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

CyberSecDome Open Call

Round 1 Guide

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

Table of Contents

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

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

1 Introduction

The information provided in this document is relevant to Round 1 of the CyberSecDome programme. Please refer to the main CyberSecDome Open Call document for the overall programme guidelines, requirements, and evaluation methodology.

1.1 Overview of Round 1

The **CyberSecDome Open Call** aims to bring together industry stakeholders, SMEs, and research organisations to advance the development of AI-enabled and VR-enhanced cybersecurity tools. **Round 1** of the Open Call focuses on the validation and testing of early-stage innovative cybersecurity solutions. Selected applicants will have the opportunity to collaborate with the CyberSecDome consortium to integrate and test the CyberSecDome early prototype and its functionalities within real-world environments, contributing to improving Europe's digital infrastructure security.

The primary goal of **Round 1** is to evaluate and refine the early prototype of the CyberSecDome system and its tools. Participants will be expected to test the system's capabilities, provide feedback, and demonstrate its potential in addressing current cybersecurity challenges. This feedback will inform future iterations of the CyberSecDome platform and guide the development of advanced use cases for Round 2.

1.2 CyberSecDome Project and Round 1 Objectives

The CyberSecDome project, funded by the European Union's Horizon Europe programme, is dedicated to improving cybersecurity by integrating advanced AI-driven tools and Virtual Reality (VR) technologies. The project aims to enhance threat detection, incident management, and response across digital infrastructures in various sectors, ensuring a more secure and resilient environment for businesses and public institutions.

Round 1 specifically aims to:

- **Validate early-stage prototypes** of the CyberSecDome system, including its AI-enhanced threat detection capabilities and VR-based situational awareness tools.
- **Engage SMEs and other stakeholders** in testing these tools in simulated or controlled environments.

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

- **Collect feedback** on the system's usability, scalability, and effectiveness to inform improvements for future iterations.
- **Demonstrate practical applications** of the CyberSecDome solutions across various sectors, including energy, transportation, finance, and healthcare.

Participants in Round 1 will play a critical role in shaping the development of the CyberSecDome platform and its applications for cybersecurity across Europe.

1.3 Scope and Focus Areas of Round 1

Round 1 of the CyberSecDome Open Call focuses on predefined **topics** that align with the project's overarching goals. Each topic reflects specific cybersecurity challenges that can be addressed using AI-driven and VR-enhanced technologies. Applicants are expected to propose solutions that align with one or more of these focus areas, showcasing how their solutions can integrate with the CyberSecDome framework.

The main focus areas for Round 1 include:

- **Threat Detection and Incident Management**: Leveraging AI to detect and respond to cybersecurity threats in real-time, reducing the time it takes to identify and mitigate incidents.
- **Collaborative Threat Intelligence Sharing**: Proposing solutions that enhance collaboration and information-sharing between stakeholders, improving collective cybersecurity resilience.
- **Immersive VR for Situational Awareness**: Using VR technologies to provide real-time visualisations of cybersecurity threats and enhance decision-making during critical incidents.
- **Scalability and Flexibility**: Ensuring that the proposed solutions can scale to meet the needs of diverse sectors and infrastructure environments.

Applicants are encouraged to propose solutions that not only address these specific areas but also demonstrate how their technology can be expanded and adapted for future rounds.

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

2 Topics for Round 1

Round 1 of the CyberSecDome Open Call focuses on specific cybersecurity challenges and use cases that align with the project's overarching goals. Applicants are invited to submit proposals addressing one or more of the following topics. Each topic reflects a critical area of cybersecurity, providing an opportunity for applicants to contribute innovative solutions.

The table below outlines the **Round 1 Topics**, including a brief description and the maximum funding available for each topic:

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

Topic No.	Topic Title	Description	Open Call Contribution (Max)
1	Evaluation & Testing of Integrated CyberSecDome Prototype	This topic focuses on a thorough evaluation & testing of the integrated CyberSecDome prototype, including its virtual reality (VR) functionalities. Applicants are expected to test the system's usability, scalability, and effectiveness in real-world cybersecurity scenarios, providing insights into system limitations and improvement opportunities. The evaluation process must cover diverse threat landscapes and operational settings.	Up to €120,000 per project
2	Advanced Risk Assessment Using the Dynamic Risk Analysis (DRA) functionality	This topic invites applicants to perform a comprehensive risk assessment leveraging **CyberSecDome's Dynamic Risk Analysis (DRA)** tool. Projects should focus on evaluating interdependencies among assets, quantifying potential threat impacts, and providing detailed insights into system vulnerabilities. Proposals should include a comprehensive list of assets to be tested, methodologies for dynamic analysis, and actionable recommendations for risk mitigation.	Up to €35,000 per project
3	Comprehensive Incident Investigation and Response	This topic addresses the end-to-end process of incident investigation and response, from log capture and intrusion detection to automated incident analysis and mitigation. Proposals should demonstrate integration of multiple CyberSecDome functionalities, such as SIEM, Prophecy, FVT, and adaptive response mechanisms. Projects should also provide feedback mechanisms for continuous system improvement.	Up to €55,000 per project

