CALL FOR PROPOSAL

OPEN CALL FOR INDEPENDENT CYBER RANGES

This activity is organized under the project CYRESRANGE - No. 101128088, funded by Digital Programme, under the call DIGITAL-ECCC-2022-CYBER-03

Contents

This activity is organized under the project CYRESRANGE - No. 101128088, funded by Digital Programme, under the call DIGITAL-ECCC-2022-CYBER-03

I. Background

The Call for Onboarding Independent Cyber Ranges is an activity conducted under CYRESRANGE project, a pioneering initiative designed to foster a collaborative ecosystem of advanced cyber ranges and facilitate the use of a cyber range capability

The primary objective of CYRESRANGE is to foster capabilities of existing cyber ranges in order to create a network based on interconnected cyber ranges, with a focus on improving experience for scenario developers and introducing a comprehensive gamified experience for students, at the national and regional level. Our ambition is to create the premises of building a community of content creators that will create the premises of a new job in cyber security and professionals that will develop their cybersecurity skills and expertise in key technologies and introducing cost-effective technology to onboard new cyber ranges. In addition, the CYRESRANGE network includes resources focused on advancing cybersecurity training, accelerating research in cyber defense, enabling large-scale cyber exercises, and providing shared resources for cyber education.

In an increasingly complex and rapidly evolving cybersecurity landscape, isolated cyber range environments are no longer sufficient to address sophisticated cyber threats or to provide learners with realistic, real-world experience. CYRESRANGE addresses this challenge by fostering a collaborative and interoperable ecosystem that enables enhanced cooperation, resource sharing, and capability development among participating cyber ranges.

II. Scope

This call for Onboarding Independent Cyber Ranges is open both to operators of existing, operational cyber ranges seeking to integrate their infrastructures into the CYRESRANGE platform, and to users interested in leveraging the capabilities of the CYRESRANGE network for training, research, education, and large-scale cyber exercises.

By onboarding the CYRESRANGE platform, cyber range operators become part of a collaborative and interoperable ecosystem, benefiting from increased visibility, shared resources, and new opportunities for cooperation and innovation. At the same time, users of the platform gain access to a diverse portfolio of interconnected cyber ranges, advanced training scenarios, and a rich, community-driven environment designed to enhance practical cybersecurity skills and real-world experience.

The scope of this grant is to support Independent Cyber Ranges through **Financial Support to Third Parties (FSTP)**, enabling their technical onboarding, integration, validation, and active participation in **cross-range, large-scale cybersecurity exercises** within the CYRESRANGE project activities.

The grant supports activities that contribute to the interoperability, scalability, and operational validation of cyber ranges by integrating external infrastructures and capabilities into the CYRESRANGE ecosystem.

In particular, the scope covers:

- The **onboarding of independent cyber range infrastructures** or hardware/software environments capable of supporting cross-range exercises;
- The **integration of unique cyber range capabilities** that enhance the overall functionality, diversity, and realism of cross-range scenarios;
- The **technical integration via REST APIs**, including both:
    - Consumption of APIs provided by the Beneficiary for onboarding and orchestration;
    - Provision of APIs by the supported third party to enable infrastructure orchestration;
- The **use of third-party cyber range infrastructures by CYRESRANGE** for:
    - Cross-range scenario development;
    - Testing and validation activities, notably during WP4 and WP5;
- Active participation in the **validation process**, including structured technical collaboration during WP3, WP4, and WP5;
- The provision of **detailed technical and operational feedback** covering onboarding, integration, testing, and validation phases.

This Open Call is implemented as **Financial Support to Third Parties (FSTP)**, in accordance with Article 6.2.D.1 of the EU Model Grant Agreement. The CYRESRANGE consortium acts as the beneficiary responsible for publishing the call, evaluating proposals, awarding financial support, and monitoring the implementation of supported projects, in line with EU principles of transparency, equal treatment, and sound financial management. The maximum **grant amount of the call is EUR 25,000 per supported project**.

