Hub Cibernetici Transfrontalieri
Cross-Border Cyber Hubs

TOPIC ID:
DIGITAL-ECCC-2026-DEPLOY-CYBER-10-CBCH

Ente finanziatore:
Commissione europea
Digital Europe Programme (DIGITAL)

Obiettivi ed impatto attesi:

Risultati attesi

1. Creazione di Cyber Hub transfrontalieri di livello mondiale in tutta l'Unione europea per la raccolta e l'analisi dei dati sulle minacce informatiche tra diversi Stati membri. Tali Hub dovranno essere dotati di infrastrutture altamente sicure e di strumenti avanzati di analisi dei dati, in grado di rilevare, raccogliere e archiviare informazioni sulle minacce informatiche, nonché di analizzare, condividere e riportare informazioni di Cyber Threat Intelligence (CTI), revisioni e analisi.
2. Rafforzamento della condivisione della Threat Intelligence tra i National Cyber Hub e definizione di accordi strutturati di condivisione delle informazioni con le autorità competenti e le reti pertinenti, incluse le Computer Security Incident Response Teams (CSIRT).

Obiettivo dell'azione
Le precedenti piattaforme SOC transfrontaliere sono state finanziate nell'ambito di call precedenti e tale modello di collaborazione è previsto anche per i Cyber Hub transfrontalieri. Questi ultimi dovrebbero fornire capacità nuove, aggiuntive e complementari, integrandosi con i SOC e i Cyber Hub esistenti, le Computer Security Incident Response Teams (CSIRT), gli Information Sharing and Analysis Centers (ISAC) e altri attori rilevanti dell'ecosistema della cybersicurezza.
L'azione è rivolta principalmente alla creazione di nuovi Cyber Hub transfrontalieri. Tuttavia, ove pertinente, potranno essere incluse attività di supporto per SOC già avviati nell'ambito dei precedenti Programmi di lavoro DIGITAL (2021–2022 e 2023–2024), al fine di garantire una collaborazione efficace con i Cyber Hub transfrontalieri.

Ambito delle attività
Oltre allo sviluppo di processi, strumenti e servizi per la prevenzione, il rilevamento e l'analisi di attacchi informatici emergenti, l'ambito dell'azione comprende anche:

- l'acquisizione e/o l'adozione di strumenti comuni, inclusi strumenti di automazione;
- la definizione di processi condivisi;
- la realizzazione di infrastrutture dati comuni per la gestione e la condivisione, a livello dell'Unione europea, di informazioni operative di cybersicurezza contestualizzate e azionabili.

Dovranno essere presi in considerazione standard aperti e ampiamente consolidati per la condivisione della Cyber Threat Intelligence, quali ad esempio MISP o altri standard riconosciuti, nonché standard per l'automazione delle informazioni di advisory (ad esempio CSAF) e per lo scambio di messaggi relativi alla cybersicurezza (ad esempio tramite IntelMQ).
I Cyber Hub transfrontalieri potranno inoltre prevedere capacità di monitoraggio di infrastrutture critiche sottomarine, come i cavi sottomarini.

Criteri di eleggibilità:
Requisiti di idoneità dei richiedenti
Per essere idonei, i richiedenti (beneficiari ed entità affiliate) devono essere entità giuridiche, pubbliche o private, ed essere stabiliti in uno dei Paesi idonei, ovvero:

- Stati membri dell'Unione europea, inclusi i Paesi e Territori d'Oltremare (OCT);
- Paesi dello Spazio Economico Europeo (SEE): Norvegia, Islanda e Liechtenstein.

I beneficiari e le entità affiliate devono registrarsi nel Registro dei Partecipanti prima della presentazione della proposta ed essere convalidati dal Servizio Centrale di Validazione (REA Validation). Ai fini della validazione, sarà richiesto di caricare la documentazione attestante lo status giuridico e il Paese di origine.
Altre entità possono partecipare al progetto con ruoli diversi all'interno del consorzio, quali partner associati, subappaltatori, terze parti che forniscono contributi in natura o altri ruoli previsti (cfr. sezione 13).

Restrizioni di sicurezza e controllo
Tutti i temi oggetto della call sono soggetti a restrizioni legate alla sicurezza. Di conseguenza, le entità partecipanti non devono essere controllate, direttamente o indirettamente, da Paesi non idonei.
Tutte le entità coinvolte devono compilare e presentare una dichiarazione di proprietà e controllo. In particolare:

- la partecipazione, in qualsiasi ruolo (beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di supporto finanziario a terzi), è limitata a entità stabilite e controllate nei Paesi idonei;
- le attività di progetto, inclusi eventuali lavori subappaltati, devono svolgersi nei Paesi idonei;
- l'Accordo di Sovvenzione può prevedere restrizioni in materia di proprietà intellettuale (cfr. sezione 10).

Le condizioni relative alla partecipazione e al controllo devono, in linea di principio, essere soddisfatte già in fase di presentazione della proposta (scadenza della call). Lo status non può essere modificato durante la fase di Grant Agreement Preparation (GAP), salvo approvazione dell'autorità concedente.

Controlli da parte dell'Unione europea
I controlli da parte dell'UE riguardano beneficiari, entità affiliate, partner associati e subappaltatori. Gli altri partecipanti devono essere verificati direttamente dal consorzio.
Ai fini dei controlli UE, i partecipanti devono essere registrati nel Registro dei Partecipanti (almeno con una bozza di PIC). Per beneficiari ed entità affiliate, i controlli si basano sui dati PIC validati; per gli altri

partecipanti, sulle informazioni pubblicamente disponibili.
Per “controllo” si intende la possibilità di esercitare un’influenza decisiva su un partecipante, direttamente o indirettamente, attraverso una o più entità intermedie, sia de jure sia de facto. Tale controllo include non solo la proprietà di oltre il 50% delle quote o azioni, ma anche qualsiasi altro elemento o diritto che consenta di esercitare un’influenza determinante.
I partecipanti soggetti a controllo UE dovranno presentare una dichiarazione di controllo della proprietà come parte della proposta e, successivamente, fornire la documentazione di supporto richiesta. Qualora siano ammesse garanzie, alle entità non idonee potrà essere richiesto di compilare il relativo modello di garanzia, farlo approvare dall’autorità competente del Paese di stabilimento e presentarlo all’autorità concedente per la valutazione.
In ogni caso, i finanziamenti saranno assegnati esclusivamente ai richiedenti che abbiano superato la valutazione dell’azione congiunta di approvvigionamento.

Composizione del consorzio
DIGITAL-ECCC-2026-DEPLOY-CYBER-10-CBCH — Cyber Hub transfrontalieri
Nel caso di nuovi Cyber Hub transfrontalieri, i consorzi devono essere composti da beneficiari provenienti da almeno tre Paesi idonei.
Nel caso di ampliamento di una sovvenzione transfrontaliera in corso, il nuovo consorzio deve essere composto dal coordinatore della sovvenzione in essere e dalle nuove entità che intendono aderire al consorzio ospitante del Cyber SOC transfrontaliero.

Contributo finanziario:
Il budget stimato disponibile per la call è di 2.000.000 EUR
Tipo di azione e tasso di finanziamento Simple Grants — tasso di finanziamento del 50%

Scadenza:
28 Maggio 2026 17:00:00 Brussels time

Ulteriori informazioni:
Call for proposals: DIGITAL-ECCC-2026-DEPLOY-CYBER-10 | European Cybersecurity Competence Centre and Network