Open Call guidelines for applicants

Project: CYberSynchrony- Harmonising People, Processes & Technology for Robust Cybersecurity,
Grant Agreement Number: 101158555

https://cybersynchrony.eu/open-calls/

Funding Authority: European Union - Horizon Europe Framework Programme (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)

Call Identifier: DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST

Date: 19-02-2026 – Version 6.0

Please carefully read this guide before submitting your application.

This document provides essential guidelines and detailed instructions for applicants interested in applying to the CYberSynchrony Open Calls for Financial Support to Third Parties (FSTP). It also contains valuable information related to the applicants who are interested in joining our external evaluators' team.

Funded by the European Union

CYberSynchrony project has received funding by the European Union's Digital Europe programme under Grant Agreement no. 101158555

Disclaimer

This document may contain material that is copyright of certain CYberSynchrony beneficiaries and may not be reproduced or copied without permission. All CYberSynchrony partners (*Table 1*) have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Table 1 CYberSynchrony Participants list

Number	Role	Short name	Legal name	Country
1	COO	MAG	MAGGIOLI SPA	IT
2	BEN	eBOS	EBOS TECHNOLOGIES LIMITED	CY
3	BEN	IANUS	IANUS TECHNOLOGIES LTD	CY
4	BEN	TRUST	TRUSTILIO BV	NL
5	BEN	UPRC	UNIVERSITY OF PIRAEUS RESEARCH CENTER	GR
6	BEN	DSA	ARCHI PSIFIAKIS ASFALEIAS	CY
7	BEN	KETYAK	ETHNIKI YPIRESIA PLIROFORION	GR
8	BEN	FP	FOCAL POINT	BE
9	BEN	BYTE	BYTE COMPUTER ANONYMI VIOMICHANIKI EMPORIKI ETAIREIA	GR
10	BEN	EGL	DIMOS EGALEO	GR
11	BEN	MER	MERIDIAN SRL	IT
12	BEN	AMC	SAMOUTIS KAI SYNERGATES IEPE	CY

The information in this document is provided "as is" and no guarantee or warranty is given that fits for any particular purpose. The user thereof uses the information at its sole risk and liability. Moreover, it is clearly stated that the CYberSynchrony consortium reserves the right to update, amend or modify any part, section or detail of the document at any point in time without prior information. The CYberSynchrony project, funded from the European Union's DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST. Call foresees as an eligible activity the provision of financial support to third parties, as a mean to achieve its own objectives.

LEGAL NOTICE

The information and views set out in this document are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Project number: 101158555
Project name: Harmonizing People, Processes, and Technology for Robust Cybersecurity
Project acronym: CYberSynchrony
Call: DIGITAL-ECCC-2023-DEPLOY-CYBER-04
Topic: DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST
Type of action: DIGITAL-JU-GFS
Service: ECCC
Project starting date: fixed date: 1 June 2024
Project duration: 36 months

Contents

1. Overview 5
1.1. Submission Platform 5
1.1.1. For Open Call Applicants (proposal submission): 5
1.1.2. For External Evaluators (application to join the evaluator pool): 5
1.1.3. Further information 6
2. Brief description of the CYberSynchrony Open Calls 6
2.1. Open Call 1: Infrastructure Resilience & Operational Readiness 6
2.2. Open Call 2: Compliance, Innovation & Regulatory Advancement 7
2.3. Open Call 3: Mutual Assistance & Cyber Collaboration Among Member States 7
2.4. CYberSynchrony objectives 8
3. Funding details and Participation Rules 8
3.1. Reallocation of Remaining Funds and Reserve List 9
3.2. Eligible Cost Types (as part of Lump Sum) 10
3.3. Payment Modalities 10
3.3.1. Proposed Payment Structure 10
3.3.2. Coordination and Internal Fund Distribution 11
4. Duration and Possible Time Extensions 11
5. Eligible Applicants per Open Call 11
6. Proposal Evaluation Criteria 13
6.1. Scoring Scale and Threshold 13
6.2. Ranking and Tie-breaking Rules 14
6.3. Final Selection 14
6.4. Redress process 14
7. Proposal structure 15
8. Intellectual property rights (IPR) and results ownership 17
9. Conflict of Interest Rules 18
9.1. Open call applicants 18
9.2. External Evaluators 18
10. Sub-grant Agreement 18
10.1. Information on which documentation is mandatory to be submitted, and which should be taken into consideration 19
11. Core CYberSynchrony Modules 20
11.1. CYRESCUE – Resilience and Incident Response 20

11.2. CYBERRA – Threat Intelligence and Risk Analysis..... 21
11.3. CYBRITE – Continuous Monitoring and Early Threat Detection.....22
11.4. CROSS-CORE – Cross-Border Coordination and Secure Information Exchange 22
11.5. CYBERWISE – Cybersecurity Awareness and Behavioural Training.....23
11.6. CYBERGOPLUS – Governance, Standards, and Regulatory Compliance ... 24
12. Access to CYberSynchrony Public Deliverables 24

List of Changes

No of change	Section	Change	Implementation date
		VERSION 2.0	
1	V2.0: Section 11	Minor changes regarding the description of the CYberSynchrony modules	08-01-2026
		VERSION 3.0	
2	V3.0: Section 5	Private research institutes are added as eligible partners for OC1	09-02-2026
		VERSION 4.0	
3	V4.0: Section 5	Eligible countries list clarified – Since Objective 3 which is related to Cybersecurity calls excludes specific countries as defined in the DEP.	13-02-2026
		VERSION 5.0	
4	V5.0: Section 3	Section 3.2: The sentence: "Not provided by the CYberSynchrony consortium", was changed to "Expertise not provided by the consortium of the proposal" Section 3.2: The following sentence was also added: "Indirect costs 25% must also included – for more details check the proposal template"	17-02-2026
5	V5.0: Section 5	Table 5: During change no2, and for OC1, SMEs were accidentally deleted from private organisations: The revised and correct sentence is: "and private organisations [research, SMEs] operating within the NIS2 sectors"	
6	V5.0: Section 7	In Table 7 (Implementation plan section), and to be consistent with the mandatory deliverables given in the proposal template, it was added the "Detailed implementation/financial plan" (M1)	
7	V6.0: Section 5	Table 5: For OC1, and OC2, NGOs were also added as eligible partners. For OC3 – Mutual Assistance & Cyber Collaboration Among Member States, to assist the applicants, more clarifications were given regarding the entities' eligibility	19-02-2026

1. Overview

CYberSynchrony delivers an integrated, modular cybersecurity framework, combining advanced threat intelligence, automated response systems, and secure channels for cross-border collaboration:

a. Support rapid detection and mitigation of cyber incidents, continuous risk monitoring, and effective information sharing between Member States and key stakeholders.
b. Emphasise on fostering a cybersecurity-aware environment, offering targeted training, awareness campaigns, and practical tools that support organisations in aligning with evolving regulatory requirements (i.e. NIS2 Directive).

Through its 3.55m € Open Call (which will comprise 3 different open calls), CYberSynchrony invites SMEs, innovators, and specialised teams to contribute tools, services, and practices that can enhance the project's platform and expand its applicability across different sectors. This financial support mechanism offers the opportunity to integrate new capabilities into real-world pilots, ensuring the solutions developed are practical, scalable, and relevant to the security needs of Europe's digital infrastructure.

For more information regarding the CYberSynchrony's modules and architecture, please refer to section 12.

Open Call submissions – Timeline

CYberSynchrony will launch the calls together with all necessary documentation (templates, guidelines, submission platform, etc), on the **1st of January 2026**. All three Open calls will run simultaneously, whilst they will remain for proposal submissions for a period of two months. Therefore, all interested applicants must submit their completed applications no later than the **1st of March 2026, 17:00 CET**.

