Sviluppo delle capacità dei Centri operativi di sicurezza (SOC)
Capacity building of Security Operation Centres (SOCs)

TOPIC ID: DIGITAL-ECCC-2022-CYBER-B-03-SOC

Ente finanziatore: Commissione europea, Programma Digital Europe

Obiettivi ed impatto attesi: L'obiettivo sarà quello di creare, sostenere e/o rafforzare e interconnettere i SOC a livello regionale, nazionale ed europeo. Ciò consentirà di rafforzare le 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 alle informazioni 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 di AI all'avanguardia, di capacità di apprendimento automatico e di 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 inoltre di 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 l'istituzione di SOC, 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:

- Sostenere i SOC esistenti o istituire SOC nazionali, regionali o settoriali al servizio di organizzazioni private (in particolare 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 della rete e dei sistemi informativi;
- Rafforzare i SOC sfruttando lo stato dell'arte dell'intelligenza artificiale (comprese le tecniche di apprendimento automatico) e la potenza di calcolo per migliorare il rilevamento delle attività dannose e apprendere in modo dinamico l'evoluzione del panorama delle minacce;
- Sostenere la condivisione delle informazioni tra le autorità pubbliche (comprese le autorità competenti e i CSIRT ai sensi della direttiva NIS), nonché con altri SOC (ad esempio gestiti da enti privati), facilitata 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 i SOC. 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 i SOC e gli enti interessati;

- Identificare le potenziali dipendenze critiche da fornitori e soluzioni estere nel settore dell'intelligence sulle minacce e sviluppare una catena di approvvigionamento dell'UE in materia di 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 cybersecurity, ad esempio la resilienza della cybersecurity civile, le forze dell'ordine, la difesa, tenendo conto di quadri di cooperazione come il Blueprint/CyCLONe e l'Unità congiunta di cybersecurity.

Per raggiungere questo obiettivo, sono previste le seguenti attività:

- Saranno messe a disposizione sovvenzioni per consentire lo sviluppo di capacità, ad esempio attraverso la creazione o il rafforzamento di SOC al servizio di organizzazioni private o pubbliche, sfruttando tecnologie all'avanguardia come l'intelligenza artificiale e l'apprendimento dinamico del panorama delle minacce.
- Sarà lanciato un invito a manifestare interesse per selezionare entità negli Stati membri che forniscano le strutture necessarie per ospitare e gestire piattaforme transfrontaliere per mettere in comune i dati sulle minacce alla sicurezza informatica tra diversi Stati membri (dati potenzialmente provenienti da varie fonti). L'invito a manifestare interesse servirà anche a sviluppare la pianificazione e la progettazione degli strumenti e delle infrastrutture necessarie.
- Sulla base dell'invito a manifestare interesse, sarà lanciato un appalto congiunto per sviluppare e gestire le capacità delle piattaforme transfrontaliere selezionate, compresi strumenti e infrastrutture avanzati per condividere e analizzare in modo sicuro grandi insiemi di dati e informazioni sulle minacce tra le piattaforme transfrontaliere selezionate (ad esempio, infrastrutture altamente sicure o analisi dei dati avanzate volte a migliorare significativamente la capacità di analizzare grandi insiemi di 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 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
I soggetti interessati sono attori pubblici e privati, nonché consorzi di entrambi i tipi o che li combinano, che possono supportare il rilevamento delle minacce informatiche e la condivisione delle CTI.

Contributo finanziario: IL budget totale della call è di EURO 26.310.858,19

Tipo di azione e tasso di finanziamento:
Simple Grants - tasso di finanziamento del 50%
Budget del progetto (importo massimo della sovvenzione): tra 1 milione di euro e 10 milioni di euro 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)