CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

CyberSecDome Open Call

Round 2 Guide

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Table of Contents

1 Introduction 3
2 Objectives and Scope of Round 2 4
3 Open Call Topic for Round 2 5
3.1 CyberSecDome Architecture and Tools Overview 5
3.1.1 Key Architectural Components 5
3.1.2 Integrated AI Tools 6
3.1.3 Role of VR Interfaces 6
4 Eligibility and Funding Scheme 7
4.1 Eligible Applicants 7
4.2 Consortium Rules 7
4.3 Funding Scheme 7
4.4 Application Limits 7
4.5 Compliance Obligations 8
5 Proposal Submission Guidelines 9
5.1 Submission Requirements 9
5.2 Platform Access and Applicant Responsibilities 9
5.3 Submission Deadline and Exceptions 9
5.4 Applicant Support 9
6 Evaluation Process 10
6.1 Evaluation Structure 10
6.2 Evaluation Criteria 11
6.3 Selection Rules ..... Error! Bookmark not defined.
6.4 Transparency and Communication 12
7 Timeline and Key Dates (Tentative) 13
8 Support and Additional Resources 14
8.1 Help Desk 14
8.2 Relevant Documentation & Resources Links 14
8.3 Additional Information 14

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

1 Introduction

The CyberSecDome project, funded under Horizon Europe (Grant Agreement No. 101120779), is an ambitious initiative aimed at enhancing the resilience, security, privacy, and accountability of complex digital infrastructures. The project integrates cutting-edge Artificial Intelligence (AI), Machine Learning (ML), and Virtual Reality (VR) technologies to support real-time intrusion detection, incident response, and forensic investigation across diverse sectors.

During its first Open Call (Round 1), CyberSecDome successfully engaged stakeholders from 22 countries, resulting in the selection of nine sub-granted projects. These projects validated core components of the platform, including AI-driven threat detection, dynamic risk assessment, and immersive VR interfaces. Round 1 provided critical insights into user experience, system integration, and sector-specific needs, focusing on initial prototyping and domain-specific feedback, particularly in the aviation and telecommunications sectors.

Round 2 of the Open Call builds upon this foundation and aims to validate the complete, integrated CyberSecDome prototype in real-world operational contexts. It incorporates lessons learned from Round 1, including improvements to documentation clarity, outreach, evaluation methodology, and domain diversity.

This General Guide provides applicants with essential information on the structure, rules, scope, and procedures of the Round 2 Open Call.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

2 Objectives and Scope of Round 2

Round 2 builds directly upon the outcomes, lessons learned, and technical maturity achieved during Round 1. It is strategically designed as the final validation phase of the CyberSecDome Open Call mechanism, aiming to demonstrate the scalability, adaptability, and effectiveness of the fully integrated CyberSecDome prototype across real-world environments.

Whereas Round 1 focused on the evaluation and testing of individual modules and components (AI-driven detection, risk analysis, automated penetration testing, and VR-based interfaces), Round 2 shifts the emphasis to end-to-end deployment. The core objective is to gather deployment-level evidence of performance and impact under operational conditions, contributing directly to final refinements and exploitation readiness.

Only one topic is included in Round 2, centred on full deployment and cross-domain validation. To maximise its relevance and reach, the call encourages participation from underrepresented or complementary domains beyond aviation and telecommunications, such as energy, healthcare, finance, manufacturing, and smart cities.

The primary goals of Round 2 are to:

1. Validate the final integrated platform, including AI-enhanced threat detection, dynamic risk assessment, incident investigation, and VR-driven situational awareness.
2. Demonstrate interoperability and impact in new critical domains, extending the reach of CyberSecDome.
3. Collect quantitative and qualitative feedback from real-world use cases to inform final technical refinements.
4. Strengthen exploitation pathways through operational testing and alignment with sector-specific requirements.
5. Support the uptake of CyberSecDome outputs by SMEs and critical infrastructure operators.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

3 Open Call Topic for Round 2

Topic Title: Full Deployment and Validation of the Final Integrated CyberSecDome Prototype

Target Domains: Healthcare, Energy, Finance, Manufacturing, Public Sector/Smart Cities etc

Maximum Funding[1]: Up to €120,000 per project

This topic invites applicants to deploy and validate the fully integrated CyberSecDome platform in real-world operational environments across diverse critical domains. Unlike Round 1, which focused on evaluating individual components or subsystems, Round 2 proposals must demonstrate end-to-end integration and the practical utility of the CyberSecDome ecosystem in specific use cases.