The rest of the dates regarding periods related to proposal evaluation, contract signing, and Open call projects starting dates, are given on the CYberSynchrony's website:

https://cybersynchrony.eu/open-calls/

External evaluators applications – Timeline

The CYberSynchrony project is looking to form a team of external evaluators to review the submitted Open Call proposals. The call for external evaluators will have a starting date which will be the **1st of January 2026** and the interested applicants must submit their completed applications no later than the **15th of February 2026, 17:00 CET.**

The rest of the dates regarding periods related to selection of the right candidates, contract signing period, and evaluation start/end dates, are given on the CYberSynchrony's website:

https://cybersynchrony.eu/external-evaluators-team/

1.1. Submission Platform

All Open Call Applicants (FSTP) and External Evaluators must use the CYberSynchrony dedicated online platform for their respective submissions/applications.

Platform link: https://cybersynchrony.grantplatform.com , ***Registration required***

1.1.1. For Open Call Applicants (proposal submission):

Proposals must be submitted exclusively through the platform. Applicants may edit their proposal after initial submission; however, no further changes will be possible after the submission deadline. Submissions sent by any other means (e.g., email) will not be accepted for evaluation.

1.1.2. For External Evaluators (application to join the evaluator pool):

Applications must be submitted exclusively through the platform. Evaluators may edit their application after initial submission; however, no further changes will be possible after the application deadline and the submission process will be locked.

1.1.3. Further information

All call-related documentation and supporting material, including detailed guidance on platform access, account creation, and step-by-step instructions for both Open Call Applicants and External Evaluators, is available at the dedicated CYberSynchrony Open Calls webpage: https://cybersynchrony.eu/open-calls/

This webpage also includes a YouTube tutorial demonstrating how to use the platform to (i) submit an Open Call (FSTP) application and (ii) apply as an external evaluator. Users are encouraged to review the available material and register on the platform early, well in advance of the applicable deadlines.

All deadlines are based on the **official platform server time (CET)**. Submissions/applications are deemed received only when successfully submitted and **time-stamped by the server**. The user's local device time, time zone settings, or location will not be taken into account.

It is strongly recommended not to wait until the last minute to submit the proposal. Failure of the proposal to arrive in time for any reason, including network communications delays or working from multiple browsers or multiple browser windows, is not acceptable as an extenuating circumstance. The time of receipt of the application as recorded by the submission system will be definitive.

2. Brief description of the CYberSynchrony Open Calls

The CYberSynchrony project will launch **three open calls** under its Financial Support to Third Parties (FSTP) scheme. These calls are designed to bring in external expertise, services, and tools to reinforce key aspects of the project platform and to support cybersecurity deployment across NIS2 sectors. The total available budget for FSTP is **€3,550,000**, and no third party may receive more than **€200,000 in total**, even if selected under multiple calls. Each third party can participate in only one proposal per call.

Each call supports a defined set of **specific topics**; their brief description is given below. In case of tools/solutions/models developed throughout the duration of the FSTP projects, these are expected to reach TRL 7.

2.1. Open Call 1: Infrastructure Resilience & Operational Readiness

Scope

This call targets the enhancement of cybersecurity infrastructure and operational readiness specifically within sectors governed by the NIS2 Directive—energy, transport, drinking water supply and distribution, and manufacturing. It supports solutions aimed at improving sector-specific resilience against cyber threats and enabling rapid, coordinated responses.

Priority Areas (all priority areas must be met)

1. **Strengthening Sector-specific Cybersecurity Operations:** Support initiatives that establish or amplify operational cybersecurity hubs tailored to the unique needs of energy, transport, water supply, and manufacturing sectors, ensuring sector-specific threat intelligence gathering, rapid incident response, and best practice sharing.
2. **Enhanced Threat Intelligence and Risk Assessment for NIS2 Domains:** Channel funds towards projects that aim to develop or adapt advanced threat intelligence platforms specific to the challenges of energy, transport, drinking water, and manufacturing sectors. Focus on real-time monitoring, predictive analytics, and proactive threat hunting tailored to the infrastructures of these domains.
3. **Promotion of Cybersecurity Awareness in NIS2 Sectors:** Fund campaigns and training programs tailored to professionals and stakeholders in the energy, transport, water, and manufacturing sectors. Promote best practices, risk mitigation, and cybersecurity hygiene specific to each sector's challenges and requirements.
4. **Supporting Cross-sector Collaborations:** Encourage projects that foster inter-sector collaboration, ensuring best practices in one domain (e.g., energy) can be shared and adapted for others (e.g., transport or water supply).

Linked CYberSynchrony Objectives (see section 2.4): #1, #3, #6, #7, #8
Mandatory KPIs to be defined by the applicants (additional KPIs may be defined):

- Number of essential entities supported
- Number of threat assessments/risk scenario analyses carried out
- Number of risk monitoring services provided

2.2. Open Call 2: Compliance, Innovation & Regulatory Advancement

Scope

This call addresses the regulatory landscape and supports innovative cybersecurity solutions specifically tailored for sectors covered by the NIS2 Directive—energy, transport, drinking water supply and distribution, and manufacturing.

Priority Areas (all priority areas should be met)

1. **Encouraging Regulatory Compliance in NIS2 Sectors:** Dedicate funding to support initiatives focusing on achieving and maintaining compliance with cybersecurity regulations specific to energy, transport, water supply, and manufacturing sectors within the EU.
2. **Boosting Innovations Tailored to NIS2 Domains:** Support research and development projects addressing the unique cybersecurity challenges and needs of the specified sectors. This includes creating sector-specific tools, technologies, and strategies ensuring a secure operational environment.
3. **Promotion of Cybersecurity Awareness in NIS2 Sectors:** Fund campaigns and training programs tailored to professionals and stakeholders in the energy, transport, water, and manufacturing sectors. Promote best practices, risk mitigation, and cybersecurity hygiene specific to each sector's challenges and requirements.
4. **Supporting Cross-sector Collaborations:** Encourage projects that foster inter-sector collaboration, ensuring best practices in one domain (e.g., energy) can be shared and adapted for others (e.g., transport or water supply).

Linked CYberSynchrony Objectives (see section 2.4): #6, #8, #9
Mandatory KPIs to be defined by the applicants (additional KPIs may be defined):

- Number of penetration tests provided
- Number of essential entities supported
- Number and nature of vulnerabilities discovered

2.3. Open Call 3: Mutual Assistance & Cyber Collaboration Among Member States

Scope

In an era where cybersecurity threats transcend borders, the collaboration between Member States (MS) is pivotal. This Open Call seeks to foster a more integrated and united approach to cybersecurity, emphasizing mutual assistance, best practice sharing, and coordinated response mechanisms among MS.

Priority Areas (Proposals must clearly address at least one of the listed priority areas and detail how the initiative will enhance mutual assistance among Member States)

1. **Establishing Unified Threat Intelligence Platforms:** Develop or enhance platforms that facilitate real-time sharing of threat intelligence between MS, ensuring a collective response to emerging cyber threats.
2. **Joint Cybersecurity Exercises & Training:** Organize joint cybersecurity exercises simulating cross-border incidents, aiming to test and improve the collective response capabilities of MS. Promote training sessions where MS can share their unique experiences, tools, and best practices, ensuring that all states benefit from individual advancements.
3. **Incident Response Coordination:** Create or amplify mechanisms that enable rapid coordination between MS when a cybersecurity incident impacts multiple countries. Develop shared playbooks

and protocols to guide coordinated responses, ensuring faster containment and mitigation of threats.

Linked CYberSynchrony Objectives (see section 2.4): #2, #4, #5

Mandatory KPIs to be defined by the applicants (additional KPIs may be defined):

- Number of potential number of users covered per test/ exercise
- Number of cross-border actions/exercises

2.4. CYberSynchrony objectives

Each FSTP application is mandatory to be aligned with some of the project's objectives, according to which open call the applicant wishes to submit to (1, 2 or 3). The objectives that the FSTP projects should be aligned with, are mentioned in Sections 2.1 (Open call 1), 2.2 (Open call 2) and 2.3 (Open call 3).