The action aims to fund a **minimum of two (2) and a maximum of three (3) projects**, selected based on a competitive evaluation process.

III. Objective

The objectives of the call for Onboarding Independent Cyber Ranges are the following:

Objective 1 – Expand the CYRESRANGE Network: onboard existing, operational cyber ranges into the CYRESRANGE platform, strengthening an interconnected network of cybersecurity infrastructures at national and regional levels.

Objective 2 – Enable access to advanced cyber range capabilities: provide users with access to shared, state-of-the-art cyber range services, tools, and scenarios that support training, education, research, and large-scale cyber exercises.

Objective 3 – Foster collaboration and resource sharing: promote cooperation among cyber range operators, educators, researchers, and industry stakeholders through shared resources, interoperable environments, and joint activities.

Objective 4 - Enhance cybersecurity skills and learning experiences: improve the quality and realism of cybersecurity training by supporting advanced scenario development, gamified learning approaches, and hands-on, real-world simulations.

Objective 5 - Build a sustainable cybersecurity community: support the development of a vibrant and sustainable ecosystem of cybersecurity professionals, content creators, and institutions, enabling innovation, knowledge exchange, and long-term capacity building.

IV. Expected outcomes

The expected outcomes of this grant are to strengthen the interoperability, operational readiness, and scalability of independent cyber ranges by integrating them into the CYRESRANGE ecosystem and validating their use in cross-range, large-scale cybersecurity exercises.

More specifically, the action is expected to deliver the following outcomes:

- **Operational integration of independent cyber ranges** into CYRESRANGE, enabling the execution of cross-range cybersecurity scenarios across heterogeneous infrastructures;
- **Improved interoperability** between cyber range platforms through standardized technical integration, notably via REST-based onboarding and orchestration interfaces;
- **Expanded availability of cyber range capabilities**, including unique or specialized functionalities contributed by third-party infrastructures;
- **Validated cross-range scenarios**, developed and tested using third-party infrastructures during WP4 and WP5, demonstrating realistic, large-scale and multi-environment cybersecurity exercises;
- **Enhanced technical maturity** of both CYRESRANGE and participating cyber ranges, resulting from hands-on validation, testing, and iteration;
- **Actionable technical and operational feedback** collected from supported third parties, contributing to the refinement of onboarding processes, orchestration mechanisms, and validation methodologies;
- **Strengthened European cyber range ecosystem**, through the engagement of EU-based independent cyber ranges and the creation of reusable integration and validation practices.

The outcomes of the action will contribute to increased **European capacity for large-scale cybersecurity training, testing, and preparedness**, while reinforcing collaboration and interoperability across independent cyber range providers.

V. Eligibility

Proposals must include **at least one** of the following activities:

a) Onboarding the applicant’s cyber range infrastructure into the CYRESRANGE platform;
or
b) Onboarding unique cyber range capabilities into the CYRESRANGE platform.

In addition, **all proposals must mandatorily include** the following activities:

c) Granting CYRESRANGE access to the infrastructure for the purposes of:
- Cross-range scenario development;
- Testing and validation activities within Work Packages WP4 and WP5.

d) Providing detailed and structured feedback covering the full onboarding, testing, and validation process.

General Eligibility Requirements

To be eligible for onboarding to CYRESRANGE, Cyber Range operators must meet the following general criteria:

- **Organization type:** Applications are welcome from a diverse range of organizations, including:
  - Academic Institutions (Universities, Colleges, Research Labs)
  - Government Agencies (Defense, Cybersecurity, Law Enforcement)
  - Commercial Cyber Range Providers
  - Non-profit Organizations focused on Cybersecurity Education and Research
  - Private organizations seeking to have their own training facilities on-premises
- **Geographic location:** Established within a European Union Member State, ensuring compliance with EU regulations including the NIS 2 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, the General Data Protection Regulation (GDPR) (EU) 2016/679, the EU Cybersecurity Strategy and Cyber Diplomacy Toolbox. This strategic alignment with European cybersecurity regulations guarantees cybersecurity resilience, mitigates risks from non-cooperative or hostile actors, and safeguards critical infrastructure against cyber threats, espionage, and foreign interference.
- **Partner's maturity level:**
  - **Infrastructure provider:** The applicant is proprietary or has access to resources (servers, datacenter, etc.) to run cyber security exercises but lacks the content, orchestration capabilities, gamification system and expertise to run this type of activities.
  - **Cyber Range provider:** The applicant must operate an existing, functional cyber range that is actively used for training, research, exercises, or other cybersecurity-related purposes. The cyber range must be demonstrable and capable of participating in integration and validation activities.

Technical Eligibility Criteria

Organizations seeking onboarding must meet the following technical criteria:

a) Infrastructure provider

Integration readiness: The infrastructure must be technically prepared for integration with CYRESRANGE. This includes:

- **Support for at least one of the preferred integration methods:** API Connection (Vsphere/Proxmox), Hybrid Connection (WireGuard/OpenVPN), API Connection (Kubernetes), Cross-Range IPSEC/VPN Tunnels or custom.

Willingness to adapt to integration requirements: Commitment to working with the CYRESRANGE technical team to adapt the infrastructure as needed for successful integration.

Resource availability: This may include:

- **Compute Resources:** Availability of compute capacity (CPU, RAM) for hosting shared scenarios or platform components. Minimum: 32 vCPU and 64GB RAM
- **Storage Resources:** Storage space for scenario data, logs, and other platform-related information. Minimum 0.5TB SSD.
- **Network Bandwidth**: Sufficient network bandwidth for reliable communication and data exchange with the platform and other connected ranges. Recommended is 1 GBit connection.

b) Cyber Range provider

Cyber Range capabilities: The Cyber Range should possess a core set of functionalities, such as:

- **Virtual environment management:** Capabilities for creating and managing virtual machines, networks, and infrastructure to support scenarios.
- **Exercise execution and control:** Mechanisms for launching, controlling, and monitoring exercises.
- **Logging and reporting:** System for logging events and generating reports on exercise activities and performance.
- **User management and access control:** Secure user authentication and authorization mechanisms.

- **Tools, technologies, and solutions that can be employed in advanced exercises encompass the following areas of expertise, though they are not limited exclusively to these fields:**
    a. Cloud Security
    b. Industrial Systems
    c. Physical Appliance (EDR/XDR/SIEM/Firewalls/IDS/IPS/DLP/Switches etc)
    d. Industry-specific technologies
    e. Mobile Security
    f. Digital forensics
    g. Threat Intelligence

Integration readiness: The Cyber Range must be technically prepared for integration with CYRESRANGE. This includes:

- **Support for at least one of the preferred integration methods:** API Connection (Vsphere/Proxmox), Hybrid Connection (WireGuard/OpenVPN), API Connection (Kubernetes), Cross-Range IPSEC/VPN Tunnels or custom.
- **Availability of technical documentation:** Provision of clear and comprehensive technical documentation describing the Cyber Range's architecture, APIs (if applicable), and integration points.

Willingness to adapt to integration requirements: Commitment to working with the CYRESRANGE technical team to adapt the Cyber Range as needed for successful integration.

Resource Availability. This may include:

- **Compute Resources:** Availability of compute capacity (CPU, RAM) for hosting shared scenarios or platform components. Minimum: 256 vCPU and 512GB RAM
- **Storage Resources:** Storage space for scenario data, logs, and other platform-related information. Minimum 1TB SSD.
- **Network Bandwidth**: Sufficient network bandwidth for reliable communication and data exchange with the platform and other connected ranges. Minimum 1 GBit connection.

