Hub Nazionali Cyber
National Cyber Hubs

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

Ente finanziatore:
Commissione europea
Digital Europe Programme (DIGITAL)

Obiettivi ed impatto attesi:
Finalità delle azioni
Le azioni mirano a creare o rafforzare i National Cyber Hubs, che svolgono un ruolo centrale nel garantire la cybersicurezza delle autorità nazionali, dei fornitori di infrastrutture critiche e dei servizi essenziali.
I Cyber Hub, in collaborazione con altre entità nazionali e regionali pertinenti, hanno il compito di monitorare, comprendere e gestire in modo proattivo le minacce alla cybersicurezza. Essi assumono un ruolo operativo cruciale nel garantire la cybersicurezza all'interno dell'Unione europea e sono responsabili della gestione di informazioni sensibili.

Impatto atteso

Creare National Cyber Hub di livello mondiale in tutta l'Unione, supportati da tecnologie all'avanguardia, che fungono da centri di raccolta e archiviazione di dati sulle minacce alla cybersecurity, analisi di tali dati e condivisione e riferimento di CTI, revisioni e analisi, tenendo conto di standard ben consolidati per i processi di condivisione e automazione.
Capacità di intelligence sulle minacce e consapevolezza situazionale e rafforzamento delle capacità a supporto della collaborazione rafforzata tra attori della cybersecurity, inclusi attori privati e pubblici.

1. Corsi di formazione mirati sulla base dell'ECSF per migliorare la capacità dei ruoli nella cybersecurity.
2. Applicazioni per la notifica automatica di attori privati e pubblici riguardo a sistemi compromessiti o insicuri

Obiettivo:
Quando uno Stato membro decide di partecipare al Sistema Europeo di Allerta per la Cybersecurity, designa o, se applicabile, istituisce un Hub Nazionale Informatico, un'entità unica che agisce sotto l'autorità dello Stato membro.
I National Cyber Hub hanno la capacità di fungere da punto di riferimento e porta d'accesso ad altre organizzazioni pubbliche e private a livello nazionale per raccogliere e analizzare informazioni su minacce e incidenti informatici e per contribuire a un Cyber Hub transfrontaliero. Sono in grado di rilevare, aggregare e analizzare dati e informazioni rilevanti per minacce e incidenti informatici, come l'intelligence sulle minacce informatiche, utilizzando in particolare tecnologie all'avanguardia e con l'obiettivo di

prevenire incidenti.
Per il ciclo di programmazione successivo, l'accento è posto sulla continuazione delle attività avviate negli anni passati.
L'obiettivo è creare o rafforzare i National Cyber Hubs, con strumenti all'avanguardia per monitorare, comprendere e gestire proattivamente eventi informatici, in stretta collaborazione con entità rilevanti come CSIRT, ISAC, ecc. Inoltre, quando possibile, beneficeranno di informazioni e feed provenienti da altri Cyber Hub nei loro paesi e utilizzeranno i dati aggregati e le analisi per fornire allerti precoci alle infrastrutture critiche di mira su base di necessità di conoscenza. I National Cyber Hub potrebbero anche considerare la possibilità di monitorare infrastrutture sottomarine, come cavi sottomarini.