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

4	AI-Driven Automated Penetration Testing	This topic seeks proposals that focus on testing CyberSecDome's automated penetration testing functionalities. Applicants will evaluate AI-driven attack modeling and simulation tools, validating their ability to identify vulnerabilities and assess system resilience. Proposals should include clear testing plans and agreement to operate within CyberSecDome's controlled infrastructure environment.	Up to €20,000 per project
5	Generation of Security-Related Datasets for AI-Enhanced Tools Training	This topic focuses on the generation of security-related datasets through simulation of cyber-attack scenarios. Proposals should describe methods for creating high-quality datasets covering a broad spectrum of threats and vulnerabilities. These datasets will contribute to the training and validation of AI models within CyberSecDome. Projects must ensure datasets are comprehensive, anonymized, and compliant with ethical and legal standards	Up to €10,000 per project

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

Important Notes:

- Applicants are allowed to submit multiple applications for different topics; however, if a proposal is selected for **Topic 1 (Evaluation & Testing of Integrated Prototype**), the other applications will be dropped.
- In each case, **the Max contribution refers to the maximum funding provided per proposal**. If applicants propose a total project budget higher than these amounts, 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).
- Proposals must demonstrate a clear **alignment** with the objectives of the selected topic(s) and provide detailed descriptions of the technical and operational approach.

3 CyberSecDome Architecture and Tools

In Round 1 of the CyberSecDome Open Call, participants will have the opportunity to validate and integrate their proposed use cases within the broader **CyberSecDome architecture**. The architecture is designed to leverage **AI-enhanced tools** and **VR-based technologies** to enhance cybersecurity capabilities, offering real-time threat detection, incident management, and risk assessment functionalities. This section provides a high-level overview of the CyberSecDome architecture and the key tools that applicants will interact with during Round 1.

3.1 CyberSecDome High-Level Architecture

The CyberSecDome architecture is a modular and flexible cybersecurity platform built to integrate cutting-edge AI technologies and immersive VR components to support the secure management of digital infrastructures. With the integration of these technologies, it provides a comprehensive, layered system that enables real-time threat monitoring, response, and assessment across various sectors, such as finance, transportation, energy, and healthcare while also greatly enhancing and optimizing the decision-making process of its operators.

Key architectural components include:

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

- **Central Threat Detection Engine (TDE):** This core engine is responsible for detecting and assessing any potential intrusion attempts. The TDE supervises and protects various endpoints of the system (e.g., workstations, computers, edge & IoT devices) and it integrates various data sources (e.g., network traffic, security logs, incident reports), applying state-of-the-art AI methods to detect and predict cyber threats in real-time. It is responsible for aggregating data from different sensors and systems to deliver a cohesive threat landscape overview.
- **Incident Management System (IMS)**: This system manages the incident response workflow, automating actions such as threat reporting and incident handling. Upon confirmation of the existence of a cybersecurity threat inside the system, the IMS is tasked with closely examining and evaluating the incident by using ML-assisted techniques in order to add valuable insight (e.g., hosts affected, potential hidden relationships with other incidents etc.) to it. Additionally, it supports security specialists by managing and composing an optimal course of action to tailored to the neutralization of each threat.
- **Dynamic Risk Assessment (DRA) Tool**: The DRA evaluates the risk posture of an organization based on real-time threat intelligence. By continually overseeing each component of the system along with its role, its functioning and importance to the system, it updates risk profiles and assesses vulnerabilities to prioritize actions for mitigating potential attacks. Should a threat arise, the DRA component attempts to evaluate in detail the estimated impact of it on the underlying system by consulting up-to-date threat databases.
- **Collaborative Threat Intelligence Sharing Module**: This module facilitates secure and collaborative threat intelligence sharing between different CyberSecDome deployments and instances. It ensures that all current threat information is shared and that each new threat identified by some CyberSecDome instance will be made known to every other active deployment to further enhance the common cause against emerging cyberthreats.
- **VR-Enhanced Situational Awareness Interface**: The innovative inclusion of the VR platform allows users to engage with live threat data in an immersive environment. This virtual environment replicates and provides various views of the actual, real-world digital infrastructure, enhancing decision-making and enabling cross-functional teams to work together during critical incidents.

