Cibercriminalità e indagini digitali
Cybercrime and Digital investigations

TOPIC ID: ISF-2022-TF1-AG-CYBER

Ente finanziatore: Commissione europea, Programma Internal Security Fund (ISF)

Obiettivi ed impatto attesi: Le domande di progetto presentate nell'ambito del presente invito a presentare proposte devono riguardare almeno una, ma idealmente più, delle seguenti priorità nel settore della criminalità informatica11 e delle indagini digitali:
1. 1. Sviluppare la capacità operativa e le competenze delle autorità di contrasto e giudiziarie e sostenere la cooperazione transfrontaliera nel settore della criminalità informatica, compresa la sicurezza informatica, se correlata;
2. Sviluppo di strumenti investigativi e forensi per affrontare le sfide poste dall'uso della crittografia da parte dei criminali e il suo impatto sulle indagini penali e sostenere l'impegno delle autorità di contrasto nel settore della governance di Internet;
3. Contribuire all'attuazione del diritto dell'UE, tenendo conto in particolare delle valutazioni disponibili:
- Per la direttiva 2013/40/UE, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione, cfr. in particolare la relazione che valuta in che misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio,
- Per la direttiva (UE) 2019/713, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, cfr. in particolare la valutazione d'impatto che accompagna la proposta della Commissione;
4. Favorire la cooperazione transfrontaliera tra autorità di contrasto/giudiziarie e soggetti privati. Ciò comprende, ad esempio, l'istituzione di meccanismi a sostegno della cooperazione pubblico-privato e di meccanismi per migliorare la segnalazione dei reati alle autorità di contrasto. Le proposte che corrispondono più da vicino a queste priorità saranno valutate come particolarmente rilevanti. I candidati sono quindi invitati a considerare molto attentamente i collegamenti tra la loro proposta e le priorità dell'invito.
Le proposte dovrebbero avere come obiettivo i seguenti aspetti s
- Migliorare la capacità operativa delle autorità di contrasto e/o giudiziarie di indagare sugli attacchi informatici e sulla criminalità informatica, ad esempio attraverso tecniche e strumenti investigativi (anche per la digital forensics) con particolare attenzione alle principali priorità delle minacce (escluso il materiale online relativo agli abusi sessuali sui minori, che è coperto da specifici inviti a presentare proposte), come presentato nella Internet Organised Crime Threat Assessment 2021.
Le aree che sono state identificate dagli Stati membri dell'UE come bisognose di particolare attenzione comprendono digital forensics (mobile forensics, computer forensics, network forensics, IoT forensics, inclusa la vehicle forensics), analisi dei dati visivi, analisi del malware e capacità

di reverse engineering, analisi e sequestro delle criptovalute, stoccaggio, elaborazione, analisi e trasferimento efficiente dei big data, comprensione e sfruttamento delle "informazioni sulle minacce" e dei metadati, monitoraggio e indagini Darkweb, OSINT
- Rafforzare la capacità operativa delle autorità di contrasto e/o giudiziarie di affrontare le sfide poste dal 5G e dalla comunicazione a livello di applicazione nel settore dell'intercettazione legale, con particolare attenzione alle attività di standardizzazione pertinenti.
- Rafforzare la capacità operativa delle autorità di contrasto e/o giudiziarie di affrontare le sfide poste dall'uso della cifratura da parte dei criminali e il suo impatto sulle indagini penali, ad esempio sostenendo la creazione, l'estensione e lo sviluppo di punti di competenza e la loro messa in rete a livello di UE o sostenendo lo sviluppo di un insieme di strumenti di tecniche investigative alternative per ottenere le informazioni necessarie cifrate dai criminali (ad esclusione delle misure che potrebbero indebolire la cifratura in generale o potrebbero avere un impatto su un numero maggiore o indiscriminato di persone)
- Migliorare la capacità operativa delle autorità di contrasto e/o giudiziarie di cooperare oltre frontiera, ad esempio, sostenendo la raccolta e la fornitura di prove digitali, sostenendo il distacco di funzionari, migliorando l'efficienza dei punti di contatto 24/7 (permanenti) per l'applicazione della legge in materia di criminalità informatica, creando piattaforme dedicate
- Migliorare la cooperazione tra enti e/o autorità private nel settore della sicurezza informatica e le autorità di polizia e/o giudiziarie, adottando misure correttive, anche attraverso la creazione di adeguati sistemi di scambio di informazioni (o interfacce per utilizzare meglio i sistemi esistenti)
- Aumentare e migliorare la segnalazione della criminalità informatica alle autorità di polizia
- Fornire alle autorità pubbliche un quadro accurato della reale (cioè inclusa la portata non denunciata) portata dei reati informatici. Cioè anche di quelli non denunciati) della portata della criminalità informatica. Le proposte che si concentrano su: - esclusivamente l'aumento del livello generale di consapevolezza sulla criminalità informatica e le indagini digitali, ad esempio quando sono rivolte al grande pubblico, - la ricerca senza chiari collegamenti con i risultati operativi, - il materiale sugli abusi sessuali sui minori (CSAM), sono coperti da altri programmi di finanziamento dell'UE o da altri inviti a presentare proposte e quindi non sono considerati pertinenti per il finanziamento nell'ambito del presente invito.

Criteri di eleggibilità: Le proposte devono essere presentate da un consorzio di almeno 3 entità indipendenti (beneficiari; non entità affiliate) di 3 diversi paesi ammissibili
Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:
• essere persone giuridiche (enti pubblici o privati)
• essere stabiliti in uno dei paesi ammissibili,
Per "soggetto giuridico" si intende qualsiasi persona fisica o giuridica creata e riconosciuta come tale ai sensi del diritto nazionale, del diritto dell'UE o del diritto internazionale, dotata di personalità giuridica e che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi, oppure un soggetto senza personalità giuridica . I beneficiari e gli enti affiliati devono registrarsi

nel Registro dei Partecipanti prima di presentare la loro domanda, al fine di ottenere un codice di identificazione del partecipante (PIC) ed essere convalidati dal Servizio Centrale di Convalida (REA Validation) prima di firmare la convenzione di sovvenzione. Per la convalida, sarà chiesto loro di caricare i documenti necessari che dimostrano il loro status giuridico e la loro origine
Composizione del consorzio
Le proposte devono essere presentate da:
- minimo 2 candidati (beneficiari; non enti affiliati) da 2 diversi paesi ammissibili.
Si noti che il paese di stabilimento di un'organizzazione internazionale partecipante non contribuisce a soddisfare il requisito minimo di composizione del Consorzio.
- Le seguenti entità NON possono candidarsi come coordinatori:
- enti a scopo di lucro, - organizzazioni internazionali29 , indipendentemente dal loro paese di stabilimento
- enti stabiliti in paesi non UE

Schema di finanziamento: Il budget disponibile per l'invito è di 8 000 000 EUR.
Budget del progetto
I bilanci dei progetti (importo massimo della sovvenzione) devono essere compresi tra 500 000 EUR e 3 000 000 EUR.
I costi saranno rimborsati al tasso di finanziamento fissato nell'accordo di sovvenzione (90%)

Scadenza: 15 settembre 2022 17:00:00 ora di Bruxelles

Ulteriori informazioni: **call-fiche_isf-2022-tf1-ag-cyber_en.pdf (europa.eu)**