INFO SCOUTING	
Periodo di scouting:	**23/01/2025**
Fonte:	https://www.acn.gov.it/portale/ncc-italia/opportunita-di-finanziamento?
DESCRIZIONE BANDO	
Ente proponente:	**Commissione europea**
Tipologia di bando:	Bando nell'ambito Digital Europe Programme
Bando/call:	**Deployment Actions in the area of Cybersecurity** **(DIGITAL-ECCC-2024-DEPLOY-CYBER-07)**
Tema/obiettivo del bando:	Il secondo programma di lavoro (WP) Cybersecurity del programma Europa digitale 2023-2024 introduce azioni che sviluppano ulteriormente le capacità di cybersecurity dell'UE e ne migliorano la resilienza nel contesto della strategia per la cybersecurity dell'UE. Le azioni incluse in questo documento di invito sosterranno in particolare gli obiettivi indicati di seguito. • *Azioni volte a creare un ecosistema avanzato (all'avanguardia) di rilevamento delle minacce e analisi degli incidenti informatici costruendo le capacità dei* ***Security Operation Centre*** *(SOC), a livello nazionale e transfrontaliero. Si tratta di azioni a supporto della creazione del sistema europeo di allerta informatica come definito nel Cyber Solidarity Act.* • *Azioni mirate a rafforzare l'ecosistema SOC esistente.* • *Azioni che mirano a sviluppare innovazioni nelle tecnologie digitali chiave come l'intelligenza artificiale (inclusa l'intelligenza artificiale generativa e l'intelligenza artificiale avversaria), l'analisi dei big data, la tecnologia quantistica, blockchain, l'elaborazione ad alte prestazioni e il software-defined networking, con l'obiettivo di consentire agli attori europei della sicurezza informatica di trarne vantaggio migliorando le capacità di rilevamento e prevenzione, l'efficienza, la scalabilità e facilitando la condivisione dei dati e la conformità normativa*

	• *Un meccanismo che mira a integrare gli sforzi degli Stati membri e di quelli a livello di Unione per aumentare il livello di protezione e resilienza alle minacce informatiche, in particolare per grandi installazioni e infrastrutture industriali.* • *Azioni incentrate sullo sviluppo di capacità e sul rafforzamento della cooperazione in materia di sicurezza informatica a livello tecnico, operativo e strategico, nel contesto delle legislazioni UE esistenti e proposte in materia di sicurezza informatica.* • *Tutti gli argomenti sono soggetti alle disposizioni dell'articolo 12(5) del regolamento sul programma Europa digitale.* Il bando è lanciato in conformità con il programma di lavoro 2023-2024 e sarà gestito dalla Commissione europea, Direzione generale per la comunicazione, le reti, i contenuti e la tecnologia (DG CONNECT), per conto dell'European Cybersecurity Competence Centre (ECCC), finché l'ECCC non avrà la capacità di implementare il proprio bilancio. Il bando riguarda i seguenti argomenti: ***– DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - SOC nazionali*** ***–DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT- Ampliamento di piattaforme SOC transfrontaliere esistenti o Lancio di nuove piattaforme SOC*** ***–DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS- Rafforzamento dell'ecosistema SOC*** ***– DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Sviluppo e Distribuzione di tecnologie chiave avanzate*** ***–DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER- Supporto alla preparazione e assistenza reciproca, mirati a operazioni e installazioni industriali più grandi*** ***–DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02- Supporto per l'implementazione della legislazione UE sulla sicurezza informatica e delle strategie nazionali di sicurezza informatica (2024)***

	DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs *L'obiettivo è creare o rafforzare i SOC nazionali, in particolare con strumenti all'avanguardia per il monitoraggio, la comprensione e la gestione proattiva degli eventi informatici, in stretta collaborazione con entità pertinenti come i CSIRT. Inoltre, ove possibile, trarranno vantaggio dalle informazioni e dai feed di altri SOC nei loro paesi e utilizzeranno i dati aggregati e le analisi per fornire avvisi tempestivi alle infrastrutture critiche mirate in base alla necessità di sapere.* **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT–Enlarging existing or Launching New Cross-Border SOC Platforms** *L'obiettivo generale delle piattaforme SOC transfrontaliere è rafforzare le capacità di analizzare, rilevare e prevenire le minacce informatiche e supportare la produzione di intelligence di alta qualità sulle minacce informatiche, in particolare attraverso lo scambio di dati da varie fonti, pubbliche e private, nonché attraverso la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi e prevenzione informatica in un ambiente affidabile. Questa azione mira a nuove piattaforme SOC transfrontaliere, nonché a supportare quelle che erano già state avviate nell'ambito del precedente programma di lavoro DIGITAL (2021-2022). Sebbene l'attenzione principale di questa azione sia sui processi e sugli strumenti per la prevenzione, il rilevamento e l'analisi degli attacchi informatici emergenti, prevede anche in particolare l'acquisizione e/o l'adozione di strumenti (di automazione), processi e infrastrutture di dati condivise comuni per la gestione e la condivisione di informazioni operative sulla sicurezza informatica contestualizzate e fruibili in tutta l'UE.* **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS– Strengthening the SOC Ecosystem** *Questo argomento integra altre azioni in questo e nel precedente Programma di lavoro, che stanno creando SOC nazionali e piattaforme SOC transfrontaliere. Rafforzerà i SOC collegati ai SOC nazionali e a una più forte collaborazione tra SOC locali, SOC*

	nazionali e piattaforme SOC transfrontaliere, portando a una maggiore condivisione dei dati e a una migliore capacità di rilevamento delle minacce informatiche. Ciò dovrebbe in particolare promuovere l'interoperabilità, identificando quali dati possono essere condivisi, come vengono condivisi e in quale formato, requisiti e accordi di condivisione e modi per consentire uno scambio migliore. Possono anche essere previsti collegamenti alle azioni finanziate nell'ambito della Cybersecurity Skills Academy (nel programma di lavoro principale Digital Europe). Le azioni dovrebbero portare a un maggiore coinvolgimento, anche da parte del settore privato, e a una migliore collaborazione verso una base di conoscenza comune sulle minacce informatiche dell'UE e all'indipendenza tecnologica. Inoltre, le piattaforme SOC transfrontaliere svilupperanno un quadro di governance completo, con ad esempio condizioni di iscrizione e procedure di verifica. L'obiettivo è promuovere la discussione tra tali piattaforme, condividendo le best practice e identificando opportunità di collaborazione. *Sarà selezionata un'azione di coordinamento e supporto, che riunisca la più ampia rete possibile di piattaforme SOC nazionali e transfrontaliere.* **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH- Development and Deployment of Advanced Key Technologies** *Le innovazioni nelle principali tecnologie digitali come l'intelligenza artificiale (compresa l'intelligenza artificiale generativa e l'intelligenza artificiale avversaria), l'analisi dei big data, la tecnologia quantistica, la tecnologia blockchain, l'elaborazione ad alte prestazioni e la rete definita dal software, creano nuove opportunità per far progredire la sicurezza informatica nelle aree di rilevamento delle vulnerabilità, rilevamento delle minacce e risposta rapida, riducendo la finestra di opportunità per gli aggressori di sfruttare queste vulnerabilità. Inoltre, potrebbero consentire nuove possibilità per proteggere la sicurezza dei dati e la privacy. L'obiettivo è consentire agli attori europei della sicurezza informatica di sfruttare queste nuove innovazioni, migliorando le capacità di rilevamento e prevenzione, l'efficienza, la scalabilità e facilitando la*