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

The architecture's modular design ensures that solutions proposed in Round 1 can be integrated smoothly and tested within this advanced ecosystem.

AI-Enhanced CyberSecDome Tools

The CyberSecDome platform integrates a suite of sophisticated **AI-enhanced tools** designed to detect potential threats in a timely manner, deeply examine security incidents and mitigate cyber threats in an optimal way. These tools form the backbone of the platform's capability to predict and respond to evolving cyber risks.

Key AI Tools:

- **The Incident Investigation Tool**: This tool uses machine learning algorithms to predict future attack vectors based on historical threat data as well as finding potential hidden relationships between attacks. By analyzing vast datasets, Prophecy can uncover links that would otherwise go unnoticed, foresee potential cybersecurity risks and suggest targeted and preventive actions before an incident occurs.
- **Dynamic Risk Assessment (DRA) Tool**: As a core element of the platform, DRA evaluates risk in real-time, incorporating the latest threat intelligence to update an organization's risk profile. Through its upkeep of a stateful and detailed inventory of all the assets of the monitored information system, it helps prioritize mitigation actions based on threat severity and impact.
- **Automated Pen-Testing Tool**: This tool automates the penetration testing process, simulating real-world cyber-attacks to identify vulnerabilities in an organization's infrastructure. It is able to run and execute an extensive selection of penetration testing workloads for a wide array of scenarios and services with minimal or no manual user intervention. The automated nature of the tool reduces the time required for security testing and increases the breadth of scenarios that can be simulated.
- **Security Information and Event Management (SIEM) Integration**: This tool integrates with existing SIEM systems to collect, analyze, and respond to security events. The SIEM, in its role of aggregating, normalizing and storing all kinds of security logs, is a significant tool of the system. By automating the upload and

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

analysis of logs from various sources, the SIEM integration ensures that incident response is timely and based on the most accurate data.

These tools work in tandem to provide a robust cybersecurity defense mechanism that is both predictive and responsive, allowing organizations to preemptively mitigate threats and respond effectively when incidents occur.

Role of VR in CyberSecDome

Virtual Reality (VR) plays a crucial role in the CyberSecDome platform, providing an immersive interface for engaging with real-time threat data, system performance metrics, and incident response workflows. Each AI tool integrated within the platform has a VR component, allowing users to visualize complex data in an intuitive and interactive environment.

VR Features of CyberSecDome Tools:

- **Incident Investigation Tools (VR Component):** The VR interface of Prophecy provides a visual representation of predicted cyber-attack vectors, allowing users to explore potential attack paths in a 3D environment. This enables security teams to better understand how future threats may unfold and prepare accordingly.
- **Dynamic Risk Assessment (VR Component):** The DRA tool's VR interface offers real-time visualization of an organization's risk profile, displaying vulnerabilities and their potential impact on critical infrastructure. Users can navigate through different risk scenarios, simulating the effects of potential attacks and the effectiveness of mitigation strategies.
- **Incident Management System (VR Component):** The IMS integrates a VR dashboard that enables cybersecurity teams to manage incidents in a fully immersive environment. Teams can coordinate responses to real-time incidents, visualize the progression of cyberattacks, and deploy countermeasures using VR-enhanced interfaces.
- **Collaborative Threat Intelligence (VR Component):** The VR-enhanced CISM allows multiple stakeholders to collaborate in a shared virtual space, analyzing

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

threat intelligence from different sources. This collaborative environment facilitates better coordination between geographically dispersed teams.

The VR components of CyberSecDome aim to enhance situational awareness and decision-making, transforming how cybersecurity professionals interact with threat data and respond to critical incidents.

4 Submission Requirements for Round 1

Applicants for Round 1 of the CyberSecDome Open Call must submit a comprehensive proposal that addresses the specific objectives and evaluation criteria outlined for the call. This section provides detailed guidance on the structure and content required for each part of the proposal, ensuring alignment with the evaluation criteria for **Alignment**, **Excellence**, **Impact**, **Implementation**, and **Value for Money**.

4.1 Administrative Information

In this section, applicants are expected to provide basic details about their organization and the proposal:

- **Proposal Title**: A concise title (maximum 100 characters) that clearly describes the project.
- **Acronym**: A short acronym for the project (maximum 12 characters).
- **Topic(s) Covered**: Enlist the topic(s) your proposal aims to cover.
- **Applicant Details**: Legal name of the organization(s), contact information, country of origin, and **Participant Identification Code (PIC)** (if applicable).
- **Consortium Members** (if applicable): A list of consortium members, including their roles and contact details.
- **Contact Person**: The primary point of contact for the proposal (name, role, email, phone).
- **Proposal Duration**: Expected project duration in months, aligned with the proposed work plan.
- **Requested Funding**: Indicate the total requested funding and ensure it complies with the funding limitations outlined.

