

## **Resilienza, coordinamento e gamme di sicurezza informatica dell'UE EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges**

**TOPIC ID:** DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE

**Ente finanziatore:** Commissione europea, Programma Digital Europe

**Obiettivi ed impatto attesi:** I risultati attesi saranno una forte capacità degli Stati membri di reagire in modo coordinato agli incidenti di cybersecurity su larga scala, nonché gamme di cybersecurity di alto livello che offrono competenze avanzate, conoscenze e piattaforme di test.

L'attuazione di questo tema ha due obiettivi principali:

- Rafforzare la capacità degli attori della sicurezza informatica nell'Unione di monitorare gli attacchi e le minacce informatiche e i rischi della catena di approvvigionamento, di reagire congiuntamente contro gli incidenti di grandi dimensioni e di migliorare le conoscenze, le competenze e la formazione pertinenti. Questo obiettivo sarà perseguito attraverso l'attuazione del Piano e della futura Unità cibernetica comune, considerando l'importante ruolo della rete dei Computer Security Incident Response Teams (CSIRTs) e della Cyber Crisis Liaison Organization Network (CyCLONE).
- Creare, interconnettere e rafforzare le gamme di sicurezza informatica a livello europeo, nazionale e regionale, nonché all'interno e tra le infrastrutture critiche, compresi, ma non solo, i settori coperti dalla direttiva sulla sicurezza delle reti e dell'informazione, al fine di condividere le conoscenze e le informazioni sulle minacce alla sicurezza informatica tra le parti interessate negli Stati membri, monitorare meglio le minacce alla sicurezza informatica e rispondere congiuntamente agli attacchi informatici.

Ambito di applicazione:

Le proposte relative al primo obiettivo dovrebbero rafforzare la capacità degli attori della cybersicurezza di reagire in modo coordinato agli incidenti di cybersicurezza su larga scala, promuovendo il ruolo dei CSIRT, della rete CyCLONE, della futura Unità congiunta di cybersicurezza e tenendo conto del piano d'azione.

Le proposte relative al secondo obiettivo dovrebbero sostenere la creazione, il funzionamento, l'aumento della capacità e/o l'adozione di gamme di cybersicurezza, nonché promuovere la creazione di reti tra di esse al fine di sviluppare le capacità e le competenze in materia di cybersicurezza nelle tecnologie chiave (ad esempio, 5G, Internet degli oggetti, cloud, intelligenza artificiale, sistemi di controllo industriale) e nei settori applicativi (ad esempio, sanità, energia, finanza, trasporti, telecomunicazioni, produzione agroalimentare, gestione delle risorse), tenendo conto anche degli effetti a cascata tra i settori. Questa azione mira a:

- scambiare conoscenze tra le gamme di cybersicurezza e creare archivi di dati comuni;
- sostenere scenari su larga scala e intersettoriali che coprono un'ampia gamma di avversari e strategie di attacco, compresi, ad esempio, esercizi di serious gaming tra centri; consentire simulazioni realistiche del

traffico che riflettano le condizioni della rete;

- supportare la formazione strutturata e le esercitazioni di cybersecurity per preparare i difensori della cybersecurity presso organizzazioni pubbliche e private a migliorare la protezione e la resilienza delle infrastrutture critiche, delle imprese e delle reti di comunicazione; consentire la conduzione di formazioni ibride che coinvolgano tutti i livelli rilevanti per l'individuazione, l'attenuazione e la prevenzione degli attacchi informatici (tattici, operativi, strategici), creando al contempo un ambiente in cui allenare la comunicazione, il coordinamento e il processo decisionale;
- fornire servizi aggiuntivi alle parti interessate, come metodologie di test strutturate, database delle vulnerabilità e strumenti forensi; sviluppare opzioni di erogazione di contenuti automatizzati a supporto di specifici profili professionali.

**Criteri di eleggibilità:** Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:

- essere persone giuridiche (enti pubblici o privati)
- essere stabiliti in uno dei Paesi ammissibili, ossia:
  - Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) per tutti i temi
  - Paesi SEE (Norvegia, Islanda, Liechtenstein) per tutti i temi.

I beneficiari e gli enti affiliati devono registrarsi nel Registro dei partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation). Per la convalida, sarà richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine. Si ricorda che tutti i temi di questo bando sono soggetti a restrizioni per motivi di sicurezza, pertanto i soggetti non devono essere controllati direttamente o indirettamente da un Paese che non sia un Paese ammissibile. Tutti i soggetti dovranno compilare e presentare una dichiarazione sulla proprietà e sul controllo. Inoltre: - la partecipazione a qualsiasi titolo (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità dei Paesi ammissibili - le attività del progetto (incluso il lavoro in subappalto) devono svolgersi nei Paesi ammissibili (si veda la sezione localizzazione geografica di seguito e la sezione 10) - la Convenzione di sovvenzione può prevedere restrizioni sui diritti di proprietà intellettuale

I progetti che coinvolgono informazioni classificate dall'UE devono essere sottoposti a un esame di sicurezza per autorizzare il finanziamento e possono essere soggetti a specifiche norme di sicurezza (dettagliate in una lettera sugli aspetti di sicurezza (SAL) allegata alla Convenzione di sovvenzione).

Target group

Il primo obiettivo è aperto a tutte le organizzazioni dell'UE con esigenze di sicurezza informatica. Per il secondo obiettivo, le principali parti interessate sono i creatori e i fornitori di servizi di Cybersecurity Range dell'UE.

**Contributo finanziario:** IL budget totale della call è di EURO 3.416.320,50

Tipo di azione e tasso di finanziamento:

Azioni di sostegno alle PMI - tasso di finanziamento del 50% e del 75% (per le PMI)

Budget del progetto (importo massimo della sovvenzione):

- per l'argomento DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE: tra 1 e 2 milioni di EUR per progetto.

**Scadenza:** 06 July 2023 17:00:00 Brussels time

**Ulteriori informazioni:**

[call-fiche\\_digital-eccc-2022-cyber-b-03\\_en.pdf \(europa.eu\)](#)