OBJ1: Improve threat and risk assessment through the use of advanced threat intelligence platforms, analytics tools, and risk assessment methods. The objective is to enable more accurate detection and proactive mitigation of cyber threats targeting essential services and digital infrastructure

OBJ2: Minimize the duration and impact of cyber incidents by integrating orchestration and automation into incident response coordination. This includes automating repetitive tasks and streamlining workflows to improve containment speed and efficiency

OBJ3: Strengthen risk monitoring and early incident detection using advanced cybersecurity analytics. This includes analysing network activity, software integrity, user behaviour, and system performance to identify anomalies and potential threats

OBJ4: Enhance mutual assistance among Member States and enable more realistic and frequent cross-border cyber exercises through the deployment of virtual cyber range platforms that simulate complex cyberattack scenarios and behavioural challenges

OBJ5: Ensure data privacy and secure communication during information sharing between Member States by establishing an encrypted and standardised communication infrastructure for threat intelligence, incident data, and best practices

OBJ6: Foster collaboration and knowledge sharing among stakeholders in the cybersecurity ecosystem by enabling real-time exchange of information and experiences to collectively strengthen cyber capabilities across the EU

OBJ7: Enhance early detection and response to cyber incidents by leveraging advanced threat intelligence and analytics while reducing the impact of potential cyber threats on critical infrastructure and essential entities

OBJ8: Promote cybersecurity awareness and behavioural change by implementing educational programs, training activities, and awareness campaigns targeting citizens, organisations, and businesses to cultivate a security-conscious society

OBJ9: Ensure high and consistent levels of cybersecurity across the EU by promoting comprehensive policies, supporting regulatory alignment, encouraging standardisation and certification, and facilitating dissemination and training across sectors

3. Funding details and Participation Rules

All financial support will be provided in the form of **lump sum grants**, in accordance with Article 6 of the Horizon Europe Model Grant Agreement. Funding is not based on reimbursement of actual costs but on the successful completion of predefined technical milestones and deliverables.

As no differentiation is made by entity type in the Grant Agreement, the funding scheme applies **equally to all beneficiaries**, regardless of their legal status (e.g., SMEs, research centres, higher education institutions, non-profit organisations, public entities, individuals). Applicants are required to define a realistic work plan and budget in line with the applicable funding caps described in Tables 1, 2, and 3.

The CYberSynchrony project allocates **€3,550,000** under the Financial Support to Third Parties (FSTP) mechanism, divided across three open calls. Financial support is granted in the form of **lump sum payments**, disbursed upon successful delivery of predefined outputs (deliverables), rather than based on actual incurred costs. Applicants must comply with the funding conditions defined in **Table 2, Table 3, and Table 4**.

Table 2 Main funding rules

Rule	Provision
Maximum funding per third party	€200,000 (across all open calls combined)
Proposal limit per each call	One proposal per third party
Multiple participations in the same Open Call	Disqualifies all such proposals
Funding scheme	Lump sum, tied to output verification

Table 3 Funding Range by Open Call according to consortium size, total budget allocation and estimated no. of proposals

Open Call	Consortium size	Min–Max funding	Total Budget Allocation	Estimated Number of Funded Proposals
Call 1 – Infrastructure & Operations	Single Entity Consortium (2 or 3)	€65,000 – €200,000 €100,000 – €200,000	€1,200,000	6–9 proposals
Call 2 – Compliance & Innovation	Single Entity Consortium (2 or 3)	€70,000 – €200,000 €120,000 – €200,000	€1,200,000	6–9 proposals
Call 3 – Cross-border Coordination	No single entity is allowed Consortium (2 or 3)	€100,000 – €200,000	€1,150,000	6–9 proposals

Table 4 shows the caps on specific expense categories. Participants should pay attention to these limits so that none is exceeded. For each call, the consortium should justify expenses in all 3 categories, but keeping in mind the budget limits showed in Table 2 and Table 3.

Table 4 Thematic Sub-caps per Open Call

Call	Activity Type	Maximum Allowed
Call 1	Infrastructure & Operational Set-up	€ 120,000
	Threat Intelligence Platform Development/adaptation	€ 65,000
	Incident Response Mechanisms	€ 55,000
Call 2	Regulatory Compliance Initiatives	€ 90,000
	R&D for Cybersecurity Challenges	€ 80,000
	Development of Sector-specific Tools & Strategies	€ 70,000
Call 3	Threat Intelligence Platforms (Cross-border)	€ 100,000
	Joint Exercises and training	€ 80,000
	Incident Response Coordination	€ 70,000

3.1. Reallocation of Remaining Funds and Reserve List

In cases where an open call concludes with unallocated funds—either due to undersized budgets of selected proposals or an insufficient number of qualifying applications—the remaining budget will not be discarded. Instead, residual funds from all open calls will be consolidated into a common reserve pool.

A fixed reserve list of three proposals per open call will be maintained. These will be the next highest-ranked proposals that have met all eligibility and evaluation thresholds but were not initially selected for funding.

Should budget become available—either from within a specific call or the combined reserve pool—the consortium may fund one or more reserve list proposals in strict ranking order, provided that:

- The proposal meets all eligibility and threshold requirements.
- Its funding request does not exceed the available remaining budget (no partial grants will be awarded).

3.2. Eligible Cost Types (as part of Lump Sum)

The following categories of activities are explicitly eligible for financial support (Indirect costs 25% must also included – for more details check the proposal template):

- **Personnel:** Costs related to participation in CYberSynchrony activities, project work, training, and collaboration.
- **Travel:** Expenses for attending meetings, events, or conferences related to the project.
- **Technical Resources:** Acquisition or use of necessary hardware, software, and datasets.
- **Infrastructure:** Access fees or usage costs essential to project implementation.
- **Subcontracting:** Permitted only if:
  - Defined clearly in the proposal,
  - Expertise not provided by the consortium of the proposal,
  - Directly related to the project objectives.
- **Communication:** Audio/visual materials and outreach tools.
- **Promotion:** Efforts to disseminate and promote the supported services and CYberSynchrony outcomes

3.3. Payment Modalities

Financial support to third parties under the CYberSynchrony open calls will be provided in the form of **lump sum grants**. The awarded amount will not be reimbursed based on actual incurred costs, but rather disbursed upon verification that specific deliverables — as defined in the funded proposal — have been completed.

This lump sum model applies to all types of activities supported under the open calls, including those carried out by individual applicants or by consortia. The exact amount of the grant and the conditions for payment will be specified in the sub-grant agreement signed between the third party and the CYberSynchrony consortium.

While CYberSynchrony provides funding under the lump sum model for selected third parties, applicants should be aware of the standard principles applied when estimating their project budget. Even though **actual costs will not be reimbursed**, and no detailed financial reporting is required during project execution, beneficiaries must be prepared to justify their cost calculations in the event of a verification or audit by the European Commission. For this reason, it is recommended that all applicants retain supporting financial documentation for their internal records.

3.3.1. Proposed Payment Structure

Payments will be made in lump sums, strictly tied to the achievement and validation of predefined deliverables and milestones, as described in the Sub-grant Agreement. To maintain effective project implementation and cash flow management, the lump sum awarded will typically be split into three instalments:

1. Prefinancing (30% of the total budget) – Month 1 (Total duration of the project will be 8 months)

- Paid within one month after signing the Sub-grant Agreement and project initiation.

2. Interim Payment (up to 40% of the total budget for Months M1-M4) (Payment will take place in M5 after checking that all deliverables have been structured according to the plan - Total duration of the project will be 8 months)

- Paid upon successful completion and validation of intermediate project milestones and deliverables, clearly defined at the beginning of the project (e.g., mid-term reports, intermediate technical or implementation deliverables).