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

4.2 Excellence Section

This section focuses on the **technical soundness**, **innovation**, and **alignment** of the proposed project with the CyberSecDome objectives. Proposals will be evaluated on their ability to address the key cybersecurity challenges identified in the Open Call topics.

- **Objectives**: Clearly state the measurable objectives of the project and explain how they align with the challenges identified in Round 1. Proposals must demonstrate how the solution will contribute to the CyberSecDome framework and EU Digital Infrastructure.
- **Relevance to CyberSecDome**: Explain how the proposal fits within the CyberSecDome architecture, focusing on AI-enhanced threat detection or VR-based situational awareness. Emphasise the technical feasibility and innovation of the solution.
- **Technical Innovation**: Highlight any novel approaches, technologies, or methodologies that will be used. The proposal must demonstrate **technical soundness** and the ability to provide innovative solutions for cybersecurity challenges.
- **Use Case Description**: Provide a detailed description of the **use case(s)** that will be tested. Ensure that the use case demonstrates relevance to the CyberSecDome domain and presents a complex infrastructure for testing the solution's capabilities.
- **Technical Feasibility**: Include a clear explanation of how the proposed technologies or tools will be integrated into the CyberSecDome system, emphasizing their ability to address sophisticated cybersecurity threats.

4.3 Impact Section

The Impact Section focuses on the potential outcomes of the proposed solution, both in terms of business and technical impact. Proposals must define measurable Key Performance Indicators (KPIs) and explain how the solution will contribute to the overall goals of CyberSecDome and the cybersecurity landscape.

- **Exploitation and Sustainability**: Detail how the results of the project will be exploited and sustained beyond the funding period. This includes plans for commercialization, scalability, or deployment in real-world environments.

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

- **KPIs (Key Performance Indicators)**: Clearly define KPIs that will be used to measure the effectiveness of the proposed solution. The KPIs should assess **cyber threat mitigation**, **incident response improvements**, or **system resilience**.
- **Market and Technical Impact**: Describe the expected impact on both the cybersecurity market and technical infrastructure. This should include how the solution will enhance cybersecurity across sectors such as finance, energy, transportation, or healthcare.
- **Stakeholder Engagement**: Explain how relevant stakeholders (e.g., end-users, partners) will be involved in the project. A strong **dissemination strategy** should be presented, outlining how the project results will be communicated to key stakeholders.
- **Contribution to CyberSecDome**: Provide a clear explanation of how the project will contribute to the CyberSecDome ecosystem. Proposals must demonstrate a pathway for providing **technical feedback** to the CyberSecDome consortium.

4.4 Implementation Section

The Implementation Section outlines how the project will be executed, including timelines, resources, risk management, and the team's expertise. This section must demonstrate that the applicant can effectively deliver the proposed solution within the specified budget and timeframe.

- **Work Plan**: Provide a detailed work plan that outlines all project activities, tasks, and milestones. The work plan should clearly show how the project aligns with the CyberSecDome objectives and includes a schedule for implementation and validation.
- **Milestones and Deliverables**: Create a timeline of key milestones and deliverables. Ensure that the work plan is realistic, with clear steps for design, integration, testing, and feedback.
- **Risk Management**: Include a detailed risk assessment, identifying potential risks to the project and outlining mitigation strategies. This section must demonstrate a clear understanding of both **technical risks** and **resource management risks**.
- **Team Expertise**: Provide an overview of the team's qualifications, highlighting relevant expertise in cybersecurity, AI, VR, and related fields. Gender balance within the team is encouraged and will be positively evaluated.

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

- **Infrastructure**: Detail the infrastructure that will be used to execute the project, including cloud environments, on-premise servers, or virtualized systems.

4.5 Ethics and Data Management

Applicants must address ethical considerations and data management plans, particularly if personal data or sensitive information is involved.

- **Ethical Considerations**: Outline any ethical concerns related to the proposed solution, particularly in the context of data collection, storage, and usage. This includes any human-centered activities, such as user testing or behavioral data collection.
- **GDPR Compliance**: If personal data is collected, processed, or stored as part of the project, describe how you will ensure compliance with the General Data Protection Regulation (GDPR).
- **Data Management Plan**: Provide a detailed Data Management Plan (DMP) that outlines how data will be collected, stored, and shared. The plan should ensure that the data is managed securely and transparently, adhering to all applicable legal and regulatory requirements.