Operational and Security Eligibility Criteria

Organizations must also meet the following operational and security criteria:

b) Infrastructure provider

- **Security standards:** Applicants must demonstrate commitment to robust security practices and adhere to relevant security standards. This includes:
- **Implementation of security best practices:** Demonstration of security best practices according to their needs.
- **Data protection and privacy:** Adherence to relevant data protection and privacy regulations, in particular the General Data Protection Regulation (GDPR).
- **Access control policies:** Implementation of strong access control policies to protect resources and data.
- **Operational capacity:** The Infrastructure Provider should demonstrate sufficient operational capacity to support integration and ongoing participation in CYRESRANGE
  - **Operational team**: Availability of a team responsible for the operation, maintenance, and support of the infrastructure.
  - **Uptime and availability**: Infrastructure should be available and should have a demonstrable track record.
  - **Support processes:** Established support processes for addressing technical issues, user inquiries, and platform-related matters.

c) Cyber Range provider

- **Security standards:** Applicants must demonstrate commitment to robust security practices and adhere to relevant security standards. This includes:
- **Implementation of security best practices:** Demonstration of security best practices in Infrastructure operation, including vulnerability management, patch management, incident response, and security monitoring.
- **Data protection and privacy:** Adherence to relevant data protection and privacy regulations, in particular the General Data Protection Regulation (GDPR).
- **Access control policies:** Implementation of strong access control policies to protect Cyber Range resources and data.
- **Operational capacity:** The Cyber Range operator must demonstrate sufficient operational capacity to support integration and ongoing participation in CYRESRANGE. This includes:
  - **Dedicated operational team:** Availability of a dedicated team responsible for the operation, maintenance, and support of the Cyber Range.
  - **Reliable uptime and availability:** Demonstrated history of reliable uptime and availability of the Cyber Range.

- **Support processes:** Established support processes for addressing technical issues, user inquiries, and platform-related matters.

- **Commitment to collaboration:** Willingness to actively participate in the CYRESRANGE community, contribute to platform development, and share knowledge and expertise with other partners.

VI. Budget and how to apply

VI.1. Budget

Financial support to third parties will be implemented in the form of **Grants for Financial Support**, in accordance with the applicable EU rules on transparency, non-discrimination, avoidance of conflict of interest, and sound financial management.

The total indicative budget available for this Open Call is allocated to support **a minimum of two (2) and a maximum of three (3) projects**.

- **Maximum grant amount per project:**
  - Minimum integration (Kubernetes, CyberEDU Infragator): 15,000 EUR
  - Advanced integration (WireGuard, OpenVPN, IPSEC, Vsphere/Proxmox API: 25,000 EUR
- **Funding rate:** of **95% of the eligible costs** incurred by the supported third party

The final grant amount awarded to each project will be determined based on the evaluation score, the proposed activities, and the available budget.

The financial support awarded under this Open Call will be provided as pre-financing. An advance payment 80% will be transferred to the beneficiary soon after the grant agreement is signed and the required administrative steps are completed, before eligible costs are fully incurred.

The Beneficiary reserves the right **not to award all available funds** or to **adjust the number of projects supported**, depending on the quality of proposals received and the outcome of the evaluation.

The budget requested under this call must be structured exclusively according to the following eligible cost categories, in line with EU funding rules:

- **Personnel costs**, covering staff directly engaged in the implementation of the proposed activities;
- **Other goods and services**, including consumables, and subcontracted services strictly necessary for the execution of the action;
- **Travel and subsistence costs**, incurred for participation in meetings, workshops, testing, validation, and other activities directly related to the action;
- **Indirect costs**, calculated in accordance with the applicable EU funding model.

Costs falling outside these categories are **not eligible**. All requested costs must be necessary, reasonable, and directly attributable to the implementation of the proposed activities, in compliance with the applicable EU financial and reporting requirements.

