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 Round 2

Full testing & validation of the final integrated CyberSecDome prototype

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 Topic Description

This call invites proposals for the testing, and validation of the final integrated CyberSecDome platform in real-world operational environments. Selected projects will support the project's final validation and deployment phase, contributing to the assessment of its scalability, usability, interoperability, and cross-sector relevance.

2 Domains of Interest

To ensure wide applicability and replication potential, proposals from the following underrepresented sectors are particularly encouraged:

- Healthcare
- Energy & Utilities
- Finance & Banking
- Manufacturing & Industrial IoT
- Public Services
- Smart Cities

3 Scope & Minimum Requirements

Each proposal must demonstrate its ability to:

- **Test and validate the integrated CyberSecDome prototype** in an operational environment, using all key functionalities:
  - AI-enhanced threat detection
  - VR-based situational awareness
  - Dynamic risk assessment
  - Collaborative threat intelligence modules
- **Define and implement a concrete, domain-specific use case** that aligns with the platform's goals and complements the project's existing pilots in aviation and telecommunications.

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

- **Deliver structured technical and operational feedback** against CyberSecDome's KPIs and contribute to platform improvement through documented insights (e.g. usability, integration challenges, interoperability).
- **Collaborate with the CyberSecDome Open Call Implementation Team (OCIT)** and relevant technical partners for onboarding, technical integration, and validation support.
- **Offer access to a representative operational environment** (e.g. infrastructure, data, stakeholders) for realistic testing and demonstration of platform capabilities.

4 Funding

- Budget for Round 2: **€780,000**
- Maximum funding available per project: **up to €120,000**
- Priority will be given to SMEs, research organisations, and technology adopters with active involvement in their domain.

5 Expected Impact:

- Demonstration of platform scalability and cross-domain applicability
- Operational validation of CyberSecDome's tools in real-world use cases
- Actionable feedback to support final technical refinements
- Strengthened innovation uptake and commercial exploitation paths

All proposals must adhere to the submission guidelines and proposal structure outlined in the official Round 2 documentation (General Guide, Proposal Template, and Submission Guidelines.

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

6 Requirements and Specifications

Module	Tool(s)	Partner(s)	Requirements
Threat Detection	Intrusion Detection System (IDS-FPGA)	TUC	Participants are asked to provide: • **PCAP files** capturing relevant network traffic. • **Metadata details**, including source and destination IP addresses and port numbers. • **Intrusion detection annotations** to highlight any identified threats-attacks. • **Timestamped PCAP files with attack traffic**, to support analysis and validation. • **Coverage of both TCP and UDP traffic layers**, including both benign and malicious flows.
	Intrusion Prediction System (IPS)	STS	Participants are asked to provide: • **PCAP files** capturing network traffic. • **Metadata details**, including source and destination IP addresses and port numbers. • **Intrusion prediction annotations** to indicate potential threats or suspicious activity. • **Timestamped PCAP files with attack traffic for system training**. • **Timestamped PCAP files with normal and attack traffic**, for baseline comparison and system validation. • A **primary focus is on TCP traffic**, while also including coverage of the **Network and Transport layers**.
Incident Management	SIEM (Graylog)	ACS	• -> input: Log/alert Syslog format (JSON)
	SOAR (Prophecy)	ACS	• -> input: alert Syslog format (JSON)

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

(Incident Investigation)	Forensic Visualisation Toolkit (FVT)	AEGIS	• GUI access over the web interface. • Connectivity with the rest of the II tools required (Graylog, Prophecy), preferably in the same network. • A Linux VM with substantial storage (disk size >50GB) and RAM is required.
Dynamic Risk Assessment	Dynamic Risk Assessment Tool (DRA)	MAG	• GUI access over the web interface
Collaborative Intelligence	Threat Information Sharing (TIS)	CBRL	• A Linux environment with the ability to run Docker Compose. ≥10GB of available storage; ≥2GB of RAM is required. • TIS needs interconnection with other TIS modules to work properly; • For inter-server connectivity, the environment must support either port forwarding with a static IP or DDNS secured by a firewall and TLS, or a VPN configuration with OpenVPN.
AI-Knowledge Sharing (AIKS)	Federated Learning	ITML	→ Linux host (bare-metal, VM or cloud) able to run **Docker & Docker-Compose**.→ **Server node**: 8 vCPU, 32 GB RAM, 50 GB SSD; optional single GPU (≥ 4 GB VRAM) for faster training/aggregation.→ **Clients** (can be lightweight VMs or containers): 4 vCPU, 8GB RAM, 20 GB disk each; spin up as many as you like on the same or separate machines. Python 3.9 +, Tensorflow, Flower, gRPC;. Supporting learning strategies: FedXgbBagging
AI-Knowledge Sharing (AIKS)	Swarm Learning	ITML	→ Minimum **three** Linux nodes/VMs (to observe leader election) – each 4 vCPU, 16 GB RAM, 20 GB SSD.→ Promote any node to "leader" by giving it 4vCPU / 8GB RAM;→ Docker-Compose bundle providing *initiator*, *leader* and *follower* micro-services.→ Python 3.9 +,nodes must reach each other directly or via VPN; supply TLS certificates for secure model traffic; allow ~20 GB per node for model/version storage and metrics. Supporting learning strategies: FedXgbBagging
Immersive Interface	VR-Enhanced Situational Awareness (VR-Interface)	IMT	• The users need a computer running on Windows. • For the XR device, they need a Meta Quest 3. • They also need a stable connection.