3. Final Payment (remaining budget for months M5-M8) – paid within 1 month after the end of the open call project

- Released upon the final validation of all remaining deliverables and the final report, demonstrating complete implementation and achievement of the project objectives.

3.3.2. Coordination and Internal Fund Distribution

In consortium-led proposals (i.e. involving more than one beneficiary), financial disbursements follow a **centralised distribution model**:

All instalments of the lump sum—prefinancing, interim, and final—are paid **exclusively to the lead partner (coordinator)**. This aligns with standard FSTP practice, where acknowledging one primary legal and financial point of contact simplifies administration and accountability.

The coordinator assumes full responsibility for allocating the funds internally to the consortium members. This distribution should adhere to the **pre-planned budget breakdown** agreed upon during proposal development and reflected in the Sub-grant Agreement. The **consortium agreement** must specify the percentages or amounts allocated to each partner.

4. Duration and Possible Time Extensions

The duration of the FSTP projects funded under the CYberSynchrony open calls is fixed to 8 months and the starting date will be clearly defined at the moment of the sub-grant agreement signature. However, in exceptional and duly justified cases (e.g., unforeseen technical delays, significant external factors beyond the beneficiary's control), the Open Call Management Team (OCMT)[1] may approve a one-time extension of the project duration by up to one month – (this will also depend to other unforeseen delays that may happen before the initiation of the FSTP projects, for example: delays in the evaluation, contract signing, etc.).

Beneficiaries seeking such an extension must submit a written request at least one month before the original end date, providing detailed justification and demonstrating that the extension will ensure successful completion of all remaining deliverables. The OCMT will evaluate each request individually and reserves the right to approve or reject extension requests based on their assessment of the circumstances and justification provided. No additional funding will be provided for extended periods, and extensions must not exceed a total duration increase of one month. In the case of an extension, the final payment will be made one month after the end of the new extended ending period, and only if all deliverables have been submitted and their content aligns with what has been described in the proposal.

5. Eligible Applicants per Open Call

General Eligibility Conditions (Applies to all three Open Calls): Eligible applicants are entities established in countries as defined in the Digital Europe Programme (DEP) which include:

[1] OCMT (Open Call Management Team) is responsible for the design and specifications of the Open Calls, and supervising the implementation of the methodology phases as detailed in the grant agreement. This team is coordinated by MAG (MAGGIOLI SPA) and will include technical representatives from the CYberSynchrony consortium. OCMT will be responsible for the recruitment of the external evaluation experts to be involved in the evaluation process and the provision of content for the promotion of the Open Calls implementation.

a. the 27 EU Member States,
b. the European Economic Area (EEA) countries (Iceland, Liechtenstein, Norway)

Each third party may submit only one proposal per call. A third party may receive a maximum of €200,000 total across all open calls.

Large companies are excluded from these open calls.

In case of monobeneficiary (single entity) projects, the applicant must be an SME.

In case of consortia of 2 or 3 entities, the coordinator must be an SME and will be responsible for the payments of the other partners of the consortium. The consortium may have additional SMEs (excluding the SME acting as the coordinator), if necessary, for the scope of the FSTP project. In this case, the legal documentation related to the SMEs must be filled in by all SMEs.

The consortium agreement will be legally bound by signing the Annex 5 - Open Call Declaration of Honour - consortium agreement (HERE).

Error! Not a valid bookmark self-reference. shows the types of the applicants that can participate depending on the open call.

Table 5 Applicant eligibility based on the open call

Open Call	Eligible Participants
Call 1 – Infrastructure Resilience & Operational Readiness	• Cybersecurity firms (SMEs only – can be more than one, but one of these SMEs must act as the coordinator) specialising in infrastructure resilience • Public & competent authorities [ministries and government departments; regional and municipal authorities and their agencies; regulators and national CERT/SOCs; public hospitals; public universities and research institutes], NGOs, and private organisations [research, SMEs] operating within the NIS2 sectors • Independent cybersecurity professionals [Individuals] with experience in sector-specific operations and infrastructure
Call 2 – Compliance, Innovation & Regulatory Advancement	• Organisations [SMEs, Public entities, NGOs] involved in regulatory compliance, and/or • Research institutions, or tech startups focused on cybersecurity innovation in NIS2 sectors, and/or • Regulatory experts [SMEs, Public entities, Individuals] and cybersecurity innovators [SMEs, Public entities, Individuals] specialised in the relevant domain
Call 3 – Mutual Assistance & Cyber Collaboration Among Member States	• The coordinating participant must be an SME and must represent or be affiliated with a Member State's government, relevant cybersecurity agency, or a recognized research institution. • To demonstrate the cross-collaboration requirement for this call, the involvement of at least one additional partner from a different MS than the coordinating participant (any type of entities as stated in OC1 and OC2, excluding individuals) is mandatory. • Demonstrated experience in international cyber collaboration or mutual assistance initiatives is an advantage. • Proposals must clearly address at least one of the listed priority areas (see section 2.3) and detail how the initiative will enhance mutual assistance among Member States.

All participants should have a valid VAT and PIC number (including the individuals who are eligible to participate in Open Call 1 and Open Call 2).

6. Proposal Evaluation Criteria

All proposals submitted under the CYberSynchrony open calls will be evaluated by two independent external experts. Evaluations will be based on four criteria, each scored from **0 to 5**, with a minimum threshold of **3 out of 5 per criterion** required for eligibility (Table 6).

Table 6 Evaluation Criteria

Criterion	Description
1. Relevance and Excellence	The proposal must clearly define the project objectives and demonstrate their relevance to CYberSynchrony. It should address specific cybersecurity vulnerabilities, describe the main goals, and show alignment with the open call objectives and KPIs.
2. Methodological Soundness	The proposal must provide a clear and logically structured methodology explaining how the proposed objectives will be achieved. This includes a breakdown of the technical and operational approach, explanation of tools and frameworks to be used, sequencing of activities, interdependencies, and validation steps. The methodology should demonstrate that the applicant has a concrete, realistic, and technically credible plan for executing the work. Alignment with the CYberSynchrony architecture and integration of relevant modules should be made explicit where applicable. Evaluators must be able to understand not just what the applicant aims to do, but exactly how they will carry it out in practice.
3. Ambition and Impact	The proposal should show a clear ambition and expected outcomes, demonstrating the technical, operational, and market-level impact. Results must contribute to the goals and KPIs defined in each CYberSynchrony open call (there are separate sections for each call (Open Call 1: Section 2.1, Open Call 2: Section 2.2, Open Call 3: Section 2.3).
4. Implementation/ Team Skills and Expertise	A credible and structured implementation plan must be presented, including a realistic timeline (describe WP and tasks, always having in mind the "lump sum" approach), defined milestones and deliverables, and effective risk mitigation measures. Inadequate justification of costs and resources will result in a below-threshold score. Applicants must demonstrate that their team possesses the required knowledge and experience, including technical and regulatory expertise relevant to the targeted NIS2 sectors. Prior experience in cybersecurity innovation or deployment should be clearly described as well as their role in the project.

6.1. Scoring Scale and Threshold

For each criterion, a maximum of **5 points** will be granted, on a scale from 0 to 5 and with increments of 0.5. The **overall maximum score** is 20 points.
The individual scores are interpreted as follows:

- **0 – Fail**: The proposal fails to address the criterion or cannot be judged due to missing/incomplete information.
- **1 – Poor**: The criterion is inadequately addressed, with serious inherent weaknesses.
- **2 – Fair**: The proposal broadly addresses the criterion, but significant weaknesses remain.
- **3 – Good**: The criterion is well addressed, although improvements are necessary.
- **4 – Very Good**: The proposal addresses the criterion very well, with only minor improvements needed.
- **5 – Excellent**: All relevant aspects of the criterion are successfully addressed; shortcomings are negligible.

