CyberSecDome
Open Call Info Day II

Spiros Fotis Jr
AEGIS
Spyros.fotis@aegisresearch.eu

CyberSecDome 2nd INFO DAY

Athens, Greece

December 4th 2024 @14:00 CET

Welcome to the CyberSecDome Open Call!

CyberSecDome

❑ Funded by the Horizon Europe Framework Programme (2021-2027).
❑ Aims to enhance cybersecurity through the integration of AI and VR technologies

The CyberSecDome Open Call is targeted toward those who can help innovate and improve cybersecurity within the digital ecosystem.

❑ SMEs focusing on cybersecurity solutions.
❑ Industry professionals looking to contribute to cybersecurity innovations
❑ Researchers in cybersecurity and related fields
❑ Academic institutions interested in collaborative projects that align with cybersecurity advancements

CyberSecDome: A Holistic Cybersecurity Solution

CyberSecDome

❑ Enhances cybersecurity with advanced AI and VR technologies for digital infrastructure protection.

| **Obj 1** | Improve the resilience and preparedness capabilities of digital infrastructure by at least **25%** |

| **Obj 2** | Improve the efficiency and agility of digital infrastructure to react to security threats by at least **25%** |

| **Obj 3** | Enhance coordinated cyber-incident response among different digital infrastructures and systems at national and European levels |

| **Obj 4** | Provide high levels of cybersecurity via a set of policies and AI-based methods for the proactive real-time management of security issues |

| **Obj 5** | Provide better interfaces between humans and cybersecurity algorithms |

| **Obj 6** | Develop solutions to automate penetration testing for proactive security using data-driven AI |

Two-Round Open Call: From Prototype Validation to Real-World Deployment

CyberSecDome

Round 1: Prototype Testing

- ❑ Validate and test CyberSecDome's prototype
- ❑ Participants integrate solutions, conduct tests, and provide feedback
- ❑ Total budget: **€480,000**
- ❑ Up to **€120,000** per project

Round 2: Real-World Deployment

- ❑ Builds on Round 1 outcomes
- ❑ Deployment of CyberSecDome in real-world settings
- ❑ Total budget: **€720,000**
- ❑ Eligible proposals from Round 1 can resubmit

Round 1 Open Call Topics: Addressing Key Cybersecurity Challenges

CyberSecDome

Topic 1 Evaluation & Testing of Integrated CyberSecDome Prototype

- **Funding: Up to €120,000** per project.

Topic 2: Advanced Risk Assessment Using the Dynamic Risk Analysis (DRA) functionality

- **Funding: Up to €35,000 per project.**

Topic 3: Comprehensive Incident Investigation and Response

- **Funding: Up to €55,000 per project.**

Topic 4: AI-Driven Automated Penetration Testing

- **Funding: Up to €20,000 per project.**

Topic 5: Generation of Security-Related Datasets for AI-Enhanced Tools Training

- **Funding: Up to €10,000 per project.**

Topics for Round 2 TBA soon

Round 1 Open Call Topics: Addressing Key Cybersecurity Challenges

CyberSecDome

Topic 1 Evaluation & Testing of Integrated CyberSecDome Prototype

- Evaluation & Testing of Integrated CyberSecDome Prototype
- Assess system usability, scalability, and effectiveness in real-world cybersecurity scenarios.
- Provide insights into system limitations and improvement opportunities.
- Cover diverse threat landscapes and operational settings.
- **Funding: Up to €120,000** per project.