Applicants are expected to:

- Deploy and test the full CyberSecDome prototype, including its AI-enhanced tools, VR interfaces, and collaborative modules.
- Propose domain-specific use cases that complement the project's existing pilots in aviation and telecommunications.
- Provide structured feedback on performance, usability, interoperability, and operational impact.
- Collaborate with the CyberSecDome Open Call Implementation Team (OCIT) and technical partners for onboarding, monitoring, and integration support.

Selected proposals will play a key role in demonstrating the maturity, relevance, and adaptability of the CyberSecDome solution in real-world settings.

3.1 CyberSecDome Architecture and Tools Overview

The CyberSecDome platform is a modular, AI-driven cybersecurity solution enhanced with Virtual Reality (VR) capabilities and real-time collaboration features. It was designed to support dynamic risk assessment, incident management, threat detection, and stakeholder coordination across digital infrastructures.

In Round 2, applicants will access and deploy the fully integrated CyberSecDome prototype, comprising the following core components and services:

3.1.1 Key Architectural Components

- Threat Detection Engine (TDE): Aggregates network, log, and system telemetry to detect and assess cybersecurity threats using advanced AI models.
- Incident Management System (IMS): Coordinates and automates response workflows, helping analysts assess incidents and recommend response paths.

[1] *If applicants propose a total project budget higher than the Maximum Funding, they must cover the difference themselves or by other funds. No proposal, regardless of the applicant's status, can receive more than €120,000 (see Annex Section 5.1.3 of the Open Call General Guide for more details).*

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- Dynamic Risk Assessment (DRA): Continuously evaluates system risk posture and simulates attack impacts based on asset criticality and threat landscape.
- Collaborative Threat Intelligence Module (CISM): Enables threat information exchange across deployments in a secure and privacy-preserving manner.
- VR-Enhanced Situational Awareness Interface: Offers immersive 3D visualisation of infrastructure, attack flows, and incident response coordination.

3.1.2 Integrated AI Tools

- Incident Investigation Tool: Predicts future attack paths and correlates incidents using machine learning on historical data.
- Automated Penetration Testing Tool: Simulates real-world attacks in a controlled manner to identify vulnerabilities with minimal manual effort.
- SIEM Integration Tool: Connects with existing SIEMs to process logs and trigger automated incident analysis across data sources.

3.1.3 Role of VR Interfaces

Most major components feature VR extensions, allowing users to:

- Manage active incidents collaboratively
- Review dynamic risk profiles visually
- Interact in shared VR workspaces with remote teams

Important for Applicants:

During Round 2, selected projects will test the platform as a complete and integrated environment. Applicants are not expected to develop or modify these tools, but to integrate them into their own infrastructure, execute test cases, and report performance and usability insights to the CyberSecDome team.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

4 Eligibility and Funding Scheme

To ensure fairness, transparency, and alignment with the Horizon Europe Programme, Round 2 of the CyberSecDome Open Call retains the core eligibility framework from Round 1, with additional clarifications and improvements based on lessons learned.

4.1 Eligible Applicants

Applicants must meet all the following conditions:

- Be legal entities (private or public) established in an EU Member State or a Horizon Europe Associated Country at the time of the Open Call deadline.
- Include at least one SME, either as a sole applicant or within a consortium. The SME must meet the definition under the EU Recommendation 2003/361/EC.
- Proposals submitted by large enterprises and academic/research institutions are also eligible only if an SME is the leading or co-leading partner.
- All applicants must confirm financial capacity to support the proposed work until reimbursement. Financial validation may be requested by the consortium.
- UK and Switzerland remain ineligible due to non-association with Horizon Europe during the 2023–2025 timeframe.

4.2 Consortium Rules

Single applicants or consortia of up to three (3) legal entities are allowed to participate, provided that at least one SME is involved and responsible for the implementation. While cross-border collaborations are encouraged to foster wider cooperation and innovation, they are not a mandatory requirement.