The budget will be included in Annex A - Application Form and will be structured as following:

Task	A. Personnel		C.1 Travel and subsistence	C.3 Other goods, works and services	E. Indirect costs	Total costs	In Kind Contribution
	Person Months	Total Euro					
WP1 - Project Management							
T1.1							
T1.2							
T1.3							
WP2 - Onboarding & Technical Integration							
T2.1							
T2.2							
....							
WP3 - Testing & Validation							
....							
Total	0	0	0	0	0	0	0

VI.2. Application submission

This Call for Proposals – Open Call for Independent Cyber Ranges is published for maximum transparency and EU-wide visibility via the EU Funding & Tenders Portal, ensuring broad outreach to eligible applicants and clear access to all official information, requirements, and submission instructions.

Open Call information website

The complete Open Call package (Guide for Applicants, Annexes, templates, FAQs, and updates) is available at **https://cyresrange.net** – the official project website. Applicants must submit their proposals electronically in accordance with the instructions set out below. The application must be finalized and submitted before the deadline.

Applications shall be prepared using **Annex A - Application Form** and **Annex B - Project Budget Form** which must be completed in full before submitting by email to **opencall@cyresrange.net**

The email submission must include:

- **Annex A – Application Form** as electronically signed (QES) PDF file attachment;
- **Annex B – Project Budget Form** in Excel (.xslx) file format;

Applicants will receive an acknowledgement of message receipt.

Please note that, in the proposal, you must select one of the five methods of connection between cyber ranges as described in the application template.

For more information about the call, you can contact us at opencall@cyresrange.net

VII. Award criteria

Applications for Onboarding Independent Cyber Ranges will be evaluated based on the following criteria, with the indicated weighting:

- **40%** – Technical Capabilities & Innovation
- **30%** – Experience & Expertise
- **30%** – Alignment with Platform Vision

1. Technical Capabilities and Innovation (Weight: 40%)

Criterion	**Description**	**Applicable To**	**High Score Indicators (Pass)**	**Low Score Indicators (Fail/Risk)**
Quality & Breadth of Functionalities	Richness of features for scenario	Cyber Range Providers	• Comprehensive feature set	• Limited/Basic feature set

	creation, virtualization, logging, and reporting.		• Advanced functionalities • Diverse scenario support • Robust operation	• Lack of advanced capabilities • Potential instability
Innovation & Uniqueness	Presence of unique technologies or approaches that differentiate the range.	Cyber Range Providers	• Demonstrable innovation • Novel approaches • Potential to set new standards	• Lack of innovation • Reliance on standard/outdated tech • Limited differentiation
New Capabilities Potential	Potential to bring new, valuable capabilities to the CYRESRANGE ecosystem.	Cyber Range Providers	• Adds significant new capabilities • Addresses unmet platform needs • Expands platform scope	• Overlap with existing functions • Minimal impact on enhancement • Limited potential
Integration Readiness	Technical preparedness for integration (APIs, interfaces, documentation).	Infra. & Cyber Range Providers	• Strong technical readiness • Clear documentation & APIs • Proactive integration planning	• Limited readiness • Lack of documentation • Significant technical hurdles • Reactive planning

2. Experience and Expertise (Weight: 30%)

Criterion	**Description**	**Applicable To**	**High Score Indicators (Pass)**	**Low Score Indicators (Fail/Risk)**

Track Record	Length and depth of experience in operating and managing cyber ranges.	Cyber Range Providers	• Extensive operational history • Proven success • Positive user feedback	• Short operational history • Lack of proven track record • Mixed or negative feedback
Team Expertise	Qualifications and skills of the team operating and supporting the range.	Infra. & Cyber Range Providers	• Highly qualified team • Specialized security expertise • Dedicated support staff	• Limited team experience • Skill gaps • Lack of specialized expertise • Limited support resources
Successful Deployments	Evidence of deployments (training, research) and user satisfaction.	Cyber Range Providers	• Strong evidence of deployments • Quantifiable satisfaction metrics • Positive case studies/testimonials	• Limited evidence of deployments • Anecdotal feedback only • Negative feedback • Small user base