4.6 Budget and Resources

Proposals must include a well-justified budget that clearly outlines the financial resources required to deliver the project. The **Value for Money** criterion will assess the efficient use of funds and the project's ambition to leverage additional funding sources.

- **Budget Breakdown**: Provide a detailed budget breakdown that outlines **personnel costs**, **equipment**, **subcontracting**, and other direct costs. Ensure that the budget is aligned with the proposed activities and milestones.
- **Value for Money**: Justify the allocation of resources and demonstrate how the requested funding will be used efficiently. This includes addressing **cost-effectiveness** and providing evidence that the project will deliver significant value relative to its costs.
- **Co-Funding and Additional Resources**: If applicable, detail any co-funding or additional financial resources that will contribute to the project. Proposals that include contributions from other funding sources will be positively evaluated.

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

- **Justification of Costs**: Explain how the proposed budget supports the project objectives and the delivery of the expected outcomes. Include details on any infrastructure or tools that require investment.

5 Evaluation and Funding Scheme for Round 1

The evaluation and funding process for Round 1 of the CyberSecDome Open Call ensures that proposals are assessed fairly and transparently. This section outlines the minimum eligibility criteria and detailed evaluation criteria that all proposals will be assessed against, including the process by which they will be reviewed and scored by expert evaluators.

5.1 Eligibility Criteria

To be eligible for consideration in Round 1, proposals must meet the following minimum criteria:

Table 1. Eligibility Criteria

Eligibility Criteria
The applicant(s) is(are) a legal entity(ies) registered in an eligible country(ies) in 2023
At least one of the applicants is a **Micro, Small, or Medium-sized Enterprise (SME)**
The proposal requests less than or equal to **€120,000** of funding.
The applicants need to demonstrate **financial capability** to support the cost of the resources until the reception of financial support upon request.
The proposal is not supported by any other **EU funding.**
All partners involved declare there is **no double funding** for the project they are submitting.
All required sections of the proposal have been completed.
All required documentation has been provided
The proposal is written fully in English.

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

Proposals that do not meet these eligibility requirements will not proceed to the evaluation stage.

5.2 Evaluation Criteria

Once the eligibility criteria are met, proposals will be evaluated against a set of detailed criteria by an independent panel of experts. The evaluation process is designed to assess the **alignment**, **excellence**, **impact**, **implementation**, and **value for money** of each proposal. Each criterion will be scored based on a set of predefined questions.

Applicants can propose a total budget higher than the **Open Call Max Contribution**, but the funding they receive will be **capped at €120,000 per proposal**, regardless of the size of the budget or the applicant's status (SME or large industry). **Proposals with larger budgets will need to clearly justify the additional resources and explain how the excess will be funded. The evaluators will assess whether the overall budget is feasible and realistic**, ensuring that the project can be completed within the financial constraints provided by the Open Call.

Evaluation Questions and Scoring

The table below outlines the key questions evaluators will ask when assessing each proposal. A score of **0-5** will be assigned for each question, based on the following scale:

- **0**: Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
- **1**: Poor. The criterion is inadequately addressed or there are serious inherent weaknesses.
- **2**: Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.
- **3**: Good. The proposal addresses the criterion well, but a number of shortcomings are present.
- **4**: Very good. The proposal addresses the criterion very well, with a small number of shortcomings.
- **5**: Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

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

Detailed Evaluation Criteria

Table 2. Review Process questions and minimum required scores.

Criterion	Question	Score Range	Threshold
Alignment	Do the defined **Key Performance Indicators (KPIs)** measure the effectiveness of CyberSecDome's solutions?	0-5	3
	Does the use case fit within the CyberSecDome domain?	0-5	3
	Is the proposal aligned with the technical requirements expected in the CyberSecDome framework?	0-5	3
Excellence	Does the proposal provide a technically sound **use case** to test the cybersecurity solutions developed by CyberSecDome?	0-5	3
	Does the proposal aim to significantly enhance the resilience and security of **EU Digital Infrastructures**?	0-5	3
	Is the proposal aligned with the **strategy** of the CyberSecDome technical environment?	0-5	3
Impact	Are measurable indicators relevant to assess the effectiveness of these enhancements in mitigating **cyber threats**?	0-5	3
	What strategies does the proposal employ for **disseminating project outcomes** to relevant stakeholders?	0-5	3
	What impact will the applicant have in adopting CyberSecDome solutions?	0-5	3

