SIX DIGITAL CALLS - Topic descriptions

”Topic descriptions” have been downloaded 2024-06-11 from the following link:

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/calls-for-proposals?callIdentifier=DIGITAL-ECCC-2024-DEPLOY-CYBER-07&isExactMatch=true&status=31094501,31094502&frameworkProgramme=43152860&order=DESC&pageNumber=1&pageSize=50&sortBy=startDate

Contents

Development and Deployment of Advanced Key Technologies

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

Topic description

ExpectedOutcome:

- Deployment of state-of-the-art technologies in the area of cybersecurity
- Tools for automated threat detection, monitoring of networks, data protection and incident response

Objective:

Breakthroughs in Key Digital Technologies such as Artificial Intelligence (including generative AI and adversarial AI), Big Data Analytics, Quantum, Blockchain Technology, High Performance Computing and Software-Defined Networking, create new opportunities for advancing cybersecurity in the areas of vulnerability detection, threat detection and rapid response, reducing the window of opportunity for attackers to exploit these vulnerabilities. Furthermore, they may enable new possibilities to protect data security and privacy.

The objective is to enable European cybersecurity actors to take advantage of these new breakthroughs, 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. They should allow organisations to deploy solutions and larger scale, and in increasingly complex environments.

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

Scope:

Activities should fortify cybersecurity capabilities using breakthrough technologies, encompassing various aspects of cybersecurity. This involves uptake and integration for the deployment of novel tools, systems and services for threat detection, incident response, malware defence, vulnerability management, data protection and so forth. In one or more of the following topics should be addressed:

- Real-time Monitoring and Incident Response: ensuring the swift identification and response to security incidents through continuous network monitoring, alert generation, and automated response mechanisms.
- Malware Defence and Analysis: mitigating malware threats by analysing code behaviour, scrutinizing network traffic, and assessing file characteristics, thereby reducing opportunities for attackers to exploit vulnerabilities.
- Proactive Vulnerability Management: identifying and addressing weaknesses proactively through automated vulnerability scanning and penetration testing to address potential threats before they can be exploited.
- Data Protection and Anomaly Detection: safeguarding sensitive data by scrutinizing access patterns and identifying abnormal behaviour to mitigate data breaches and protect critical information.
- Incident investigation to help uncover cause, scope and impact of security incidents or breaches that have occurred.
- Data Utilisation with Privacy: enabling organisations to harness data for analysis and insights while preserving data security and privacy through techniques such as anonymisation and de-identification.

By addressing such issues, the cybersecurity resilience of organisations should be enhanced, improving overall cybersecurity posture, encompassing various aspects such as threat detection, incident response, and vulnerability management.

In well justified cases, access requests to the EuroHPC high performance computing infrastructure could be granted.

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.

This action aims at the deployment of key technologies in cybersecurity, in particular also in the context of securing national authorities, providers of critical infrastructures and essential services. As this involves the handling of cyber incidents, malware and management of vulnerabilities that could be exploited by malicious actors, the deployment of such technologies must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, 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. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

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

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

Topic description

ExpectedOutcome:

- preparedness support services
- threat assessment and risk assessment services
- risk monitoring services

Objective:

This mechanism aims to 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.

Scope:

The provision of preparedness support services (ex-ante) shall include activities listed 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. The proposed scenarios may cover Networks, Applications, Virtualisation solutions, Cloud solutions, Industrial Control systems, and IoT.
- Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.

- Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises such as the development of standardised cyber-ranges or other testing facilities, able to mimic features of critical sectors (e.g., energy sector, transport sector etc.) to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant.
- Evaluation and/or testing of MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents).
- Consulting services, providing recommendations on how to improve infrastructure security and capabilities

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.

Preparedness actions should benefit entities (including SMEs and start-ups) in sectors indicated as critical infrastructure sectors in NIS2 (Directive (EU) 2022/2555), such as energy, transport and banking, and entities in other relevant sectors.

This action aims at the 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. This involves data and operational measure regarding cybersecurity, including penetration tests and exploitable vulnerabilities. Such information could be exploited by malicious actors, and thus it must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, 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. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

Strengthening the SOC Ecosystem

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

Topic description

ExpectedOutcome:

- Events, workshops, stakeholder consultations, architectural designs and white papers on technical coordination and interconnection support platforms.

- Stronger links between public sector and industry SOCs
- Technical frameworks to allow for information exchange between SOC platforms
- A blueprint for the use of HPC facilities for the benefit of SOCs

Objective:

This topic complements other actions in this and the previous Work Programme, which are building up National SOCs and Cross-Border SOC platforms. 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. This should in particular 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. Links to the actions funded under the Cybersecurity Skills Academy (in the main Digital Europe work programme) can also be envisaged.

These actions should lead to increased engagement, including from the private sector, and to a better collaboration towards a common EU cyber threat knowledge base and technological independence.

Additionally, Cross-Border SOC Platforms will 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.

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

Scope:

Actions should address one or more of the following:

- Activities and technical frameworks that 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.
- Actions that 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.
- Actions to 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.
- Actions to foster links between SOCs and industrial stakeholders in artificial intelligence and in other enabling technologies, fostering the adoption of such technologies, including AI techniques and tools rand facilitating getting acquainted with existing state of the art tools (such as for example those developed in Action 1.1.4 of this work programme) and knowledge exchange.
- Actions to 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, and next steps to make this happen, as well as raising awareness of this in the wider SOC community.

These actions aim at creating or strengthening national and/or cross-border SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, 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. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694.

National SOCs

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

Topic description

ExpectedOutcome:

- World-class National SOCs across the Union, strengthened with state-of-the-art technology, acting as clearinghouses for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses.
- Threat intelligence and situational awareness capabilities and capacity building supporting strengthened collaboration between cybersecurity actors, including private and public actors.