A **threshold of 3 out of 5 per criterion** is required for a proposal to qualify for selection. It is noted that **inadequateness of the justification on costs and resources**, as judged by expert evaluators, will result in a **below-threshold score in the Implementation category**.

6.2. Ranking and Tie-breaking Rules

Proposals will be ranked by their total score. In case of ties, evaluators will apply the following sequence of prioritisation criteria:

- **Rule 1:** Priority will be given to innovation of the concept (Criterion 1 – see Table 6).
- **Rule 2:** In case following Rule 1 there are proposals in the same position, priority will be given to proposals that their technology better fit to CYberSynchrony scope (Criterion 2 – see Table 6).
- **Rule 3:** In case following Rule 2 there are proposals in the same position, priority will be given to proposals that have higher impact and market potential (Criterion 3 – see Table 6).
- **Rule 4:** In case following Rule 3 there are proposals in the same position, priority will be given to the application that has lower funding request.
- **Rule 5:** In case following Rule 4 there are proposals in the same position, priority will be given to the number of female researchers participating in the team.
- **Rule 6:** In case following Rule 5 there are proposals in the same position, priority will be given to the application that increases CYberSynchrony project footprint in Europe.

If proposals are still ranked identically after applying these factors, an additional evaluator from the external evaluators' pool, will be appointed to re-evaluate the tied submissions and break the tie. A reserve list of the highest ranked proposals (after the funded ones) will be maintained, in case that any of the applicants of the successful proposals withdraw or fail to fulfil contractual obligations.

6.3. Final Selection

The CYberSynchrony Open Call Management Team (OCMT) will gather the reviews from the external evaluators. All reviews will be checked for accuracy (or errors) and consensus meetings will be held with the external evaluators if any inconsistencies are identified in order to eliminate inconsistencies and maximise clarity. After this, the provisional successful list of the awarded proposals will be documented, and all applicants will receive notification of the results accompanied with an Evaluation Summary Report (ESR). If the number or quality of eligible proposals is insufficient, the CYberSynchrony consortium has the right to re-open the call at a later date.

6.4. Redress process

The applicants who will receive a rejection letter, will have 3 working days to submit a request for redress, limited to eligibility errors or procedural issues affecting the evaluation. In that case, an internal review committee of the OCMT will examine the request for redress. The OCMT's role is to ensure a coherent interpretation of such requests, and equal treatment of applicants.
Requests must be:

- Related to the evaluation process or eligibility checks.
- Clearly describe the complaint.
- Received within the time limit (3 working days) from the reception of a rejection letter considering the proposal as non-eligible or the ESR information letter delivered.
- Sent by the applicant legal representative that has also submitted the proposal.

The committee will review the complaint and will recommend an appropriate course of action. If there is clear evidence of a shortcoming that could affect the eventual funding decision, it is possible that all or part of the proposal will be re-evaluated.
Please note:

- This procedure is concerned only with the evaluation and/or eligibility checking process. The committee will not call into question the scientific, technical or impact judgement of appropriately qualified experts.

- A re-evaluation will only be carried out if there is evidence of a shortcoming that affects the final decision on whether to include the partner in CYberSynchrony consortium or not. This means, for example, that a problem relating to one evaluation criterion will not lead to a re-evaluation if a proposal has failed anyway on other criteria.
- The evaluation score following any re-evaluation will be regarded as definitive. It may be lower than the original score.
- Only one request for redress per proposal will be considered by the committee. All requests for redress will be treated in confidence and must be sent to the OCMT at info@cybersynchrony.eu.

7. Proposal structure

Applicants must submit a concise proposal document that clearly presents the objectives, methodology, relevance, and expected impact of the proposed work. The proposal must be written in **English** and submitted in **PDF format** through the official CYberSynchrony submission platform (see section 1.1).

The maximum length of the proposal is **10 pages** (excluding any required annexes). Proposals exceeding this limit **will be considered ineligible and will be not evaluated.**

To facilitate fair and consistent evaluation, applicants are strongly encouraged to structure their proposal using the following format. Please keep the following information as a guideline on what information you should provide in order your proposal to be competitive (The template for your proposal can be downloaded from HERE). Each section is aligned with the evaluation criteria used by the reviewers (Table 7):

Table 7 Content description of each proposal section and corresponding linked criteria (see ***Table 6***)

Section	Content Description	Linked Evaluation Criterion
1. Executive Summary	Provide a high-level summary of the proposal, including the selected open call, the main cybersecurity challenge being addressed, the proposed solution, key activities, expected outcomes, and total requested funding. This section should give evaluators a complete snapshot of what the project is about and its strategic relevance.	***(All criteria – contextual overview)***
2. Project Objectives and Alignment	Clearly state the specific objectives of the proposal and explain how they respond to the priorities and scope of the selected open call. Indicate which CYberSynchrony project objectives (OBJ1–OBJ9, see 2.4) and KPIs the proposal contributes to. Make the connection between the sectoral challenge and the proposed approach explicit.	**Relevance and Excellence**
3. Technical and Methodological Approach	Describe in detail *how* the proposed objectives will be achieved. Include your methodological framework, selected tools or technologies, implementation logic, and key phases or work packages. Explain how CYberSynchrony modules (e.g. CYRESCUE, CYBERRA, etc) will be used, extended, or integrated. This section should show technical depth and internal coherence.	**Methodological Soundness**
4. Implementation Plan	Outline the structure and flow of work across the project duration. Include a realistic timeline, key tasks, list of milestones and deliverables, resource allocation, and risk mitigation strategies. If a consortium is proposed, specify the roles and responsibilities of each partner and their coordination plan. As part of our dissemination strategy, each FSTP project must include in its deliverables list (expected to be submitted at the end	**Implementation**

of the FSTP project (M8)) a demo video of their solution, a "final results" report and a "Detailed implementation/financial plan":

1. Demo video: Each funded project must prepare a presentation video (minimum duration 8 minutes – maximum 12 minutes) as part of its final reporting. The video should clearly explain the project's objectives, highlight the **main outcomes and results**, and include a **short demonstration** of how the developed tool/module/algorithm/model/service/activities functions in practice. The presentation should be structured for both technical and non-technical audiences, using clear visuals and narration. The final video must be submitted in **MP4 format (Resolution: 1920 × 1080 (Full HD, 16:9), Frame rate**: 25), and will be published on the CYberSynchrony website/social media for dissemination purposes.

2. Final Results Report (PDF/DOCX): Each funded project must prepare a **Final Results Report** in PDF and DOCX format, which will summarise the main achievements, technical outcomes, and impacts of the project. The report will be uploaded to CyberSynchrony's website, and will be publicly accessible. Hence, please ensure that not confidential information is included in it. The report should be around **2,000 words** in length and must include a **2000-character summary (including spaces)** that will be used for dissemination purposes. The report should also include **figures, diagrams, screenshots, or other visual elements** to make the results more accessible and engaging. Font size and type, margins and other layout rules, are the same as used in the proposal template.

To ensure uniformity, the report should follow the structure below:

1. **Cover Page**
   - Project title, acronym, beneficiaries, contact person.
2. **Executive Summary (2000 characters including spaces)**
   - Concise overview of objectives, results, and significance.
3. **Introduction and Objectives**
   - Brief context, problem addressed, project goals.
4. **Methodology and Technical Approach**
   - How the work was carried out (methods, tools, integration with CYberSynchrony modules).
5. **Main Results and Achievements**
   - Description of the key results, innovations, or demonstrators.
   - Include figures, screenshots, and technical evidence.
6. **Impact and Relevance**
   - Expected or achieved impact (technical, regulatory, sectoral, or market).
   - Contribution to CYberSynchrony objectives and KPIs.
7. **Conclusions and Next Steps**
   - Lessons learned, sustainability, and future exploitation potential.