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

			• We also need the asset list, asset dependencies and asset locations for suitable visualisations
Automated Security Testing	Automated Pen-Testing Tool (APT)	LiU	**For integration:** Debian-based Linux environment with the tools.To be used by the pen-testing engine. Kali Linux comes with all tools pre-baked so that is the easiest integration. Exact specs depend on the tools to be used by the pen-testing engine. **For remote testing:** • The pentesting engine requires access to the environment to be tested. • If the environment lives in CyberSecDome then we need a Gate to it or to share a workspace. • If the environment is in the Pilot's premises, then a suitable connection is required. We have tested • VPN access before, tunnelling over SSH should also work if that is preferable.

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

7 Proposal Format

Proposals must be uploaded in PDF format using the official Round 2 Proposal Template available on the **CyberSecDome website**.

The proposal must:

- Be written in English.
- Not exceed 30 pages (excluding annexes).
- Include all sections indicated in the template.
- Use font size 11 (Calibri or Arial recommended).

8 Submission Rules

- Proposals must be submitted via the submission form on the F6S platform, following the submission guidelines.
- Only one proposal is allowed per applicant or consortium.
- No extensions to the deadline will be granted.
- Technical issues must be reported to the Helpdesk at least 2 hours prior to the deadline.
- It is highly recommended to submit proposals well in advance of the deadline to prevent last-minute issues.

9 Mandatory Proposal Content

Applicants must complete all parts of the Proposal Template:

- General Information
- Proposal Summary
- Applicant(s) Details
- Relevance & Alignment
- Excellence
- Impact

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

- Implementation
- Cost Effectiveness
- Budget Overview
- Ethical and Legal Considerations

10 Notifications and Results

Applicants will be informed of the evaluation outcome through the F6S platform and email. Results will include feedback from reviewers and show whether the proposal was chosen for funding.

11 Applicant Responsibilities

- Monitor the F6S platform regularly for communications and updates.
- Respond promptly to requests for clarification or additional information.
- Ensure compliance with Horizon Europe rules and CyberSecDome eligibility conditions

12 Support and Assistance

- For queries or assistance during the application process:
    - Email: Reach out to opencall@cybersecdome.eu or info@cybersecdome.eu
    - Social Media: Updates and announcements are shared on:
    - LinkedIn: CyberSecDome LinkedIn
    - X (Twitter): @CyberSecDome_EU
    - YouTube: CyberSecDome Channel
- Submission Platform: For technical issues and/or questions, please contact F6S support at support@f6s.io or opencall@cybersecdome.eu regarding any difficulties you may encounter on the submission platform.

13 Steps for Proposal Submission

1. Registration on F6S Platform:

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

- Access the CyberSecDome Open Call Round 2 submission page at https://www.f6s.com/cybersecdome-open-call-round-2.
- Applicants with existing F6S accounts can log in directly, simplifying the process. Registration on F6S is not mandatory but is recommended for updates on the proposal status.

2. Proposal Preparation:
   - Use the Proposal Template provided. Ensure all sections are completed, and supporting documentation (e.g., budget breakdowns, CVs, and letters of commitment) is included.
   - Adhere to the formatting and length requirements outlined in the Proposal Template.
3. Proposal Submission:
   - Upload the completed proposal and additional documents (if required) on the F6S platform.
   - Select the relevant topic(s) addressed by your proposal.
   - Double-check that all mandatory fields and documents are completed.
4. Submission Confirmation:
   - Once submitted, applicants will receive an email confirmation with a unique reference number.
   - Use this reference number for any correspondence regarding your application.

14 Key Tips for Successful Submission

- **Start Early**: Begin preparing your proposal well before the submission deadline to allow time for clarifications or adjustments.
- **Read All Materials**: Ensure you understand the scope, objectives, and evaluation criteria of the Open Call.
- **Ask for Help**: Contact the CyberSecDome team for assistance with unclear sections or technical difficulties.
- **Review Thoroughly**: Ensure compliance with all submission requirements and verify that documents are free of errors.