Objective:

The objective is to 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. They will also, where possible, 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.

Scope:

The aim is capacity building for new or existing National SOCs, e.g., equipment, tools, data feeds, as well as costs related to data analysis, interconnection with Cross-Border SOC platforms, etc. 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. National SOCs should also leverage state of the art technology such as artificial intelligence and dynamic learning of the threat landscape and context. This also includes the 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.

A key element is the 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 (e.g., to boost the correlation and detection features of cross-border platforms).

Another key role for National SOCs is knowledge transfer, such as training of cybersecurity analysts. For example, SOCs dealing with critical infrastructures play a key role and should benefit from the knowledge and experience acquired by or concentrated in National SOCs.

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.

To achieve this aim, a call for expression of interest will be launched to select entities in Member States that provide the necessary facilities to host and operate National SOCs. Applicants to the call for expressions of interest should describe the aims and objectives of the National SOC, describe its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the National SOC, the services it will offer, the way they will operate and be operationalised, and describe 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 procured and integrated to build up the National SOC, its services and its infrastructure.

To support the above activities of a National SOC, the following two workstreams of activities are foreseen:

- [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
- [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 workstreams. Applications will be object of evaluations procedures. Grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

These actions aim at creating or strengthening national SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, 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. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

Enlarging existing or Launching New Cross-Border SOC Platforms

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

Topic description

ExpectedOutcome:

- World-class cross-border SOC platforms across the Union for pooling data on cybersecurity threat between several Member States, equipped with a highly secure infrastructures and advanced data analytics tools for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses.
- Sharing of Threat Intelligence between National SOCs, and information sharing agreements with competent authorities and CSIRTs.

Objective:

The general objective of cross-border SOC platforms is to strengthen capacities to analyse, detect and prevent cyber threats and to support the production of high-quality intelligence on cyber threats, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention capabilities in a trusted environment.

This action aims at new cross-border SOC platforms, as well as supporting 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.

Scope:

Cross-border SOC platforms will contribute to enhancing and consolidating collective situational awareness and capabilities in detection and CTI, 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 by the consortia members.

The platforms should 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 (e.g., CERTs/CSIRTs, ISACs, operators of critical infrastructures).

Also, 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).

The platforms will 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 at Union level, without undue delay, where they obtain information related to an ongoing large-scale, cross-border incident, or to a major threat or a major vulnerability likely to have significant cross-border impacts or significant impacts on services and activities falling within the scope of the Directive (EU) 2022/2555.

A call for expression of interest will be launched to select entities in Member States that provide the necessary facilities to host and operate Cross-Border SOC platforms for pooling data on cybersecurity threat between several Member States. Applicants to the call for expressions of interest should describe the aims and objectives of the Cross-Border SOC platform, describe its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the Cross-Border SOC platform, the services it will offer, the way they will operate and be operationalised, and describe 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 procured and integrated to build up the Cross-Border SOC platform, its services and its infrastructure.

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

- [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.
- [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 workstreams. Applications will be object of evaluations procedures. Grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

These actions aim at creating or strengthening cross-border SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, 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. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

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

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

Topic description

ExpectedOutcome:

- Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
- Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States.
- Organisation of events, workshops, stakeholder consultations and white papers.
- Enhanced cooperation, preparedness and cybersecurity resilience in the EU.
- Support actions and cooperation for further advanced of cybersecurity certification.
- Effective supervision and enforcement of the CRA by the market surveillance authorities and adequate capabilities of notifying authorities and national accreditation bodies for the implementation of the CRA.

Objective:

The action focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity in particular the NIS2 Directive (Directive (EU) 2022/2555), the Cybersecurity Act, and

the Directive on attacks against information systems (Directive 2013/40). It complements the work of SOCs in the area of threat detection. It is a continuation of work currently supported under the previous Digital Work Programme.

In addition, this action also aims at supporting the implementation of the proposed Cyber Resilience Act (CRA) by market surveillance authorities/notifying authorities/national accreditation bodies, by increasing their capacities to ensure effective implementation of the CRA.

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 (including in relation to the CSIRT Network) or cooperation of Operators of Essential Services 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 (Directive (EU) 2022/2555).
- Support cybersecurity certification in line with the 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 activities, knowledge exchange and training, including through the use of cybersecurity ranges, of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555).
- Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies, tools, processes and methods 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 since the design and development phase and throughout the whole life cycle.

- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers.
- Enhance the transparency of security properties of products with digital elements.
- Enable businesses across all sectors and consumers to use products with digital elements securely.
- Support to Cybersecurity certification, including support to national cybersecurity certification authorities and other relevant stakeholders, such as SMEs. This includes activities such as threat-led penetration testing, acquiring certification testbeds, sharing best practices, implementing innovative evaluation methods for specific ICT products or components.

Proposals may target, where relevant, Member State competent authorities, which play a central role in the implementation of NIS2 (Directive (EU) 2022/2555), as well as other actors within the scope of this Directive.

Proposals may support, amongst others, the continuation of cybersecurity activities funded through the CEF Telecom programme, building where relevant on the results from the CEF projects.

Proposals may support, amongst others, for the onboarding to the CEF Cybersecurity Core Service Platforms of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555) and are potential contributors to the goals of the CEF Cybersecurity Core Service Platform.

This action seeks to support the European cybersecurity posture by creating a European ecosystem of companies and organisations that will support the implementation of EU cybersecurity legislation that will contribute to strengthening the European capacities in protecting the cyberspace. The results from the work carried out in the projects funded under this action may include implementation, validation, piloting and deployment of technologies, tools and IT-based solutions, processes and methods for monitoring and handling cybersecurity incidents involving cybersecurity of providers of essential services and critical infrastructures, as well as other actors. As previously noted, 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. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.