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

	Can the applicant demonstrate a clear pathway to provide **technical feedback** to the CyberSecDome consortium?	0-5	3
Implementation	Does the proposed **implementation plan** align with the objectives outlined in the Open Call, with clear milestones	0-5	3
	How does the applicant team's **expertise** contribute to the successful execution of the proposed activities	0-5	3
Value for Money	Does the proposed work plan account for **risks and challenges** with proper mitigation strategies in place?	0-5	3
	Is the budget well-justified, and does the proposal include a contribution from **additional funding**?	0-5	3

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

Scoring and Thresholds

Each of the five criteria (Alignment, Excellence, Impact, Implementation, and Value for Money) will be scored based on a set of questions, each question scored on a scale of **0 to 5**. The total score for each criterion is calculated by summing the scores for each question within that criterion.

Weighting of the Criteria:

- **Alignment**: 20%
- **Excellence**: 30%
- **Impact**: 30%
- **Implementation**: 10%
- **Value for Money**: 10%

The final weighted score for each criterion will be calculated based on the following table:

Table 3. final weighted score for each criterion

Criterion	Max Points	Weighting	Maximum Contribution to Final Score
Alignment	15	20%	3.0
Excellence	15	30%	4.5
Impact	20	30%	6.0
Implementation	10	10%	1.0
Value for Money	10	10%	1.0

The **maximum possible score** for a proposal is **15.50**, based on the weighted contribution from each criterion.

Minimum Threshold:

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

- To be considered for funding, proposals must achieve a **minimum threshold score of 9.30.** This score is calculated by summing the minimum required scores across all questions.
- Each criterion must meet its respective minimum threshold for the proposal to proceed.

In the Event of a Tie: If two or more proposals receive the same final score, the **Impact** score will be used as the deciding factor.

5.3 Evaluation Process

The evaluation process consists of **several steps**, ensuring that each proposal is reviewed thoroughly and fairly:

Individual Evaluation: Each evaluator will review the assigned proposal independently and complete an Individual Evaluation Report (IER), scoring each criterion and providing written feedback.

Consensus Meeting: After the individual evaluation, evaluators will meet to discuss their scores and reach a consensus on each proposal. The **Evaluation Summary Report (ESR)** will reflect the agreed scores and include detailed comments on strengths, weaknesses, and areas for improvement.

Additional Evaluator (if needed): In cases where consensus cannot be reached, an additional evaluator will be assigned to review the proposal and help resolve any disagreements.

Final Ranking: Proposals that meet the minimum score will be ranked based on their total score. In the event of a tie, the **Impact** criterion score will be used to decide the ranking.

6 Timetable for Round 1

This updated section now includes the eligibility and evaluation criteria as well as the scoring process for **Round 1** of the CyberSecDome Open Call. Let me know if this updated version works for you or if further adjustments are needed!6. Timetable for Round 1

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

The following timetable outlines the key dates and deadlines for **Round 1** of the CyberSecDome Open Call. Applicants are encouraged to adhere strictly to these deadlines to ensure their proposals are considered for funding.

6.1 Key Dates and Deadlines

The timeline for Round 1 is structured to provide applicants with sufficient time for proposal preparation, submission, evaluation, and project execution. Missing any of the deadlines may result in disqualification from the call.

- Open Call Announcement: December 4, 2024
  The CyberSecDome Open Call is officially announced, and detailed information, including submission guidelines and topics, is made available to the public.
- Submission System Opens: December 10, 2024
  Applicants can submit their proposals via the CyberSecDome Digital Submission System built by AEGIS using the F6S platform.
- Proposal Submission Deadline: February 10, 2025 (17:00 CET)
  The final deadline for submitting proposals. Late submissions will not be accepted under any circumstances.
- Eligibility Check and Initial Review: February 12-13, 2025
  Submitted proposals undergo an eligibility check to ensure compliance with the administrative and eligibility requirements.
- Evaluation by Expert Panel: February 17-27, 2025
  The independent panel of experts evaluates eligible proposals based on the Alignment, Excellence, Impact, Implementation and Value for Money criteria.
- Consensus Meeting and Ranking: March 1-7, 2025
  The expert panel convenes to discuss the final scores and create a ranked list of proposals for funding.
- Notification of Results: March 14, 2025
  Applicants are notified of the evaluation results, including feedback from the expert panel.
- Grant Agreement Signing: March 24-28, 2025
  Successful applicants will sign the Grant Agreement, formalising the terms and conditions of the funding.
- Project Start: April 1st 2025
  Funded projects officially begin their activities.