3. Detailed implementation/financial plan: Apart from your technical deliverables that should be stated in your Work Packages,

	you have to include a deliverable entitled: "Detailed implementation/financial plan" (Delivery month: M1). In this deliverable you will have to provide a more detailed implementation/financial plan than what you will provide in your proposal, split per partner (all cost categories, Person Months, etc) and per payment period. More instructions and a template for this will be provided before the initiation of the projects.	
5. Expected Impact	Present the technical, operational, regulatory, or market impact of your proposed work. Clarify how the results will improve cybersecurity resilience, readiness, or compliance in the selected NIS2 sector(s). Reference the call-specific KPIs and describe any expected benefits across borders or sectors.	**Ambition and Impact**
6. Team and Organisational Capacity	Provide short profiles of the applicant(s) as entities (not description of CVs of the team), highlighting relevant experience, technical expertise, and sectoral knowledge. Emphasise any previous participation in cybersecurity projects or regulatory initiatives. For collaborative proposals, explain how the team composition enhances the proposal's strength.	**Team Skills and Expertise**
7. Budget Overview	Specify the total lump sum requested and provide a high-level distribution across main activities (e.g. personnel, software, training). Justify how the requested amount relates to the scope and effort involved. Respect the funding limits and sub-caps described in Tables 1, 2, and 3. No detailed cost breakdown is needed, but the budget must appear proportionate and credible.	**Implementation**

8. Intellectual property rights (IPR) and results ownership

Third-party beneficiaries funded under the CYberSynchrony Financial Support to Third Parties (FSTP) mechanism will retain ownership of all results they generate during the implementation of their funded projects. This includes, but is not limited to, software, data, algorithms, designs, prototypes, training materials, and documented methodologies developed with FSTP support.
However, in line with Horizon Europe obligations and the principles of open innovation and public value, the following conditions will apply:

1. Ownership and Responsibility

- All results produced by a single beneficiary belong solely to that beneficiary.
- In collaborative projects, ownership arrangements must be clearly agreed upon and described in a consortium agreement or internal partnership declaration.
- The above does not exclude the possibility for specific agreements to be made between the Beneficiary and one or more of the partners of CYberSynchrony.
- Beneficiaries are solely responsible for ensuring the protection of their results where appropriate (e.g., through patents, copyright, or trade secrets) and for managing any potential conflicts or shared ownership issues.

2. Access Rights for CYberSynchrony and the European Commission

- The CYberSynchrony consortium and the European Commission will be granted non-exclusive, royalty-free rights to access the results for purposes of:
  - Monitoring and verifying project implementation,
  - Dissemination of non-confidential information and success stories,
  - Ensuring policy alignment and program evaluation.
- This access is strictly for non-commercial and public-interest use and does not affect the beneficiary's commercial exploitation rights.

3. Exploitation and Use of Results

- Beneficiaries are encouraged to actively exploit their results beyond the funding period. This may include commercial use, standardisation activities, integration into existing product portfolios, licensing to third parties, or contributing to open-source ecosystems where relevant.
- The exploitation route should be compatible with the objectives of the CYberSynchrony project and the NIS2 Directive sectors targeted in the open calls.

4. Licensing and Third-Party Use

- Any licenses granted by beneficiaries to third parties must not restrict the access rights of the CYberSynchrony consortium or the European Commission as described above.
- Licenses must respect applicable intellectual property laws and must not compromise security-sensitive components, if such restrictions apply.

5. Confidentiality and Dissemination

- While results may be used for dissemination and public communication, confidential or security-sensitive information will not be shared without explicit consent from the beneficiary.
- The CYberSynchrony consortium may request non-confidential summaries of the results for use in project-level reporting and communication.

9. Conflict of Interest Rules

9.1. Open call applicants

The applicant must take all measures to prevent any situation where the impartial and objective implementation of the proposed tasks are compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest ('conflict of interests').

They must formally notify to the CYberSynchrony coordinator without delay any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation. The CYberSynchrony coordinator may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

9.2. External Evaluators

All evaluations of proposals submitted to the CYberSynchrony Open Calls will be carried out under strict conflict of interest and confidentiality rules.

1. **Confidentiality**: The external evaluators engaged in the evaluation process are bound to treat all information contained in proposals as strictly confidential. This obligation applies during the evaluation and continues indefinitely after the process has concluded.
2. **Non-disclosure**: The external evaluators must not reveal to any third party the identity of applicants, the content of proposals, or the opinions and assessments of other evaluators, either during the evaluation process or afterwards.
3. **Independence**: Evaluators must not have any involvement in the preparation of proposals submitted to the call and must not benefit, either directly or indirectly, from their selection or rejection.
4. **Conflict of Interest**: Evaluators are required to declare any potential conflict of interest immediately. If such a conflict is identified, the evaluator must withdraw from the assessment of the affected proposal(s).

10. Sub-grant Agreement

Within one week of final result notification, the OCMT will contact the successful applicants to begin contract preparation.
The Sub-grant Agreement will be signed between the CYberSynchrony Coordinator and each third party and will include:

- Specific clauses on cascading funding under Horizon Europe,
- Payment conditions and linked deliverables,

- General legal obligations (IPR, audits, etc.).

Sub-granted projects will then enter the roll-out and monitoring phase under the oversight of the project's implementation team. If a selected legal entity fails to submit the required documentation on time, it will be excluded from the CYberSynchrony programme. The sub-grant agreement can be found on the Open call Synchrony website and is available to all applicants.

10.1. Information on which documentation is mandatory to be submitted, and which should be taken into consideration

Each proposal must include the following mandatory documents at the time of submission. All files must be uploaded via the official CYberSynchrony submission platform before the call deadline.

DOCUMENTATION FOR OPEN CALL APPLICANTS
1. Proposal technical template (MANDATORY) A single PDF file, maximum 10 pages, structured according to the recommended format described in the "Proposal Structure" section. It must include the core technical, implementation, and impact content. The template is provided HERE.
2. Annex 2 - Declaration of Honour SME form (MANDATORY) For monobeneficiary (single entity) proposals, the applicant must be an SME, and the form is mandatory. For consortia of 2 or 3, an SME must be the coordinator of the consortium, and a Declaration of Honour SME form must be filled in and submitted throughout the submission platform. If the consortium has additional SME partners (apart from the SME which will act as the coordinator), the form must be completed by them too. The template is provided HERE.
3. Annex 3 - SME Self-Declaration Form *(MANDATORY)* For monobeneficiary (single entity) proposals, the applicant must be an SME, and the form is mandatory. For consortia of 2 or 3, an SME must be the coordinator of the consortium, and an SME Self-Declaration form must be filled in and submitted throughout the submission process. If the consortium has additional SME partners (apart from the SME which will act as the coordinator), the form must be completed by them too. The template is provided HERE.
4. Annex 5 - Open Call Declaration of Honour - consortium agreement (MANDATORY - ONLY FOR CONSORTIA) For collaborative proposals involving more than one entity, a signed statement confirming joint participation, role allocation, and lead partner must be included. The lead partner must be an SME. The template is provided HERE.
5. ONLY FOR OPEN CALL 3 - MANDATORY REPRESENATION/AFFILIATION LETTER (FOR OPEN CALLS 1 and 2, this document is not required): The coordinator of the consortium must be an SME and is mandatory to provide a letter that proves that the SME represents or is affiliated with a Member State's government, relevant cybersecurity agency, or a recognized research institution. The letter must be signed by both sides. There is no specific template for this letter, applicants should provide their own format, ensuring the above condition.
6. Letters of Support *(Optional)* Applicants may attach letters of support or intent from relevant stakeholders, especially if their proposal includes cooperation with national cybersecurity agencies, sector operators, or Member State institutions. These are not scored but may support the credibility of the implementation. Up to 3 letters of support can be submitted through the submission platform if applicants believe that this is necessary and assists with their content proposition.
7. CYberSynchrony Sub-grant agreement for FSTP (Read only, not required to be submitted at this stage). FSTP applicants are advised to read through the agreement, to clarify questions that may have and concern legal and contractual obligations and terms. This agreement will be signed only by the successful applicants.