3. Alignment with Platform Vision and Goals (Weight: 30%)

Criterion	**Description**	**Applicable To**	**High Score Indicators (Pass)**	**Low Score Indicators (Fail/Risk)**
Understanding of Vision	Articulation of CYRESRANGE goals and the collaborative approach.	Infra. & Cyber Range Providers	• Clear/Accurate understanding	• Vague or inaccurate understanding

			• Insightful perspective on collaboration • Well-articulated alignment	• Lack of appreciation for collaborative approach
Commitment to Collaboration	Willingness to share knowledge and contribute to the community.	Infra. & Cyber Range Providers	• Strong commitment to sharing • Active community participation • Proactive engagement	• Reluctance to share resources • Passive or no engagement • Limited commitment
Contribution to Success	Potential to enhance the overall value, reach, and impact of the platform.	Infra. & Cyber Range Providers	• Clear value proposition • Expands platform reach • Aligns with strategic objectives	• Unclear value proposition • Minimal impact on reach • Misalignment with objectives
Motivation & Benefits	Rationale for joining and expected benefits from onboarding.	Infra. & Cyber Range Providers	• Compelling motivation • Strategic alignment with goals • Clear expectations of benefits	• Weak or unclear motivation • Poorly defined rationale • Unclear understanding of value

VIII. Project start, duration and deliverables

The project will start after the signature of the Grant Agreement and the completion of all mandatory administrative steps.

The project duration will be up to two (2) months.

Prior to the start of project activities, selected applicants will be required to sign a Non-Disclosure Agreement (NDA) and any other mandatory intellectual property and confidentiality documents, as required by the Beneficiary.

Deliverables

Supported projects will be required to deliver, at a minimum:

- Completion of the onboarding and integration activities in line with the approved application:
    - API Connection (VSphere/Proxmox) [O]:
        - Administrative API access (full permissions)
        - NAT for VPN service, configured according to our specifications
        - Specific network segments, and appropriate routing and network policies configured according to our specifications
        - Run minimum one scenario on the infrastructure managed by CyberEDU using the infrastructure of the applicant
    - Hybrid Connection (WireGuard/OpenVPN) [O]
        - Specific network segments, and appropriate routing and network policies configured according to our specifications
        - Run minimum one scenario on the infrastructure managed by CyberEDU using the infrastructure of the CyberEDU and resources accessible from the Beneficiary
    - API Connection (Kubernetes) [O]
        - Administrative API access (full permissions) on a namespace to create services, pods, volumes, host ports etc
        - Appropriate routing and network policies configured according to our specifications to access remotely the nodes services
        - Run minimum one scenario on the infrastructure managed by CyberEDU using the infrastructure of the applicant
    - Non-standard Integration with CyberEDU Infragator [O]
        - Root access to at least 1 Virtual Machine
        - Appropriate routing and network policies configured according to our specifications to access remotely the nodes services from the machine
        - Run minimum one scenario on the infrastructure managed by CyberEDU using the infrastructure of the applicant

    - Cross-range using IPSEC/VPN tunnels [O]
        - Configuration of an IPSEC
        - Appropriate routing and network policies configured according to our specifications to access remotely the infrastructure
        - Run minimum one scenario on the infrastructure managed by CyberEDU using the infrastructure of the CyberEDU and resources accessible from the Beneficiary

- Active participation in the testing and validation activities during the project period;
- Submission of structured technical and operational feedback covering onboarding, integration, and validation phases;
- Any additional deliverables specified in the Grant Agreement.

Intellectual Property and Confidentiality

All intellectual property rights, confidentiality obligations, and access rights to results will be governed by the Grant Agreement, the Non-Disclosure Agreement, and any additional intellectual property documents signed prior to project start.

Failure to comply with these obligations may result in suspension of activities, reduction of the grant, or termination of the Grant Agreement.

This activity is organized under the project CYRESRANGE - No. 101128088, funded by Digital Programme, under the call DIGITAL-ECCC-2022-CYBER-03