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

Table 4: Open Call Round 1 Timetable

Stage	Date	Description
Open Call Announcement	December 4, 2024	The CyberSecDome Open Call is officially announced, and detailed information, including submission guidelines and topics, is made available to the public.
Submission System Opens	December 10, 2024	Applicants can start submitting their proposals via the CyberSecDome Digital Submission System.
Proposal Submission Deadline	February 10, 2025 (17:00 CET)	The final deadline for submitting proposals. Late submissions will not be accepted under any circumstances.
Eligibility Check and Initial Review	February 12-13, 2025	Submitted proposals undergo an eligibility check to ensure compliance with the administrative and eligibility requirements.
Evaluation by Expert Panel	February 27-27 2025	The independent panel of experts evaluates eligible proposals based on the Alignment, Excellence, Impact, Implementation, and Value for Money criteria.
Consensus Meeting and Ranking	March 1-7, 2025	The expert panel convenes to discuss the final scores and create a ranked list of proposals for funding.
Notification of Results	March 14, 2025	Applicants are notified of the evaluation results, including feedback from the expert panel.
Grant Agreement Signing	March 24-28, 2025	Successful applicants will sign the Grant Agreement, formalizing the terms and conditions of the funding.
Project Start	April 1, 2025	Funded projects officially begin their activities.

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

6.2 Application Process and Timeline

The application process follows a structured timeline to ensure that each phase of the Open Call is transparent and allows adequate time for proposal preparation, submission, and evaluation. The timeline is as follows:

- **Proposal Submission (December 10, 2024 – February 10, 2025)**: The submission system will be open for applicants to upload their proposals. It is recommended that applicants submit their proposals well in advance of the deadline to avoid last-minute technical issues.
- **Eligibility and Evaluation (February 10 – March 23, 2025)**: After the submission period closes, proposals will be checked for eligibility, and eligible proposals will be evaluated by an independent panel of experts.
- **Contracting and Project Start (March 24 – April 1, 2025):** Once the successful proposals are notified, the Grant Agreements will be signed, and projects will officially commence.

7 Frequently Asked Questions (FAQs) for Round 1

This section addresses common questions that applicants may have regarding the Round 1 submission process, eligibility, and technical details. These FAQs aim to provide clarity and guidance to ensure a smooth and successful application process.

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

Submission Process FAQs

Q1. How do I submit my proposal for Round 1?

All proposals must be submitted through the **CyberSecDome Digital Submission System**. Proposals submitted via email or other channels will not be considered. The submission platform will open on **December 10, 2025**, and the final deadline for submission is **February 10, 2025 (17:00 CET)**.

Q2. Can I edit my proposal after submission?

Yes, you can edit your proposal any time before the submission deadline. Once the deadline has passed, no further changes will be allowed.

Q3. What file format should I use for my proposal submission?

Proposals must be submitted in **PDF format only**. Ensure that all required sections are included and that the document complies with the formatting guidelines outlined in the submission form.

Q4. What happens if I encounter technical issues with the submission system?

If you experience technical issues while submitting your proposal, you should immediately contact the **CyberSecDome Help Desk**. Be sure to report any issues well before the submission deadline to avoid complications.

Q5. Can I submit multiple proposals?

Applicants can submit more than one proposal for round 1 only if they do not want to address topic 1.

Eligibility FAQs

Q6. Who is eligible to apply for Round 1 of the CyberSecDome Open Call?

Eligible applicants include SMEs, large enterprises, research institutions, and academic organisations established in an EU Member State or a Horizon Europe-associated country. Entities from the UK and Switzerland can also apply and successfully pass the evaluation process but are not eligible for funding due to the regulations under Horizon Europe that were in place in 2023.

Q7. Can applicants from Round 1 reapply in Round 2?

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

Yes, applicants who applied for Round 1 and did not receive funding may reapply for Round 2 with a revised proposal, provided that they meet the eligibility criteria for Round 2.

Q8. Are consortia allowed to apply?

Yes, consortia of a maximum of three (3) participating entities are allowed to apply. The consortium should include **at least one SME** as a partner. Each partner in the consortium must meet the eligibility criteria and contribute to the project objectives.

Q9. What are the funding limits for Round 1?

The maximum funding for any proposal in **Round 1 is €120,000**, regardless of the total project budget, the number of topics addressed, or the size of the consortium. This means that even if your proposed project budget exceeds €120,000, the Open Call Max Contribution will be capped at €120,000.

Q10. What is the % of the funding?