	condivisione dei dati e la conformità normativa. In particolare, le tecnologie innovative dovrebbero consentire l'elaborazione di grandi quantità di dati, automatizzando il riconoscimento di modelli in tempo reale, l'analisi dei log, la scansione delle vulnerabilità, consentendo al contempo ai professionisti della sicurezza di concentrarsi su un'interpretazione di livello superiore dei dati e sulle decisioni di risposta. Dovrebbero consentire alle organizzazioni di implementare soluzioni su larga scala e in ambienti sempre più complessi. Una priorità è creare e rafforzare la capacità di fornire informazioni originali sulle minacce informatiche (CTI), ad esempio sotto forma di feed o servizi CTI. **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER- Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations** *Questo meccanismo mira a integrare e non duplicare gli sforzi degli Stati membri e di quelli a livello di Unione per aumentare il livello di protezione e resilienza alle minacce informatiche, in particolare per i grandi impianti e infrastrutture industriali, assistendo gli Stati membri nei loro sforzi per migliorare la preparazione alle minacce e agli incidenti informatici fornendo loro conoscenze e competenze.* **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)** *L'azione si concentra sullo sviluppo delle capacità e sul potenziamento della cooperazione sulla sicurezza informatica a livello tecnico, operativo e strategico, nel contesto della legislazione UE esistente e proposta sulla sicurezza informatica, in particolare la direttiva NIS2 (direttiva (UE) 2022/2555), il Cybersecurity Act e la direttiva sugli attacchi contro i sistemi di informazione (direttiva 2013/40). Integra il lavoro dei SOC nell'area del rilevamento delle minacce. È una continuazione del lavoro attualmente supportato nell'ambito del precedente Digital Work Programme. Inoltre, questa azione mira anche a supportare l'attuazione del proposto Cyber Resilience Act (CRA) da parte delle autorità di vigilanza del mercato/autorità di*

	notifica/organismi di accreditamento nazionali, aumentando le loro capacità di garantire un'attuazione efficace del CRA. Le proposte devono contribuire al raggiungimento di almeno uno di questi obiettivi: • *Sviluppo della fiducia tra gli Stati membri.* • *Supporto alle autorità di vigilanza del mercato/autorità di notifica/organismi di accreditamento nazionali per implementare il CRA.* • *Efficace cooperazione operativa delle organizzazioni incaricate della sicurezza informatica a livello nazionale dell'UE o degli Stati membri, in particolare la cooperazione dei CSIRT (anche in relazione alla rete CSIRT) o la cooperazione degli operatori di servizi essenziali, comprese le autorità pubbliche.* • *Migliori processi e mezzi di sicurezza e notifica per le entità essenziali e importanti nell'UE, compresi i sistemi di notifica degli incidenti transfrontalieri (automatizzati).* • *Migliore segnalazione degli attacchi informatici alle autorità di contrasto in linea con la direttiva sugli attacchi contro i sistemi di informazione.* • *Maggiore sicurezza dei sistemi di rete e di informazione nell'UE.* • *Maggiore allineamento delle implementazioni NIS2 degli Stati membri (direttiva (UE) 2022/2555).* • *Supporto alla certificazione della sicurezza informatica in linea con la legge sulla sicurezza informatica modificata*.
Requisiti:	***Le candidature saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione dell'argomento per il quale sono state presentate.*** ***Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:*** *− Essere persone giuridiche (enti pubblici o privati)* *− Essere stabiliti in uno dei paesi ammissibili, vale a dire:* *−Stati membri dell'UE (inclusi i paesi e territori d'oltremare (PTOM))* *− Paesi SEE (Norvegia, Islanda, Liechtenstein)*

	Si prega di notare che tutti gli argomenti di questo bando sono soggetti a restrizioni dovute alla sicurezza; pertanto, le entità non devono essere direttamente o indirettamente controllate da un paese che non sia un paese ammissibile. *− la partecipazione a qualsiasi titolo (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità stabilite e controllate da paesi ammissibili* *− le attività del progetto (incluso il lavoro subappaltato) devono svolgersi in paesi ammissibili* *− il Contratto di sovvenzione può prevedere restrizioni IPR. Infine, per gli argomenti* **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC** e **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT** *le sovvenzioni saranno assegnate solo ai candidati che hanno superato la valutazione dell'azione di appalto congiunto.* *Per l'argomento* **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC** *- SOC nazionali: solo le entità designate a livello di Stato membro come SOC nazionali possono presentare domanda di finanziamento e il progetto deve essere mono-beneficiario.* *Per l'argomento* **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT** *i consorzi devono essere composti da beneficiari di almeno 3 paesi ammissibili in caso di nuovi SOC transfrontalieri. In caso di ampliamento di una sovvenzione transfrontaliera in corso, il nuovo consorzio deve essere composto dal coordinatore della sovvenzione in corso più le nuove entità che desiderano unirsi al consorzio ospitante del SOC.* **Per tutti gli altri argomenti***: nessuna restrizione* **DURATA:** *36 mesi (Durate differenti non sono escluse).* **Tipo di finanziamento per progetto:** • **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs:** **Simple Grant—** *tasso di finanziamento del 50%*

