# Sviluppo delle capacità dei centri operativi di sicurezza (SOC).

## Capacity building of Security Operation Centres (SOCs)

**TOPIC ID:** DIGITAL-ECCC-2022-CYBER-03-SOC
**Ente finanziatore:** Commissione europea, Digital Europe Programme (DIGITAL)

**Obiettivi ed impatto attesi:** L'obiettivo sarà quello di creare, sostenere e/o rafforzare e interconnettere le capacità di rilevamento delle minacce informatiche, consentendo il rafforzamento delle capacità di monitoraggio e rilevamento delle minacce informatiche, la creazione di conoscenze collettive e la condivisione delle migliori pratiche.
Inoltre, i dati e le capacità relative all'intelligence sulle minacce alla sicurezza informatica saranno riuniti da più fonti (come i CSIRT e altri attori rilevanti della sicurezza informatica) attraverso piattaforme transfrontaliere in tutta l'UE. L'uso dell'IA all'avanguardia, delle capacità di apprendimento automatico e delle infrastrutture comuni consentirà di condividere e correlare in modo più efficiente e rapido i segnali rilevati e di creare informazioni sulle minacce di alta qualità per le autorità nazionali e le altre parti interessate, consentendo così una conoscenza completa della situazione e una reazione più rapida.

L'obiettivo è migliorare la resilienza della cybersecurity con un rilevamento e una risposta più rapidi agli incidenti e alle minacce di cybersecurity a livello nazionale e dell'UE attraverso la creazione di capacità di rilevamento e analisi delle minacce informatiche, lo sfruttamento di tecnologie dirompenti e la condivisione di informazioni che portino a una maggiore consapevolezza della situazione e a catene di approvvigionamento dell'UE più forti.

In particolare, i consorzi dovrebbero concentrarsi su almeno uno dei seguenti aspetti:
- sostenere gli enti che si occupano di rilevamento e analisi delle minacce informatiche al servizio di organizzazioni private (in particolare le PMI) e/o pubbliche con il monitoraggio e l'analisi in tempo reale dei dati provenienti dal traffico della rete Internet pubblica per individuare attività e incidenti dannosi che compromettono la resilienza dei sistemi di rete e di informazione.
- Rafforzare tali entità sfruttando lo stato dell'arte dell'intelligenza artificiale (comprese le tecniche di apprendimento automatico) e la potenza di calcolo per migliorare l'individuazione di attività dannose e apprendere in modo dinamico l'evoluzione del panorama delle minacce.
- Sostenere la condivisione delle informazioni tra gli enti che si occupano dell'individuazione e dell'analisi delle minacce informatiche o le autorità pubbliche (comprese le autorità competenti e i CSIRT ai sensi della direttiva NIS) o altri soggetti pubblici o privati che trattano informazioni rilevanti sulle minacce, agevolata da opportuni accordi di condivisione, nel rispetto di tutti gli obblighi relativi alla privacy e alla protezione dei dati personali.

- Sviluppare e distribuire strumenti, piattaforme e infrastrutture adeguate per condividere e analizzare in modo sicuro grandi insiemi di dati tra gli enti che si occupano di rilevamento e analisi delle minacce informatiche. Ove possibile e opportuno, saranno riutilizzati gli elementi costitutivi

esistenti, compresi i risultati dei progetti Connecting Europe Facility e Horizon 2020.
- Sostenere una maggiore disponibilità, qualità, utilizzabilità e interoperabilità dei dati di intelligence sulle minacce tra gli enti interessati.
- Identificare le potenziali dipendenze critiche da fornitori e soluzioni straniere per l'intelligence sulle minacce e sviluppare una catena di approvvigionamento dell'UE per l'intelligence sulle minacce.
- Fornire agli organismi degli Stati membri capacità di intelligence sulle minacce e di consapevolezza situazionale che aiutino ad anticipare e a rispondere agli attacchi informatici, in particolare nel quadro del Blueprint/CyCLONe e dell'Unità congiunta di cibersicurezza;
- Creare un ponte di cooperazione tra le varie comunità di cibersicurezza, ad esempio la resilienza civile della cibersicurezza, le forze dell'ordine, la difesa, tenendo conto dei quadri di cooperazione come il Blueprint/CyCLONe.
Se da un lato queste azioni consentiranno lo sviluppo di capacità, ad esempio attraverso la creazione o il rafforzamento di entità che si occupano di rilevamento e analisi delle minacce informatiche al servizio di organizzazioni private o pubbliche, sfruttando tecnologie all'avanguardia come l'intelligenza artificiale e l'apprendimento dinamico del panorama delle minacce, dall'altro saranno abbinate a un invito a manifestare interesse per selezionare entità negli Stati membri che forniscano le strutture necessarie per ospitare e gestire piattaforme transfrontaliere per la messa in comune di dati sulle minacce alla sicurezza informatica tra diversi Stati membri (dati potenzialmente provenienti da varie fonti).

Verrà lanciato un appalto congiunto per sviluppare e gestire le capacità delle piattaforme transfrontaliere selezionate.

Risultati e risultati
- Capacità di rilevamento delle minacce informatiche di livello mondiale in tutta l'Unione, rafforzate con tecnologie all'avanguardia in settori quali l'intelligenza artificiale.
- Condivisione delle informazioni sulle minacce tra gli enti che si occupano di rilevamento e analisi delle minacce informatiche.
- Capacità di intelligence delle minacce e di consapevolezza situazionale a sostegno di una collaborazione rafforzata nel quadro del Blueprint/CyCLONe, nonché con le forze dell'ordine e la difesa.
- Le azioni possono anche contribuire alla creazione di una piattaforma transfrontaliera per la condivisione dei dati sulle minacce alla sicurezza informatica tra diversi Stati membri, dotata di infrastrutture altamente sicure e di strumenti avanzati di analisi dei dati.

**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 a soggetti provenienti da Paesi ammissibili
- le attività del progetto (incluso il lavoro in subappalto) devono svolgersi in Paesi ammissibili (si veda la sezione localizzazione geografica qui sotto e la sezione 10)
- l'Accordo di sovvenzione può prevedere restrizioni sui DPI

**Contributo finanziario:** Tipo di azione e tasso di finanziamento
Sovvenzioni semplici - Tasso di finanziamento del 50%.

Bilancio tematico : 75.000.000 EUR
I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno stabiliti nella Convenzione di sovvenzione
Budget del progetto (importo massimo della sovvenzione) per il tema: tra 1 e 10 milioni di euro per progetto.

**Scadenza:** 24 gennaio 2023 17:00:00 ora di Bruxelles

**Ulteriori informazioni:**
**call-fiche_digital-eccc-2022-cyber-03_en.pdf (europa.eu)**