Round 1 Open Call Topics: Addressing Key Cybersecurity Challenges

CyberSecDome

2 Topic 2: Advanced Risk Assessment Using the Dynamic Risk Analysis (DRA) functionality

- Perform comprehensive risk assessments using the DRA tool.
- Evaluate asset interdependencies and quantify potential threat impacts.
- Identify system vulnerabilities and propose actionable mitigation strategies.
- Include detailed asset testing plans and dynamic analysis methodologies.
- **Funding: Up to €35,000 per project.**

3 Topic 3: Comprehensive Incident Investigation and Response

- Address the end-to-end process of incident investigation and response.
- Integrate functionalities like SIEM, Prophecy, FVT, and adaptive response mechanisms.
- Include log capture, intrusion detection, and automated incident analysis.
- Provide feedback mechanisms for continuous system improvement.
- **Funding: Up to €55,000 per project.**

4 Topic 4: AI-Driven Automated Penetration Testing

- Test CyberSecDome's AI-driven penetration testing functionalities.
- Validate attack modeling and simulation tools for identifying vulnerabilities.
- Propose testing plans and operate within CyberSecDome's controlled environment.
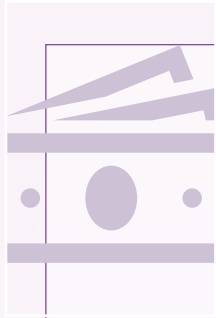- **Funding: Up to €20,000 per project.**

5 Topic 5: Generation of Security-Related Datasets for AI-Enhanced Tools Training

- Simulate cyber-attack scenarios to generate high-quality datasets.
- Cover a broad spectrum of threats and vulnerabilities.
- Ensure datasets are anonymized, comprehensive, and legally compliant.
- Contribute to training and validation of CyberSecDome's AI models.
- **Funding: Up to €10,000 per project.**

⏰ **Topics for Round 2 TBA soon**

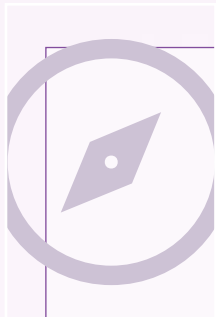# Why Participate in the CyberSecDome Open Call?

CyberSecDome

Financial Support

- Receive up to **€120,000 per project**.
- Funding tailored to support innovative cybersecurity solutions.

Access to Cutting-Edge Technology

- Collaborate on advanced AI and VR tools for cybersecurity.
- Use CyberSecDome's testing environment to refine solutions.

Expert Guidance and Mentorship

- Work with the CyberSecDome consortium, including top European experts.
- Benefit from technical and operational support throughout the project lifecycle
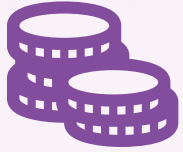
Networking and Visibility

- Build relationships with industry leaders, researchers, and innovators.
- Gain recognition within the cybersecurity community.

Real-World Impact

- Contribute to the advancement of cybersecurity across Europe.
- Shape the future of secure digital infrastructures.

Funding Details: Supporting Your Innovation
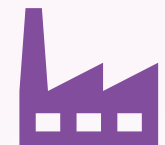
CyberSecDome

Total Budget: €1.2 million

Max Funding Per Project: €120,000

Round 1 Budget: €480,000

SMEs Eligible for up to 100% of eligible costs

Other Organisations Co-funding of up to 50% of eligible costs.

Eligible Costs

- Personnel costs
- equipment
- travel
- subcontracting
- other direct costs, and
- indirect costs (25% flat rate).

Who Can Apply? Eligibility Criteria

CyberSecDome

Legally Established Entities

- Applicants must be legally established in the **EU Member States** or **Horizon Europe Associated Countries**.

SME Inclusion

- Proposals must include **at least one SME** in cases of consortia.

Alignment with CyberSecDome Goals

- Projects must align with the **CyberSecDome Open Call objectives**, addressing critical cybersecurity challenges.