For **SMEs, up to 100% of eligible costs will be funded**, while **larger industries and other organisations will be funded at 50%** of their eligible costs, but no entity nor proposal, including those from consortia, will receive more than €120,000 from the Open Call. If a proposal's total budget exceeds €120,000, the applicants must cover the remaining costs from their own resources.

Q11. Are costs incurred before the project starts eligible for funding?

No, only costs incurred after the project start date (following the signing of the Sub-Grant Agreement) are eligible for funding.

Technical FAQs

Q12. What type of cybersecurity use cases are expected in Round 1?

Round 1 focuses on early-stage validation of **AI-enhanced** and **VR-based** cybersecurity solutions. Applicants should propose cases that align with the topics outlined in **Section 2**, including threat detection, incident response, and situational awareness using VR technologies.

Q13. How will integration with the CyberSecDome architecture be managed?

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

Applicants are expected to integrate their use cases with the **CyberSecDome architecture** during the project. Detailed technical documentation and support from the CyberSecDome technical team will be provided to assist with the integration process

Q14. What kind of infrastructure is required for testing the use cases?

Applicants should ensure that they have access to the necessary infrastructure to test and validate their proposed solutions. This may include **cloud environments**, **on-premise servers**, or **virtualized environments**. Specific infrastructure requirements should be outlined in the proposal.

Q15. Will I need to share my data during the project?

Yes, data sharing may be required during the project to ensure effective testing and validation of the CyberSecDome tools. However, all data sharing must comply with GDPR regulations, and any sensitive or personal data must be anonymized or pseudonymized.

Q16. What type of support will I receive during the project?

Successful applicants will have access to **technical support** from the CyberSecDome **Open Call Implementation Team (OCIT)**, including guidance on tool integration, system testing, and performance evaluation. Regular checkpoints will be scheduled to ensure smooth project execution.

Financial FAQs

Q17. How will the funding be disbursed?

Funding will be disbursed in **stages** based on the project's milestones. The initial payment of **30%** will be made **upon the signing of the Sub-Grant Agreement**, followed by an **interim payment** (up to **30%**) based on a positive interim assessment, and the **final payment after the completion** of the project.

Q18. Are there any restrictions on how the funds can be used?

Yes, the funds must be used strictly for eligible project costs, such as **personnel**, **equipment**, **travel**, and **subcontracting**. Detailed justification of all expenses will be required in the financial reports.

Q19. Can I include subcontracting in my budget?

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

Yes, subcontracting is allowed but should be justified as necessary for the completion of project tasks. Subcontracting costs must be duly justified in the application and detailed in the budget, and subcontractors must comply with the same eligibility and reporting requirements as the primary beneficiary.

Q19. What happens if my project is delayed?

If unforeseen delays occur, you must notify the **CyberSecDome Open Call Management Team (OCMT)** as soon as possible. Extensions may be granted in exceptional cases, but failure to meet key milestones may result in funding reductions or project termination.

8 Additional Resources for Round 1

To assist applicants in preparing their proposals and successfully navigating the submission process for Round 1, the CyberSecDome consortium offers several resources, including webinars, info sessions, and support services. These resources are designed to provide applicants with valuable insights and guidance to enhance the quality and relevance of their proposals.

Webinars and Info Sessions

Several webinars and info sessions will be held to provide potential applicants with a detailed overview of the Open Call, the submission process, and key expectations for Round 1. These events will cover critical topics such as proposal preparation, CyberSecDome architecture, integration of AI and VR technologies, and addressing the evaluation criteria.

Applicants can register for the webinars and info sessions via the CyberSecDome website. All sessions will be recorded and made available on the website for those unable to attend live.

8.1 Help Desk Information

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:

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

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 in a timely manner.

8.2 Relevant Documentation & Resources Links

Several documents are available to assist applicants in preparing their proposals and understanding the requirements for Round 1. These resources provide detailed information about the Open Call, submission guidelines, and the evaluation process.

CyberSecDome Round 1 Submission Form Template: [Download Here]

A template to help applicants structure their proposal according to the required sections and formatting guidelines.

CyberSecDome Open Call General Guide: [Download Here]

A comprehensive document outlining the rules, eligibility criteria, and requirements for participating in the CyberSecDome Open Call.

To get an overview of the CyberSecDome Architecture and Tools, you can check this webpage on the CyberSecDome website: https://cybersecdome.eu/concept/

Learn more about GDPR Compliance and Guidelines applicable to CyberSecDome Open Call processes by visiting the official EU website here: https://commission.europa.eu/law/law-topic/data-protection_en.

FAQs Document: [Download Here]

A detailed list of frequently asked questions regarding the CyberSecDome Open Call, including eligibility, submission, and evaluation.

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.