4.3 Funding Scheme

Maximum funding per proposal is €120,000. Funding rates vary depending on the type of organisation: SMEs can receive up to 100% of eligible costs, while large enterprises, RTOs, and universities can receive up to 50%. This means that the proportion of funding you can get depends on your organisation's category, covering a significant part of the costs directly related to the project, within the specified limits.

Eligible costs must be incurred after the Sub-Grant Agreement is signed and should be directly related to the proposed use case and implementation activities. Additionally, these costs need to comply with Horizon Europe cost eligibility guidelines, meaning they should be actual, necessary, documented, and reasonable.

4.4 Application Limits

To ensure diversity and equal opportunity:

- Each legal entity can submit only one proposal under Round 2 (as there is only one topic).

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- Applicants who submitted to Round 1 but were not selected for funding may re-apply in Round 2 with an updated and aligned proposal.
- Projects funded in Round 1 cannot re-apply.

4.5 Compliance Obligations

Applicants must ensure the following:

- **No double funding**: The same activities cannot be funded by other EU instruments.
- **No conflicts of interest**: Applicants must disclose any conditions that could affect the objectivity of the evaluation process.
- **No fraudulent activity**: Entities must not be under investigation or conviction for fraud or financial irregularities.

Proposals must be submitted in English and include all required sections and documentation as defined in the Proposal Template.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

5 Proposal Submission Guidelines

All proposals for CyberSecDome Open Call Round 2 must be submitted exclusively via the F6S platform, the designated interface for managing submissions and communications.

5.1 Submission Requirements

Format: Proposals must be submitted as a single PDF file, following the official Round 2 Proposal Template (available at the CyberSecDome website).

- Proposals must be written entirely in English.
- Only proposals responding to the Round 2 topic will be considered eligible.
- All required sections and documents must be complete and submitted before the deadline.

5.2 Platform Access and Applicant Responsibilities

F6S platform access requires registration. The submission portal will open alongside the launch announcement.

Applicants are strongly advised to:

- Begin preparing early to avoid system bottlenecks near the deadline
- Upload their final proposal well in advance of the closing date
- Regularly check their F6S dashboard and messages for updates, clarifications, or communication from the CyberSecDome OCMT

5.3 Submission Deadline and Exceptions

- No deadline extensions will be granted under any circumstances.
- No exceptions will be made for late submissions due to platform issues or user error.
- If technical difficulties are encountered, these must be reported to the help desk via F6S no later than one hour before the final deadline.
- Proposals uploaded or modified after the deadline timestamp will not be considered.

5.4 Applicant Support

One or more public webinars will be organised during the call period to explain the call objectives, topic scope, and submission process, including live Q&A. No personalised proposal review or one-on-one consultations will be provided

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

6 Evaluation Process

The evaluation process for CyberSecDome Open Call Round 2 will be based on a simplified and transparent scoring model, ensuring clarity for applicants and efficiency for evaluators.

6.1 Evaluation Structure

Each proposal will be reviewed by:

- Two expert evaluators will be assigned based on topical expertise and absence of conflict of interest.
- If significant discrepancies arise between the two evaluator scores, a HoT may consult both evaluators before finalising the ESR.

All evaluations will be coordinated by the Open Call Management Team (OCMT), which ensures process integrity, scoring consistency, and compliance with the Grant Agreement.

Scoring scale:

- 0 – Fail (not addressed)
- 1 – Poor
- 2 – Fair
- 3 – Good
- 4 – Very Good
- 5 – Excellent

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

6.2 Evaluation Criteria

Each proposal will be assessed based on the following five criteria, using a simplified scoring scale from 0 to 5 points per criterion:

Criterion	Thinks to be considered during evaluation process	Weight	Score Range	Threshold
Relevance & Alignment	Do the defined **Key Performance Indicators (KPIs)** measure the effectiveness of CyberSecDome's solutions?/ Does the use case fit within the CyberSecDome domain?/ Is the proposal aligned with the technical requirements expected in the CyberSecDome framework?	25%	0-5	3
Excellence	Does the proposal provide a technically sound **use case** to test the cybersecurity solutions developed by CyberSecDome?/ Does the proposal aim to significantly enhance the resilience and security of EU Digital Infrastructures?/ Is the proposal aligned with the strategy of the CyberSecDome technical environment?	25%	0-5	3
Impact	Are measurable indicators relevant to assess the effectiveness of these enhancements in mitigating **cyber threats**?/ What strategies does the proposal employ for disseminating project outcomes to relevant stakeholders?/ What impact will the applicant have in adopting CyberSecDome solutions?/ Can the applicant demonstrate a clear pathway to provide technical feedback to the CyberSecDome consortium?	25%	0-5	3
Implementation	Does the proposed **implementation plan** align with the objectives outlined in the Open Call, with clear milestones/ How does the applicant team's expertise contribute to the successful execution of the proposed activities	15%	0-5	3
Value for Money	Does the proposed work plan account for **risks and challenges** with proper mitigation strategies in place?/ Is the budget well-justified, and does the proposal include a contribution from additional funding?	10%	0-5	3

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

6.3 Selection Rules

- Proposals must score at least 3 out of 5 in each individual criterion.
- They must also achieve a minimum overall weighted score of 3.5 out of 5 to be eligible for funding.
- In the event of a tie, the **Excellence** score will serve as a tiebreaker.
- Final selection will depend on the available budget and the ranking position.

6.4 Transparency and Communication

All applicants will receive their Evaluation Summary Report (ESR) once the selection process is completed.

Successful applicants will be invited to sign a Sub-Grant Agreement and begin onboarding with the CyberSecDome implementation team.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

7 Timeline and Key Dates (Tentative)

The Round 2 Open Call will follow a tightly managed timeline to ensure proper coordination with the implementation and monitoring phases of the Round sub-projects. All dates below are tentative and subject to confirmation at the time of the call launch.

Milestone	Tentative Date / Period	Description
Finalisation of Documentation	July 2025 (M23)	Open Call documentation and internal procedures finalised by the OCMT.
Open Call Announcement	August, 2025 (M24)	Official call launch, full documentation bundle published on F6S and website.
Proposal Submission Window	August – September 2025 (M24–M25)	Applicants submit proposals via F6S. Deadline: **September 30, 2025 at 17:00 Brussels Time**
Eligibility Check	October 1–7, 2025 (M26)	Formal verification of applicant and proposal eligibility.
Evaluation Period & Ranking	October 8 - November 3, 2025 (M27)	Independent review and scoring of eligible proposals by evaluators and HoTs. Final consolidation of evaluations and proposal ranking by topic.
Notification of Results	November 7, 2025 (M27)	Applicants receive Evaluation Summary Reports and funding decisions.
Sub-Grant Agreement Signing	November 10–21, 2025 (M27)	Selected beneficiaries sign their Sub-Grant Agreements with the coordinator.
Project Start	December 1, 2025 (M28)	Funded projects officially commence activities.
Project End Final Review & Reporting	August 15, 2026 (M36)	End of implementation period for Round 2 projects. Final progress assessment and reporting against KPIs.

Important: No deadline extensions will be granted. Applicants are responsible for submitting their proposals before the indicated deadline. Technical issues must be reported at least one hour prior to the closing time

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

8 Support and Additional Resources

8.1 Help Desk

The CyberSecDome Help Desk is available to provide support during the proposal preparation and submission process. Applicants are encouraged to reach out to the Help Desk for assistance with technical issues, clarification on submission guidelines, or any other inquiries related to the Open Call.

Help Desk Contact:

Email: info@cybersecdome.eu

Applicants are advised to contact the Help Desk well in advance of the submission deadline to ensure any issues are resolved on time.

8.2 Relevant Documentation & Resources Links

Several documents are available to assist applicants in preparing their proposals and understanding the requirements for Round 2. These resources provide detailed information about the Open Call, submission guidelines, and the evaluation process. Round 2 Full Documentation Bundle: https://cybersecdome.eu/open-call-round-2/

8.3 Additional Information

To stay updated on announcements, deadlines, and new resources, applicants are encouraged to check the CyberSecDome website regularly. Updates will also be sent via the CyberSecDome newsletter, which applicants can subscribe to for the latest news and reminders.

This document is subject to validation by the CyberSecDome OCMT and Project Coordinator. Final release will accompany the official Open Call announcement.