIONEUPQC - Roadmap for the transition of European public administrations to a post-quantum cryptography era (3/3)

Indicative duration of the action:	Up to 36 Months
Indicative budget:	0.75 MEUR
Type of Action:	Coordination and support action grant
Type of Beneficiaries:	National Security Agencies and related stakeholders

Upcoming Calls – DIGITAL EUROPE PROGRAMME

TOPIC	Title	Type of Action	Open Date	Deadline	Budget
DIGITAL-ECCC-2024-DEPLOY-NCC-06	Deploying The Network of National Coordination Centres with Member States	Simple Grant	14/02/2024*	14/05/24 and 14/10/24*	65 M EUR
	Call for Expression of Interest on National SOCs	Join Procurement and Simple Grant	May 2024*		20.8 M EUR
	Call for Expression of Interest for Enlarging existing or Launching New Cross-Border SOC Platforms	Joint Procurement and Simple Grant	May 2024*		22 M EUR
	Support to EU cybersecurity legislation (2024)	Simple Grant	July 2024*	November 2024*	20 M EUR

*dates to be confirmed

Upcoming Calls – HORIZON EUROPE

TOPIC	Title	Type of Action	Open Date	Deadline	Budget
HORIZON-CL3-2024-CS-01-01	Approaches and tools for security in software and hardware development and assessment	IA	27/06/24	20/11/24	37 M EUR
HORIZON-CL3-2024-CS-01-02	Post-quantum cryptography transition	RIA	27/06/24	20/11/24	23.40 M EUR

Info Days

DIGITAL EUROPE PROGRAMME CYBERSECURITY INFO DAY

- Info Day, Bucharest 22nd February

https://cybersecurity-centre.europa.eu

DIGITAL EUROPE PROGRAMME

European Commission

Thank you!