	• **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT– Enlarging existing or Launching New Cross-Border SOC Platforms:** **Simple Grants —** *tasso di finanziamento del 50%* • **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS– Strengthening the SOC Ecosystem:** **Coordination and Support Actions-** *tasso di finanziamento del 100 %* • **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH- Development and Deployment of Advanced Key Technologies** **SME Support Actions —** *tasso di finanziamento del 50% e 75% per le PMI* • **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER- Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations** **Grants for Financial Support —** *tasso di finanziamento del 100%* • **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)** **Simple Grants —** *tasso di finanziamento del 50%*
Soggetti responsabili/ammessi:	**Università:** **☒ Sì** **☐ No**

	Altri soggetti responsabili/ ammessi: Enti pubblici o privati stabiliti in uno degli stati Membri
Link:	**TESTO DEL BANDO** **BANDO**
Scadenza domanda:	27/03/2025 ore 17:00
Finanziamento (Max/Min/Co-fin):	**Budget complessivo:** 102.800.000 € **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs** **Budget:** 5.800.000 € **DIGITAL-ECCC-2024-DEPLOY- CYBER-07-SOCSYS -Strengthening the SOC Ecosystem** **Budget:** 2.000.000 € **DIGITAL-ECCC-2024-DEPLOY- CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies** **Budget:** 35.000.000 € **DIGITAL-ECCC-2024-DEPLOY- CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations** **Budget:** 35.000.000 € **DIGITAL-ECCC-2024-DEPLOY- CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies(2024)** **Budget:** 20.000.000 €
VALUTAZIONE AD OPERA DELL'UFFICIO RICERCA	
Costi ammissibili:	Categorie di budget per questo bando: **– A. Costi del personale** • A.1 Dipendenti, • A.2 Persone fisiche con contratto diretto, • A.3 Persone distaccate • A.4 Proprietari di PMI e beneficiari persone fisiche **– B. Costi di subappalto**

	– C. Costi di acquisto • *C.1 Travel and subsistence* • *C.2 Equipment* • *C.3 Other goods, works and services* **-D. Altre categorie di costi** • *D.1 Supporto finanziario a terzi (per argomento DIGITAL-ECCC-2024-DEPLOYCYBER-07-LARGEOPER)* • *D.2 Beni e servizi fatturati internamente* **– E. Costi indiretti** **Condizioni specifiche di ammissibilità dei costi per questo bando:** – **costi del personale:** ○ **costi medi del personale** (costo unitario secondo le consuete pratiche di contabilità dei costi): **Sì** ○ **costo unitario del proprietario/persona fisica della PMI**: **Sì** – **costi unitari di viaggio e soggiorno**: **No (**solo costi effettivi**)** – **costi delle attrezzature:** ○ *ammortamento (per l'argomento DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS e DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02)* ○ *ammortamento + costo totale per le attrezzature elencate (per gli argomenti DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC, DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT, DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH, DIGITAL-ECCC-2024-DEPLOYCYBER-07-LARGEOPER)* – **altre categorie di costi:** – **costi per il supporto finanziario a terzi: obbligatorio per le sovvenzioni:** ○ per l'argomento DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER: importo massimo per terza parte 60.000 EUR, a meno che non sia richiesto un importo superiore perché l'obiettivo dell'azione sarebbe altrimenti

	impossibile o eccessivamente difficile da raggiungere e ciò è debitamente giustificato nel modulo di domanda. ▪ In questo caso, i destinatari del supporto finanziario a terzi devono cofinanziare l'attività per almeno il 50% dei costi totali dell'attività. ▪ Un minimo del 50% della sovvenzione deve essere riservato al sostegno finanziario a terzi. La Commissione stima che il 70% della sovvenzione per il sostegno finanziario a terzi consentirebbe di affrontare l'argomento in modo appropriato. − beni e servizi fatturati internamente (costo unitario secondo le consuete pratiche di contabilità dei costi): **Sì**
Note e considerazioni:	

Livello di interesse: ☒ **Alto** ☐ **Medio** ☐ **Basso**	**Infografica:** ☐ **Sì** ☐ **No** ☐ **In attesa**