CRDF GLOBAL
REQUEST FOR PROPOSAL Announcement

CRDF Global is seeking a contractor for Cyber Range Platform development.

This information serves for announcement purposes only.

Interested candidates must request the Request for Proposal (RFP) document with the detailed requirements from Oleksiy Fomin <ofomin@crdfglobal.org>.
Please indicate the RFP number in the "subject" line of your request: #RFP-31-UA-2023

Proposal submission deadline: January 31, 2024 (6:00 PM, Kyiv)

Summary:

CRDF Global is seeking proposals from qualified contractors to design and implement a Cyber Range Program to enhance critical infrastructure organizations' cybersecurity capabilities. The program's mission is to create a simulation environment that fosters collaboration, advanced training, research, verification, and testing in the field of cybersecurity.

Scope:

The Cyber Range Program includes the development of a cyber range platform and associated infrastructure. The program aims to facilitate training, research, verification, and collaboration within a simulated environment. The key objectives include:

1. Training:
   - Develop advanced exercises for cybersecurity specialists, teams, and teams of teams.
   - Conduct training in a simulated environment replicating real-world architectures.
   - Provide a safe space, including hardware execution of malicious content and activities.
2. Research:
   - Create a simulated environment for active and reactive cyber defense research.
   - Conduct research on an appropriate representation of the desired target systems.
   - Ensure a safe space for executing malicious content and activities.
3. Verification:
   - Develop a simulation environment for testing systems against existing cyber threats.
   - Verify new systems before deployment.
   - Replicate actively deployed systems for vulnerability and remediation activities.
   - Ensure a secure space for executing malicious content and activities.
4. Collaboration:
   - Enable participants to share intelligence, data, techniques, and best practices.
   - Facilitate collaboration across sectors and industries, including non-technical teams.
   - Establish best practices, policies, and procedures for active and reactive defense teams.

Tasks and Deliverables:

Respondents are expected to propose solutions that address the following tasks:

1. The contractor is expected to design and implement a Cyber Range Platform based on the guidelines provided in the comprehensive "Cyber Range Platform Architecture" document. This document includes a detailed description of the best approach, system architecture, specifications, requirements, and platform-building guidelines. The detailed "Cyber Range Platform Architecture" document attached to this RFP.
2. Design and implement a Cyber Range Platform with orchestration software, hardware infrastructure, and a learning management system.
3. Develop operational networks, servers, and storage for the infrastructure hosted on physical infrastructure.
4. Specify the choice of cloud infrastructure with detailed responsibilities for operations and configurations.
5. Design and implement a User Interface (UI) for the management system, accessible through supported web browsers.
6. Ensure different layouts based on access levels, simulation modes, and participation types.
7. Provide documentation outlining technical requirements and architectural options for Cyber Range deployment.
8. Collaborate with stakeholders to define learning objectives, exercise scenarios, and collaboration frameworks.
9. Conduct training sessions for key personnel involved in the operation of the Cyber Range Program.

https://www.prostir.ua/?post_type=grants&p=511172&preview=true