Unique Proposals Only

- Proposals cannot receive **double funding** for the same activities from other EU sources.
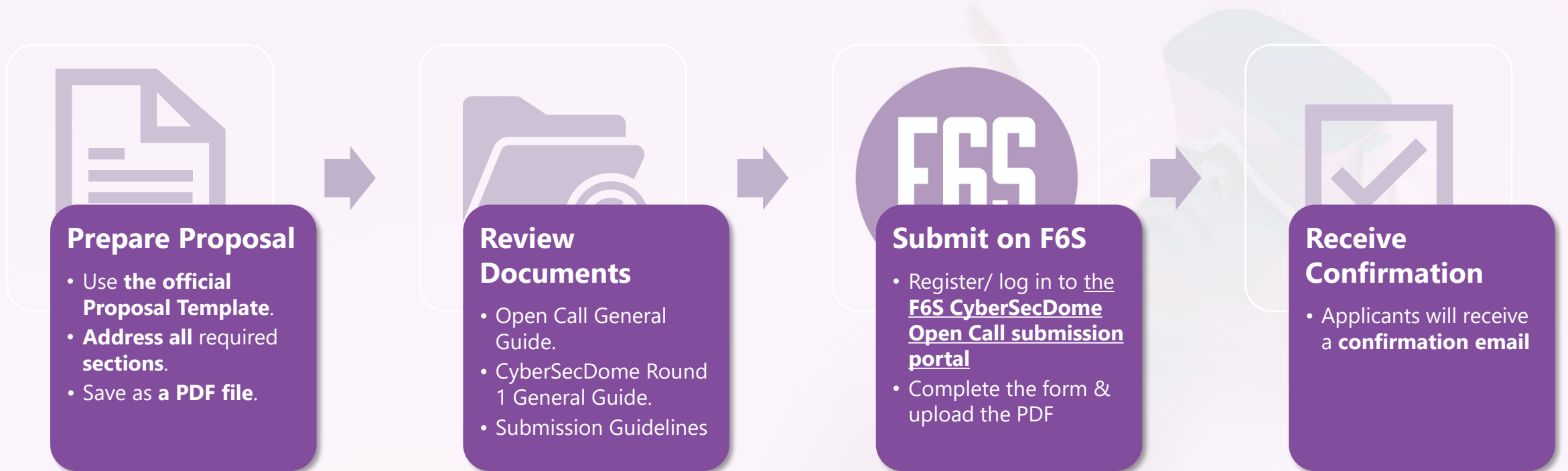
Compliance with Ethical and Legal Standards

- All participants must adhere to **ethical guidelines** and demonstrate compliance with relevant **legal frameworks**.

Financial Capability

- Applicants must demonstrate the financial capacity to support project implementation and cover any costs not funded by the Open Call.

How to Apply: A Step-by-Step Guide

Prepare Proposal
- Use **the official Proposal Template**.
- **Address all** required **sections**.
- Save as **a PDF file**.

Review Documents
- Open Call General Guide.
- CyberSecDome Round 1 General Guide.
- Submission Guidelines

Submit on F6S
- Register/ log in to <u>the **F6S CyberSecDome Open Call submission portal**</u>
- Complete the form & upload the PDF

Receive Confirmation
- Applicants will receive a **confirmation email**

Evaluation Criteria: Ensuring Excellence

CyberSecDome

Criterion		Score Range	Threshold
Alignment	Relevance to CyberSecDome objectives and focus areas.	0-5	3
Excellence	Innovation, methodology, and scientific/technical quality	0-5	3
Impact	Potential benefits for the cybersecurity ecosystem, including societal, business, and technical impacts.	0-5	3
Implementation	Feasibility of the work plan, resource allocation, and risk management.	0-5	3
Value for Money	Cost-effectiveness and efficient use of resources.	0-5	3

Eligibility Check   **Expert Review**   **Consensus Meeting**   **Ranking**
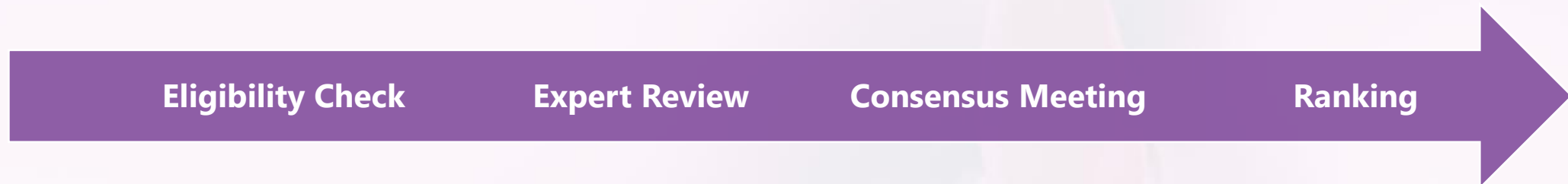
Mark Your Calendars!

