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

An innovative Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security, privacy and accountability of complex and heterogeneous digital systems and infrastructures.

CyberSecDome Open Call

FAQs

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.

1 Submission Process FAQs

Q. How do I submit my proposal for Round 1?
A. All proposals must be submitted through the CyberSecDome Digital Submission System set on the F6S platform. Proposals submitted via email or other channels will not be considered. The submission platform will open on **December 10, 2024**, and the final deadline for submission **is February 10, 2025 (17:00 CET)**.

Q. Can I edit my proposal after submission?
A. Yes, you can edit your proposal any time before the submission deadline. Once the deadline has passed, no further changes will be allowed.

Q. What file format should I use for my proposal submission?
A. Proposals must be submitted in **PDF format only**. Ensure all required sections are included and the document complies with the formatting guidelines which are outlined in the Proposal Submission Template.

Q. What happens if I encounter technical issues with the submission system?
A. If you experience technical issues while submitting your proposal, you should immediately contact the F6S support and CyberSecDome Help Desk (opencall@cybersecdome.eu)to report any issues before the submission deadline to avoid complications.

Q. Can I submit multiple proposals?
A. Applicants can submit more than one proposal for Round 1 only if they do not want to address Topic 1.

2 Eligibility FAQs

Q. Who is eligible to apply for Round 1 of the CyberSecDome Open Call?
A. 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 apply but are not eligible for funding due to Horizon Europe regulations.

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

A. 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.

Q. Are consortia allowed to apply?
A. Yes, consortia of a maximum of three participating entities are allowed to apply. The consortium should include at least one SME as a partner.

Q. What are the funding limits for Round 1?
A. 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 consortium size.

Q. What percentage of costs will be funded?
A. SMEs can receive up to 100% of eligible costs, while larger industries and organisations will be funded at 50% of their eligible costs. No single proposal will receive more than €120,000.

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

3 Technical FAQs

Q. What type of cybersecurity solutions are expected in Round 1?
A. Round 1 focuses on early-stage validation of AI-enhanced and VR-based cybersecurity solutions. Applicants should propose use cases that align with the topics outlined, including threat detection, incident response, and situational awareness.

Q. How will integration with the CyberSecDome architecture be managed?
A. Applicants are expected to integrate their use cases with the CyberSecDome architecture. Technical documentation and support will be provided.

Q. What kind of infrastructure is required to test the use cases?
A. Applicants should ensure access to infrastructure such as cloud environments, on-premises servers, or virtualised environments. Specific requirements should be outlined in the proposal.

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

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

A. Yes, data sharing may be required for testing and validation, but all data sharing must comply with GDPR regulations, and sensitive data must be anonymised.

Q. What type of support will I receive during the project?
A. Applicants will have access to technical support from the CyberSecDome Open Call Implementation Team, including guidance on tool integration and system testing.

Financial FAQs

Q. How will the funding be disbursed?
A. Funding will be disbursed in stages: 30% upon signing the Sub-Grant Agreement, up to 30% upon interim assessment, and the remaining amount after project completion.

Q. Are there restrictions on how the funds can be used?
A. Yes, funds must be used for eligible costs such as personnel, equipment, travel, and subcontracting. All expenses must be justified in financial reports.

Q. Can I include subcontracting in my budget?
A. Yes, subcontracting is allowed but must be justified as necessary for project tasks. Subcontractors must comply with the same eligibility and reporting requirements as the primary beneficiary.

Q. What happens if my project is delayed?
A. Notify the CyberSecDome Open Call Management Team as soon as possible. Extensions may be granted in exceptional cases, but failure to meet key milestones may lead to funding reductions or project termination.