CYSSDE — CYSSDE OC3 Application form

Type:
Owner:
Application Id:
Created at: :
Last edited:
Submitted at: —

BASIC INFO

Organisation Details

We are looking for applications from **individual entities or consortia** (up to two entities) specialising in cybersecurity. Eligible applicants include SMEs (including micro-enterprises and start-ups), mid-caps, large companies, research centres (including universities), and public bodies. Applications have to be submitted by Penetration Testing and Vulnerability Assessment expert organisations. All entities must be registered in, and controlled by entity or person established in a Member State of the European Union or an EEA country.

Organization Name *
—

Primary contact person

Name and Surname *
—

Position: *
—

Email: *
—

Phone Number: *
—

Location of the applicant

Address *

—

Country of registration *

—

European headquarters based in a Member State? *

—

Website *

—

Does your entity have experience in Cybersecurity? *

—

Are you applying individually or in a consortium *

—

Project Summary

Provide a brief summary of your project, focusing on how it aligns with the objectives of the CYSSDE Open Call. Include the main goal and intended outcomes of the Penetration Testing and/or Vulnerability Assessment activities.

Project Summary - outline in a few lines why you think you need to be considered for this funding. *

Provide essential information such as experience, size, references, domain expertise, identified needs, access to infrastructure, relation to critical, essential or important domain, speed to execute, and other relevant information. (max 1000 chars)

—

How many penetration tests do you plan to perform over the next 18 months? Please note that the minimum required number is 10 penetration tests, and this number cannot be lower if your proposal is selected. The proposed number of tests will be assessed and scored by the expert evaluators as part of the evaluation process. *

—

Type of Entities Covered *

Who are the key end users or entities your project will serve (e.g., Essential Service Operators, SMEs, Critical Infrastructure, etc.)?

—

Type of Entities Covered *

Who are the key end users or entities your project will serve (e.g., Essential Service Operators, SMEs, Critical Infrastructure, etc.)?

—

Type of Entities Covered *

Who are the key end users or entities your project will serve (e.g., Essential Service Operators, SMEs, Critical Infrastructure, etc.)?

—

Type of Entities Covered *

Who are the key end users or entities your project will serve (e.g., Essential Service Operators, SMEs, Critical Infrastructure, etc.)?

—

Penetration Test Details and Focus Areas. *

Please provide a short description of the type of penetration tests you intend to perform, including their priorities and focus areas. Include information such as: Type of systems or assets tested (web, cloud, OT/ICS, mobile, IoT, etc.), Security focus (e.g., vulnerability assessment, network security, application security, compliance testing) and Key priorities or critical areas to address. (max 1000 chars)

—

Number of Penetration tests by type and property *

—

Focus area - Infrastructure Landscape (more than 1 option possible) *

—

Excellence

Describe technical quality, relevance, and innovation of the proposed; try to be concise, but clear and detailed in your answer. Address the following topics:

Objectives: What specific goals does your project aim to achieve in the context of Penetration Testing or Vulnerability Assessments? *

Describe the overall Project Plan and Argumentation - providing evidence of project objectives in view of overall activities (1000 chars)

—

Ambition and Innovation *

Describe how your proposal aligns with the objectives of the Open Call, focusing on the identification of vulnerabilities and cybersecurity resilience of the end-users, particularly in relation to Penetration Testing and Vulnerability Assessments for Critical Infrastructure, Essential and Important Services, or SMEs (including sectors like high-tech appliances, AI, fintech, medtech, etc.). What innovative approaches or methodologies will you use in your assessment activities? (3000 chars)

—

Technical Competence. *

Provide evidence of your company and team's technical expertise and previous experience in conducting Penetration Testing and Vulnerability Assessments. Highlight any relevant publications, research, or responsible disclosures made in the field. Indicating previous experiences with similar projects or in this domain. (1500 chars)

—

Technical Competence - Level of Expertise *

Indicate Level of Experience between 1 and 5, where 1 is not so experienced and 5 is highly experienced (for each competence)

—

Research done and Technical achievements *

Please detail your contribution in the following Areas: Research work you have conducted, particularly in areas like CVE identification, cybersecurity, or related fields (mention if published). Research publications (please include links or attach non-confidential documents). Tools, methods, or applications you have developed. Capture The Flag (CTF) challenges you have completed, including notable achievements. Blog posts, articles, or other written contributions (include links if available). Any other relevant contributions (e.g., open-source projects, community work) , you can include links and reference to work done. (1500 chars)

—

Methodologies and Scenarios. *

Describe the methodologies, tools, and approaches you will use for the penetration tests, including specific use cases and testing scenarios. Explain how your approach addresses vulnerabilities in supply chains, IoT, cloud, applications, systems, appliances, and OT devices (if applicable). List established frameworks or tools (e.g., OWASP, NIST, PTES) and/or innovative approaches. Include example scenarios for the types of systems or assets you will test. Highlight strategies to tackle high-risk areas and challenges (supply chain, OT, IoT, cloud, apps). Explain why your approach is credible and suitable for the systems under test. (2000 chars)