DOCUMENTATION FOR EXTERNAL EVALUATORS
1. **Annex A - Open Call contract for external evaluator (Read only, not required to be submitted at this stage)** This is the contract that has to be signed only by the external evaluators who will be selected to review the FSTP proposals. All external evaluators are advised to read through the contract to clarify questions that may have and concern legal and contractual obligations and terms.
2. **Annex B - Conflict of Interest (Read only, not required to be submitted at this stage)** This document contains the terms and conditions related to any conflict of interest related to the proposals that external evaluators will evaluate.
3. **Annex C - Bank details (Not required to be submitted at this stage)** After the selection process, all successful external evaluators should provide their bank details to get the payments according to the number of proposals evaluated.

11. Core CYberSynchrony Modules

The applicants have to ensure that their proposals are strictly aligned with the CYberSynchrony objectives (see section 2 – each Open Call refers to different CYberSynchrony objectives) and Open Call description/KPis (see also section 2). Their proposed work must involve the use of one or more of the CYberSynchrony modules: These modules constitute the technical foundation of the project and represent the operational areas where third-party technologies must connect, integrate, or extend functionality. Each module addresses a specific dimension of cybersecurity preparedness, detection, response, and compliance across national and sectoral environments. Below, there is more information regarding each CYberSynchrony module, however more detailed information concerning our modules can be found in our public deliverables (see section 12).

11.1. CYRESCUE – Resilience and Incident Response

This module acts as the incident response and resilience orchestration layer, coordinating detection results, automating countermeasures, and preserving digital evidence for forensic and legal verification. In addition, the module includes Cyber Security Posture Assessment (CSPA), Purple Team Assessment (PTA), and Security Breach Simulation (SBS) to test operational readiness, validate incident response playbooks, and quantify resilience improvements over time.

List of tools included in CYRESCUE:

1. Cyber Security Posture Assessment (CSPA)
2. Purple Team Assessment (PTA)
3. Security Breach Simulation (SBS)

CSPA – Cyber Security Posture Assessment (more info in D3.2, section 12):

- Web-based dashboard for assessing organizational maturity and compliance posture.
- REST API for automated submission of system metrics and retrieval of posture scores.
- Export capability in JSON and CSV for integration with compliance reporting tools.

PTA – Purple Team Assessment (more info in D3.2, section 12):

- Controlled environment for conducting coordinated Red/Blue team exercises.
- Provides simulation templates (attack scenarios, MITRE ATT&CK mappings).
- Results accessible via secure API or downloadable JSON reports.

SBS – Security Breach Simulation (not included in a deliverable yet):

- Cloud-deployable engine for executing controlled breach and ransomware simulations.
- Configurable scenarios via web dashboard or API endpoints.
- Generates forensic data and reports for analysis within the CYRESCUE environment.

- Campaigns with Caldera (SBS uses MITRE Caldera to conduct realistic, campaign-style red team simulations within dockerised environments. These simulated attacks reproduce various threat actor behaviours and test the organisation's detection and response mechanisms. SBS provides a visual and interactive way to assess readiness against evolving adversary tactics through discovery and attack lifecycle emulation).

Which are the general requirements for the tools/solutions that will be developed for CYRESCUE Integration:

- Strict adherence to data formats such as JSON, STIX 2.1, and TAXII, for structured threat intelligence sharing.
- A sandbox environment with mock data is available to selected applicants for testing.

11.2. CYBERRA – Threat Intelligence and Risk Analysis

CYBERRA enables Member States and critical infrastructures to understand, anticipate, and mitigate evolving cyber threats through real-time intelligence and data-driven risk assessment. It provides continuous threat monitoring, vulnerability correlation, and contextual risk analysis tailored to national or sectoral environments. The module aggregates global threat intelligence, correlates Indicators of Compromise (IoCs) with local events, and models customized risk scenarios to identify high-impact vulnerabilities before they are exploited. It also supports the execution of controlled attack simulations and security posture evaluations to strengthen organizational readiness. In addition, CYBERRA supports operational decision-making through **Defensive Cyber Operations (DCO)** playbooks, which translate threat intelligence findings into structured response actions. These playbooks assist security teams in evaluating response options, understanding potential impact, and preparing coordinated mitigation actions before threats materialise into incidents. All threat intelligence data and analytical outputs are stored and processed with verifiable forensic integrity, ensuring that information remains reliable, traceable, and tamper-resistant. CYBERRA integrates MISP as its core threat intelligence platform and provides the analytical foundation that informs downstream modules responsible for incident response coordination and resilience assessment.

List of tools included in CYBERRA:

1. MISP
2. Defensive Cyber Operations/Response Playbooks (DCO)

MISP – Threat Intelligence Platform (more info in D3.1 – see section 12):

- Web-based interface for viewing and managing Indicators of Compromise (IoCs).
- REST API for automated ingestion and export of threat data in STIX/TAXII or JSON format.
- Supports authentication via API keys and HTTPS/TLS for secure communication.

DCO (Response Playbooks (more info in D4.2 - D4.4, section 12):

- Playbooks are pre-defined, step-by-step guides that outline responses to specific cybersecurity incidents.

Which are the general requirements for the tools/solutions that will be developed for CYBERRA Integration:

- Strict adherence to data formats such as JSON, STIX 2.1, and TAXII, for structured threat intelligence sharing.
- Organisations can run MISP on its own server or VM (PHP/MySQL stack), collect Indicators of Compromise (IoCs) manually or via feeds (STIX/TAXII), and export IoCs in multiple formats (JSON, CSV, XML) or expose them via its REST API.
- A sandbox environment with mock data is available to selected applicants for testing.

11.3. CYBRITE – Continuous Monitoring and Early Threat Detection

CYBRITE focuses on enabling real-time monitoring of cyber threats and the rapid detection of anomalies before they escalate into full-scale incidents. It forms the core detection and monitoring layer of the CYberSynchrony ecosystem, integrating host-based, network-based, and behavioural analytics tools. Through the combined use of Security Information and Event Management (SIEM) technologies (e.g., Wazuh), network intrusion detection systems (e.g., Suricata), and machine-learning-based anomaly analysis (Anomaly Detector IDS and WEKA), the module provides full visibility over infrastructure and user activity. The combination of these multiple data sources enables CYBRITE to achieve early threat detection, proactive risk identification, and timely responses to evolving cybersecurity incidents.

List of tools included in CYBRITE:

Wazuh – Security Information and Event Management (SIEM) (More info in D4.1, section 12):

- Centralised monitoring and alerting interface for endpoints, servers, and applications.
- Collects security event logs via deployed agents and integrates Sysmon telemetry.
- Accessible through the Wazuh Dashboard (HTTPS) and REST API for automation.

Suricata – Network Intrusion Detection and Analysis (More info in D4.1, section 12):

- Inspects live network traffic for suspicious or malicious activity.
- Applies open rule sets (Emerging Threats, custom IDS signatures).
- Outputs JSON-formatted logs (EVE format) compatible with Wazuh's indexer.
- REST API (via Elastic/OpenSearch) for querying and correlation.

Anomaly Detector IDS – Behavioural Anomaly Detection (More info in D4.1, section 12):

- Cloud-based AI/ML engine analysing aggregated Wazuh and Suricata logs.
- Detects abnormal system, network, or user behaviour compared to baselines.
- Provides alert scoring and classification (critical/high/medium/low).
- Exposes REST endpoints for retrieving anomaly reports (JSON).