Stage	Date
Open Call Announcement	December 4, 2024
Submission System Opens	December 10, 2024
Proposal Submission Deadline	February 10, 2025 (17:00 CET)
Eligibility Check and Initial Review	February 12-13, 2025
Evaluation by Expert Panel	February 17-27, 2025
Consensus Meeting and Ranking	March 1-7, 2025
Notification of Results	March 14, 2025
Grant Agreement Signing	March 24-28, 2025
Project Start	April 1, 2025

FAQs (I)

CyberSecDome

Q1. How can I apply for the CyberSecDome Open Call?

- You can apply through the CyberSecDome Digital Submission System on the F6S platform. The link will be shared on the CyberSecDome website.

Q2. What are the funding limits for projects?

- The funding limit for Round 1 is up to €120,000 per project, depending on the topic addressed and the project scope.

Q3. Can I participate as part of a consortium?

- Yes, consortia of up to three entities are allowed. At least one partner must be an SME, and all partners must meet the eligibility criteria.

Q4. What types of projects are eligible?

- Projects should focus on early-stage validation of AI-enhanced and VR-based cybersecurity solutions of CyberSecDome, aligning with the topics outlined in the Open Call.

Q5. Will I receive technical support during the project?

- Yes, successful applicants will receive technical guidance from the CyberSecDome Open Call Implementation Team (OCIT), including help with integration and testing.

FAQs (II)

CyberSecDome

Q6. Can entities from outside the EU apply?

- Entities from associated countries (e.g., the UK and Switzerland) can apply but are not eligible for funding due to Horizon Europe regulations.

Q7. What is the deadline for proposal submission?

- The submission deadline for Round 1 is February 10, 2025, at 17:00 CET.

Q8. Can I resubmit a revised proposal if I am not selected in Round 1?

- Yes, applicants who were not selected in Round 1 can resubmit for Round 2, provided they meet the eligibility criteria.

Q9. What should I do if I encounter technical issues with the submission platform?

- Contact the F6S support to resolve technical issues and the CyberSecDome Help Desk to report problems well before the deadline.

Q10. Are there restrictions on how the funding can be used?

- Yes, funding can only be used for eligible project costs, such as personnel, equipment, travel, and subcontracting. All expenses must be justified in financial reports and comply with Horizon Europe rules.

Next Steps: Get Started with the CyberSecDome Open Call

CyberSecDome

1. Read the Open Call Documentation
- Download the Open Call Guide, Proposal Template, and FAQs from the CyberSecDome website.
- Familiarize yourself with the eligibility criteria, funding details, and evaluation process.

2. Prepare Your Proposal
- Identify which Round 1 topic aligns with your expertise and innovation.
- Develop a clear and concise proposal using the provided template.

3. Register on the Submission Platform
- Create an account or log in to F6S CyberSecDome Open Call.
- Upload your proposal and supporting documents.

4. Stay Connected
- Follow CyberSecDome on social media for updates and announcements.
- Reach out to the Open Call Management Team for assistance.

16-Dec-24

Contact & Communication

For General Inquiries
📧 Email: info@cybersecdome.eu

For Open Call Support

📧 Email: opencall@cybersecdome.eu

🌐 Submission Platform: F6S CyberSecDome Open Call

Stay Updated

- LinkedIn: CyberSecDome LinkedIn Page

- X (Twitter): @CyberSecDome_EU

- YouTube: CyberSecDome Channel

Need Technical Assistance?
📞 F6S Support Team: Available through the F6S platform.

Contact

Spiros Fotis Jr
25 Humboldt Str.
Braunschweig, GERMANY
Tel. +30 6936186603
Email: spyros.fotis@aegisresearch.eu

Sicherheit durch Technologie

Follow

CyberSecDome Online Kickoff Meeting