—

Impact

Describe the contribution and expected benefits of the project in approximately 3000 characters. **Try to be concise, but clear and detailed in your answer.**

Contribution to Capabilities and Capacities *

How will the project contribute to the improvement of NIS2 Compliance and resilience? Will the vulnerabilities found impact Essential Service Operators or SMEs significantly? Provide examples of how these assessments will enhance cybersecurity practices. (2000 chars)

—

Exploitation plans, Long-Term Impact *

Describe how your activities will contribute to sustained cybersecurity improvements beyond the project's duration. For example, will the project develop tools that can scale over time to enhance the detection of vulnerabilities? Describe how you plan to utilize the results, and exploit them, both commercially or in other ways. (1000 chars)

—

Market and Social Impact *

How will your project contribute to the overall European Cybersecurity industry? Describe the societal benefits and the broader market impacts of your activities, such as the effects on Critical Infrastructure security or large volumes of end-users. (1000 chars)

—

Implementation

Describe the Feasibility and practicality of the project

Resources and Capabilities *

Describe the resources and capabilities available to carry out the proposed activities (personnel, tools, expertise). If additional resources or specialized equipment are required, outline your plans for acquiring them. Describe dependencies and potential risks and how you will mitigate them. (1500 chars)

—

Scope of Planned Actions *

Provide a plan detailing at least 10 Penetration Testing and/or Vulnerability Assessment activities, including the target appliances, applications, end-users, and the anticipated value they will bring. Include any expected outcomes, such as the publication of CVEs. Summarise the planned activities for delivering the proposed penetration testing and vulnerability assessments over the 18-month support period. Responses must be consistent with Section 1.2 of the Terms and Conditions. (2000 chars)

—

GANTT Chart *

Based on the section above and the timeline defined in the Open Call Terms and Conditions (sections 1.2 and 4), please prepare and upload a Gantt chart showing all key activities and milestones

—

Describe your prior experiences *

Please describe the methodologies, tools, and approaches you will use for the penetration tests. Include the types of systems or assets you will test, specific scenarios or use cases, and how your approach will address vulnerabilities in supply chains, IoT, cloud, applications, systems, appliances, or OT devices (if applicable). Mention established frameworks or tools (e.g., OWASP, NIST, PTES) or credible innovative approaches Provide examples of testing scenarios relevant to your end-users' systems. Explain how your approach addresses high-risk areas or challenges. Highlight why your methodology is credible, suitable, and well-documented. (1500 chars)

—

Prior experiences - Quantitative *

—

Personnel *

Please describe the number of employees and freelancers (please specify) involved in penetration testing. We would also like to evaluate the expertise of these employees. Types of relevant certifications (e.g., OSCP, CEH, CISSP, CREST, etc.). Briefly highlight relevant experience or areas of specialization. Gender distribution (e.g., number of male, female, non-binary team members)(1500 chars)

—

Quantitative Personnel details *

—

End-User Engagement Approach *

Describe how you plan to identify, reach, and engage relevant end-users during the project. Explain how you will maintain communication and ensure active participation throughout the project. Include any existing commitments or partnerships with NIS2 entities, Essential Service Operators, or SMEs that will support engagement. (1500 chars)

—

Please upload here any evidence that supports the End-User Engagement Approach

—

Project Budget

Provide a breakdown of costs. Overheads and Totals are calculated automatically. *

—

Totals

5. Overheads (7% of 1+2+3)

€0.00

5. Requested Overheads (7% of 1+2+3)

€0.00

GRAND TOTAL Project Cost

€0.00

GRAND TOTAL Amount Requested

€0.00

Final Grant Share (%)

0%

Declaration of Honour

Please read carefully the statements below. You will not be able to change the statements after the deadline. By ticking the boxes below, I confirm that

I have read and understood the information about the project, as provided in the Open Call Terms and Conditions *

—

I acknowledge that the evaluators and the European Commission and its bodies and agencies may have access to the data collected under the open call *

—

The data provided in the application form are true and up-to-date *

—

The entity I represent meets the eligibility conditions described in the GfA. *

—

There is no conflict of interest between the company I represent and any of the consortium partners *

—

I did not make false declarations in supplying the information required, as a condition of participation in the Open Call or do not fail to supply this information *

—

I voluntarily agree to be registered at CYSSDE Community at DISCORD and I understand that I can delete my profile from the above-mentioned Community by informing the CYSSDE Team via helpdesk mail *

—

Do you have a 'Gender Equality Plan'? (Public bodies, higher education institutions, and research organisations from EU countries and associated countries are obliged to have it.) *

—

The entity I represent is not directly or indirectly controlled by a country that is not an eligible country (i.e. any country outside of EU member states) or an ineligible country entity. *

—

Processing Personal Data

Please read the privacy notice available at https://fundingbox.com/privacy-notices/open-call/.

I confirm that I read and understood the information clause concerning processing of the personal data provided above. *

—

I confirm that I have legal basis for processing personal data of the team members listed in the application form. *

—

I will pass the information clause provided above to all team members mentioned in the application form. *

—