WEKA – Machine Learning Analytics Engine (More info in D4.1, section 12):

- Supports data-driven pattern discovery and predictive threat analysis.
- Consumes normalised datasets exported from Wazuh and Suricata pipelines.
- Used for UEBA (User and Entity Behaviour Analytics) to detect insider threats.
- Accessible through API for automated retraining and model testing.

Technical Integration Requirements:

- Logs must follow ECS (Elastic Common Schema) and EVE JSON structures for SIEM and IDS compatibility
- Integration with anomaly detection tools (WEKA, AI classifiers) is recommended for behavioural analysis
- Applicants must demonstrate support for cross-system log correlation and real-time alerting.

11.4. CROSS-CORE – Cross-Border Coordination and Secure Information Exchange

CROSS-CORE enables secure collaboration and evidence exchange between Member States, national CERTs, and critical infrastructure operators during cross-border cybersecurity incidents. It ensures that alerts, forensic data, and incident packages can be shared safely, verified for authenticity, and used as trusted evidence in coordinated investigations. The module's architecture combines a Secure Data Exchange Platform with blockchain-based integrity verification, establishing a tamper-proof chain of custody for every exchanged dataset. Through these mechanisms, CROSS-CORE promotes transparency, accountability, and non-repudiation in multi-country operations. It also enforces compliance with European cybersecurity regulations (GDPR, NIS2) by guaranteeing that all shared data follows standardized evidence handling formats and privacy-preserving protocols. In addition to integrity verification and secure transmission, CROSS-CORE supports privacy-aware analytical workflows through

the combined use of Differential Privacy and Homomorphic Encryption. Differential Privacy is applied during dataset processing to limit inference risks, while Homomorphic Encryption enables authorized entities to perform computations directly on encrypted data. These mechanisms complement blockchain-based integrity verification, strengthening trust and accountability in cross-border information exchange without exposing underlying datasets. This module comprises one tool called ***Blockchain integrity validator and more information can be found in D5.1, section 12***.

Technical Integration Requirements:

- Solutions must integrate with the Secure Data Exchange Platform via REST APIs, using:
  - JSON Web Tokens for API authentication
- Data integrity is ensured through SHA-256 hashing and blockchain anchoring
- Supports privacy-aware analytical exchange by integrating Differential Privacy during dataset processing, reducing the risk of attribute inference while maintaining analytical relevance.
- Enables encrypted collaborative analytics through Homomorphic Encryption, allowing computations on protected datasets while ensuring that intermediate components never access plaintext information.
- Data Integrity and Encryption Hyperledger
  - Ensures the authenticity and immutability of all incident data and forensic evidence shared across Member States.
  - Applies SHA-256 hashing and blockchain anchoring to create tamper-proof audit trails.
  - Manages encryption of data in transit and at rest, maintaining confidentiality during exchange.
  - Supports secure data transfer between national SOCs/CSIRTs through JWT-authenticated sessions.

11.5. CYBERWISE – Cybersecurity Awareness and Behavioural Training

CYBERWISE addresses the human dimension of cybersecurity by promoting education, behavioural change, and social resilience against common threats. It combines gamified training modules, interactive awareness platforms, and behavioural analytics tools to engage users across different sectors and levels of expertise. The module also includes capabilities for simulating social engineering attacks, allowing organisations to measure user responses and adapt their awareness strategies accordingly. It also includes behavioural and human risk assessment mechanisms (HRM) that help correlate technical alerts with user-level insights, creating a unified picture of both machine and human threat vectors. Through these mechanisms, CYBERWISE aims to build a culture of security-conscious behaviour that complements technical defences and reduces the likelihood of successful attacks.

List of tools included in CYBERWISE:

HRM - Human Risk Management (more info in D4.1, see section 12)

- Evaluates employee awareness levels, behavioural risk factors, and compliance with cybersecurity policies.
- Generates dynamic risk scores for individuals and departments, highlighting human-related vulnerabilities.
- Integrates with the platform to visualize awareness trends and improvement over time.

Phishing & Social-Engineering Campaigns

- Runs configurable phishing/social-engineering exercises (templates, targeting, scheduling).
- Captures metrics: deliver/open/click/submit/report, and time-to-report.

Cyber-Gate: Gamified Awareness and Training (not included in a deliverable yet)

- Interactive, game-based learning environment that teaches cybersecurity concepts using MITRE ATT&CK tactics and real-world attack paths.
- Users play through simulated cyber incidents, learning how attackers operate and how to defend systems.

- Includes missions, minigames, and progress scoring to engage users while reinforcing secure behaviour.

11.6. CYBERGOPLUS – Governance, Standards, and Regulatory Compliance

CYBERGOPLUS provides tools and environments that help organisations align with European cybersecurity regulations, standards, and certification frameworks. It enables entities to define and enforce internal security policies, monitor compliance across systems and departments, and conduct structured audits. The module incorporates vulnerability management and policy enforcement mechanisms to ensure continuous alignment with NIS2, GDPR, and ISO 27001 requirements. By integrating attack surface visibility (ASA), code-level vulnerability scanning (Snyk), and centralized policy control, CYBERGOPLUS creates a unified compliance layer that bridges technical and organisational cybersecurity governance. This module ultimately strengthens accountability, simplifies regulatory reporting, and promotes harmonisation of compliance practices across sectors and Member States.

List of tools included in CYBERGOPLUS:

ASA – Attack Surface Assessment (more info in D3.2, see section 12)

- Scans infrastructure and endpoints to identify exposed assets, open ports, and misconfigurations.
- Maps discovered assets to vulnerabilities (CVE, CWE, ATT&CK) and provides prioritised remediation guidance.
- Outputs reports for compliance and risk benchmarking against NIS2 or internal standards.

Snyk – Code and Dependency Vulnerability Scanner (not included in a deliverable yet)

- Scans source code, containers, and dependencies for known security flaws.
- Provides developers and auditors with prioritised vulnerability data and recommended fixes.
- Integrates with CI/CD pipelines and exports structured results (JSON) for governance dashboards.

Policy Tools – Compliance and Governance Frameworks

- Enforcement and monitoring of internal cybersecurity policies, track policy adherence
- Map technical controls to compliance frameworks (NIS2, GDPR, ISO 27001).

12. Access to CYberSynchrony Public Deliverables

Applicants interested in submitting proposals under the CYberSynchrony FSTP Open Calls are strongly encouraged to consult the project's public deliverables (Table 8). These documents provide essential technical, architectural, and functional information about the CYberSynchrony ecosystem, which is critical for preparing targeted, high-quality proposals aligned with the project. The deliverables in the green rows in Table 8 are related to the modules of CYberSynchrony whilst the deliverables in the orange rows describe specific aspects of the framework and architecture of CYberSynchrony project. The project consortium has made (and will make in the future) all public deliverables available on the CYberSynchrony project website (link) as they pass through the official approval and publication process. The Open call applicants are strongly advised to consult all deliverables listed in Table 8, to understand technical specifications, architectural principles, and integration expectations relevant to their proposal.

Access to non-public, technical implementation details (e.g., API documentation, sandbox access) will only be granted to successful applicants during the sub-grant agreement preparation phase.

Table 8 CYberSynchrony public deliverables related to the Open Calls

Deliverable Title	Deliverable no.	Access Links (PDF files)
Cybersecurity landscape and threat analysis, end-user requirement analysis, use case definition, and CYberSynchrony Framework – Final version	D2.2	Link
Enhanced Threat Intelligence System v1	D3.1	Link
Risk Scenario Analysis Toolkit v1	D3.2	Link
Integrated Cybersecurity Monitoring Suite v1	D4.1	Link
Automated Response Toolkit v1	D4.2	Link
Secure Data Exchange Platform v1	D5.1	Link
Evidence Integrity System v1	D5.2	Link
CYberSynchrony Integration Blueprint & Use Case Portfolio v1	D8.1	Link