L'obiettivo è costruire capacità per i nuovi o esistenti Cyber Hub Nazionali, ad esempio attrezzature, strumenti, flussi dati, così come i costi legati all'analisi dei dati, all'interconnessione con i Cyber Hub transfrontalieri, ecc. Questo può includere, ad esempio, strumenti di automazione, analisi e correlazione e flussi di dati che coprono l'Intelligence sulle Minacce Cibernetiche (CTI) a vari livelli, che vanno dai dati sul campo ai dati di Security Information and Event Management (SIEM) fino a CTI di livello superiore.
L'automazione è un aspetto chiave nella gestione e elaborazione efficiente delle informazioni. Dove disponibili, dovrebbero essere utilizzati standard già consolidati, come il Common Security Advisory Framework (CSAF)1, per avvisi di sicurezza o per la raccolta e l'elaborazione di messaggi relativi alla cybersecurity (ad esempio il progetto IntelMQ2). Le applicazioni sviluppate dai Cyber Hub/SOC dovrebbero essere compatibili con progetti europei di standardizzazione come il database delle vulnerabilità dell'UE (EUVD). I National Cyber Hub dovrebbero inoltre sfruttare tecnologie all'avanguardia come l'intelligenza artificiale e l'apprendimento dinamico del panorama e del contesto delle minacce. Ciò include anche l'uso di informazioni di cybersecurity condividete, per quanto possibile basate su tassonomie e/o ontologie esistenti, e hardware per garantire lo scambio e l'archiviazione sicuri delle informazioni. Le operazioni dovrebbero essere basate sui dati di rete in tempo reale e su altri dati di addestramento richiesti nelle fasi iniziali. Quando rilevante, si dovrebbe considerare le PMI come destinatari finali delle informazioni operative sulla cybersecurity.
Un elemento chiave è la traduzione di IA avanzata, analisi dei dati e altri strumenti di cybersecurity rilevanti dai risultati della ricerca agli strumenti operativi, e ulteriori test e validazioni in condizioni reali in combinazione con l'accesso a strutture di supercalcolo (ad esempio per potenziare le funzionalità di correlazione e rilevamento delle piattaforme transfrontaliere). Tali attività sono identificate e proposte per il finanziamento nella sezione 2.3, dedicata all'IA per la Cybersecurity, e nell'argomento 2.3.1.
Inoltre, i National Cyber Hub potrebbero anche considerare di implementare soluzioni per la sorveglianza e la protezione di infrastrutture sottomarine critiche, come cavi sottomarini, e per il rilevamento di attività dannose intorno a esse, per migliorare la resilienza e la sicurezza di queste infrastrutture, fondamentali per le comunicazioni globali. La risposta a tali minacce ibride potrebbe includere anche la consapevolezza situazionale effettuata attraverso la raccolta e l'analisi di dati sensori in situ, basati sul mare, nonché di immagini satellitari rilevanti. Per tali attività sono necessarie sinergie operative con il Programma Spaziale Copernicus dell'UE e in particolare con il suo Servizio di Sicurezza.
Un altro ruolo chiave per i National Cyber Hub è facilitare il trasferimento e la condivisione delle

conoscenze, oltre a supportare iniziative di formazione per tutti i ruoli necessari nella cybersecurity basati, ad esempio, nel Quadro Europeo delle Competenze in Cybersecurity (ECSF3). Ad esempio, i Cyber Hub/ SOC che si occupano delle infrastrutture critiche svolgono un ruolo chiave e dovrebbero beneficiare delle conoscenze e delle esperienze acquisite o concentrate nei National Cyber Hubs.
I National Cyber Hub devono condividere informazioni con altri stakeholder in uno scambio reciprocamente vantaggioso e impegnarsi a fare domanda per partecipare a un Cyber Hub Transfrontaliero entro i prossimi 2 anni, con l'obiettivo di scambiare informazioni con altri National Cyber Hubs.
Per raggiungere questo obiettivo, sarà lanciato un appello alla manifestazione di interesse a determinate entità degli Stati Membri che forniscano le strutture necessarie per ospitare e gestire i National Cyber Hub. I candidati alla chiamata per espressioni di interesse dovrebbero descrivere gli obiettivi e gli scopi del National Cyber Hub, descrivere il suo ruolo e come tale ruolo si relazioni ad altri attori della cybersecurity, come i CSIRT, e la sua potenziale cooperazione con altri stakeholder pubblici o privati della cybersecurity. I richiedenti devono inoltre fornire la pianificazione dettagliata delle attività e dei compiti del National Cyber Hub, dei servizi che offrirà, del modo in cui opererà e sarà operativo, e descrivere la durata dell'attività, nonché i principali traguardi e risultati realizzativi. Dovrebbero inoltre specificare quali attrezzature, strumenti e servizi devono essere acquistati e integrati per costruire il National Cyber Hub, i suoi servizi e la sua infrastruttura.
Per supportare le attività sopra descritte di un National Cyber Hub, sono previste le seguenti due linee di attività:

1. [Acquisti] Un'azione congiunta di approvvigionamento con lo Stato membro dove si trova il National Cyber Hub: questo coprirà l'acquisto delle principali infrastrutture, degli strumenti e dei servizi necessari per costruire il National Cyber Hub.
2. [Costruzione e gestione del National Cyber Hub] Sarà inoltre disponibile un finanziamento per coprire, tra le altre cose, le attività preparatorie per l'istituzione del National Cyber Hub, la sua interazione e cooperazione con altri portatori di interesse, nonché i costi operativi coinvolti, che consentano il funzionamento efficace del National Cyber Hub, ad esempio l'utilizzo dell'infrastruttura, Strumenti e servizi acquistati tramite l'acquisto congiunto. Questi indicheranno anche traguardi e risultati per monitorare i progressi

Le domande devono essere presentate a entrambi i flussi di lavoro. Le domande saranno soggette a una procedura di valutazione. I finanziamenti saranno assegnati solo ai richiedenti che hanno superato la valutazione dell'azione congiunta di approvvigionamento.

Criteri di eleggibilità:

Quadro normativo e condizioni di applicazione
Ai sensi dell'articolo 12, paragrafo 5 bis, della Legge sulla Solidarietà Informatica, che modifica l'articolo 12 del Regolamento (UE) 2021/694, il paragrafo 5 del medesimo articolo non si applica qualora le condizioni stabilite dal paragrafo 5 bis siano soddisfatte in modo cumulativo.
La valutazione di tali condizioni deve tenere conto dei risultati della mappatura della disponibilità di

strumenti, infrastrutture e servizi per i National Cyber Hubs, da effettuarsi da parte dell'ECCC ai sensi dell'articolo 9, paragrafo 4, della Legge sulla Solidarietà Informatica.
Il primo esercizio di mappatura è attualmente in corso. Fino al completamento di tale mappatura e in conformità con le disposizioni pertinenti della Legge sulla Solidarietà Informatica, la partecipazione alle call finanziate nell'ambito di questo tema è soggetta alle restrizioni previste dall'articolo 12, paragrafo 5, come specificato nell'Appendice 3 del Programma di lavoro.
Tali condizioni di sicurezza potranno essere successivamente modificate, tenendo conto dei risultati finali della mappatura dei servizi effettuata dall'ECCC ai sensi dell'articolo 9, paragrafo 4, della Legge sulla Solidarietà Informatica.

Restrizioni su proprietà intellettuale e controlli
L'Accordo di Sovvenzione può prevedere restrizioni in materia di proprietà intellettuale (cfr. sezione 10).
Per le restrizioni che limitano la partecipazione a specifici Paesi idonei, la relativa condizione deve essere, in linea di principio, soddisfatta già nella fase di presentazione della proposta (alla scadenza della call). Lo status non può essere modificato durante la fase di Grant Agreement Preparation (GAP), salvo approvazione dell'autorità concedente.
I seguenti partecipanti sono soggetti a controlli da parte dell'Unione europea:

- beneficiari;
- entità affiliate;
- partner associati;
- subappaltatori.

Gli altri partecipanti devono essere controllati dal consorzio.
Per i 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, sui dati pubblicamente disponibili.
Ai fini delle restrizioni di controllo sulla proprietà, 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.
Anche in questo caso, la condizione deve essere soddisfatta già in fase di presentazione della proposta e non può essere modificata durante il GAP, salvo approvazione dell'autorità concedente.
I partecipanti soggetti a controllo UE dovranno compilare e presentare una dichiarazione di controllo di proprietà come parte integrante della proposta e, successivamente, fornire la documentazione di supporto richiesta.
Quando sono consentite garanzie, alle entità non idonee potrà essere richiesto di compilare il modello di garanzia, farlo approvare dall'autorità competente del Paese di stabilimento e presentarlo all'autorità concedente, che ne valuterà la validità.
Infine, per tutti i temi, i finanziamenti saranno assegnati esclusivamente ai richiedenti che abbiano superato la valutazione relativa all'azione congiunta di approvvigionamento.

Composizione del consorzio

Per il tema DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs, possono richiedere il finanziamento esclusivamente le entità designate a livello di Stato membro come National SOC.
Il progetto deve essere presentato da un unico beneficiario.

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

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