# Cybersecurity e sistemi per una maggiore resilienza

## Cybersecurity and systems for improved resilience

**TOPIC ID:** LIFE-2022-STRAT-NAT-SNAP-two-stage

**Ente finanziatore:** Commissione europea, EDF European Defence Fund

**Obiettivi ed impatto attesi:** Le operazioni militari cinetiche e digitali fanno sempre più affidamento su computer e comunicazioni in rete per la raccolta di informazioni, l'intelligence, il coordinamento e il controllo delle armi. Contemporaneamente alla rapida crescita della dipendenza dalle tecnologie digitali, aumentano anche le potenziali minacce e vulnerabilità. La comunità globale, le forze armate e il campo di battaglia possono essere colpiti da minacce crescenti. Inoltre, l'Internet degli oggetti (IoT) si è ampiamente integrato in una varietà di settori e industrie, offrendo soluzioni "pronte all'uso" per la sorveglianza, il monitoraggio, la sanità e le piattaforme militari. Esempi di dispositivi IoT sono i droni, le radio definite dal software, i sensori (telecamere, umidità, temperatura), i dispositivi TV, le automobili/veicoli). Molte soluzioni IoT sono progettate principalmente per la funzionalità, senza essere adeguatamente protette. Di conseguenza, gli attacchi agli ambienti IoT hanno guadagnato slancio a causa della maggiore superficie di attacco. Pertanto, è necessario affrontare la necessità di servizi di cybersecurity che garantiscano un livello adeguato di controllo e prevenzione (ad esempio, su dati, comunicazioni e sistemi).

Obiettivo specifico

Attualmente sono in uso o in fase di sviluppo o di ricerca molte soluzioni di cybersecurity. Tuttavia, le minacce informatiche continuano ad evolversi, colpendo i sistemi e i servizi su cui la comunità odierna fa affidamento.

Un ambiente di test è indispensabile per determinare come migliorare la sicurezza di un sistema, di un prodotto o di un componente, attraverso la generazione di test efficaci per analizzare il sistema in questione, la sua capacità di risposta alle minacce, con conseguente divulgazione forense, procedure e proposte di architetture migliorate.

La maggior parte dei sistemi militari specializzati legacy non è direttamente vulnerabile agli attacchi informatici e alle minacce informatiche impiegate nell'Internet aperto, tuttavia il crescente uso di componenti ICT/IoT Commercial Off The Shelf (COTS) e l'aumento della connettività possono aumentare la probabilità di attacchi mirati che utilizzano i metodi, se non gli strumenti, impiegati negli attacchi informatici nell'Internet aperto.

Il crescente utilizzo del dominio cibernetico richiederà alle forze di difesa di operare in scenari

inaspettati e di conseguenza ai sistemi di funzionare al di fuori degli ambienti per cui sono stati progettati.

È quindi essenziale comprendere l'entità della minaccia, sviluppare un'infrastruttura per valutare continuamente la sicurezza rispetto a un panorama di minacce in evoluzione, costruire la resilienza garantendo la sicurezza della missione anche in caso di compromissione parziale, utilizzando hardware, applicazioni software, protocolli di comunicazione e sistemi operativi affidabili.

Ambito di applicazione

Le proposte devono preparare, progettare e/o dimostrare un laboratorio di test cyberfisico con strumenti hardware e software a supporto delle competenze, incentrato sulla generazione di test efficaci per sistemi, prodotti e componenti cyberfisici comuni e rilevanti con dati realistici provenienti da un caso d'uso pertinente.

Deve fornire capacità di analisi della cybersecurity dell'architettura di sistema reale e pianificata, compresa un'analisi dimostrata delle minacce di un sistema o di un componente selezionato. Sulla base di questa analisi, l'architettura può essere aggiornata per aumentare la sicurezza del sistema a un livello adeguato.

Possono essere inclusi strumenti integrati per test di validazione informatica automatizzati ed efficienti dal punto di vista dei costi, basati sui requisiti indicati dagli standard internazionali. Gli strumenti devono essere in grado di emulare il sistema da testare, memorizzare le configurazioni dettagliate, condurre test automatizzati e la convalida dell'architettura militare, memorizzare i risultati ed essere in grado di ripetere i test periodicamente in modo economicamente efficiente, considerando la riconfigurazione e l'estensione del sistema durante il ciclo di vita e il panorama aggiornato delle minacce.

Le proposte dovrebbero contribuire a migliorare la sicurezza informatica degli Stati membri e della Norvegia, con soluzioni e servizi per le infrastrutture digitali critiche di sicurezza, crittografia e sistemi di comunicazione, dal livello strategico a quello tattico.

La proposta deve sostenere lo sviluppo del prodotto finale.

**Criteri di eleggibilità:** Qualsiasi soggetto giuridico, indipendentemente dal suo luogo di stabilimento, compresi i soggetti giuridici di paesi terzi non associati o le organizzazioni internazionali (comprese le organizzazioni internazionali di ricerca europee) può partecipare (indipendentemente dal fatto che sia ammissibile o meno al finanziamento), purché siano soddisfatte le condizioni stabilite nel regolamento del programma, insieme a qualsiasi altra condizione stabilita nello specifico argomento dell'invito. 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 durante la fase di preparazione della sovvenzione.

Composizione del consorzio
Le proposte devono essere presentate da almeno 3 candidati indipendenti (beneficiari; non entità affiliate) provenienti da 3 diversi Paesi ammissibili.

Durata del progetto: tra 12 e 48 mesi Progetti di durata superiore possono essere accettati in casi debitamente giustificati. Sono possibili proroghe, se debitamente giustificate e attraverso un emendamento.

Sicurezza
I progetti che coinvolgono informazioni classificate 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). I progetti in cui gli Stati membri dei beneficiari partecipanti e degli enti affiliati decidono di istituire un quadro di sicurezza specifico ai sensi dell'articolo 27, paragrafo 4, del regolamento FES, saranno soggetti a tale quadro di sicurezza specifico e le informazioni classificate preliminari (risultati) generate dal progetto saranno sotto la responsabilità di tali Stati membri. Se non viene istituito un quadro di sicurezza specifico entro la firma della convenzione di sovvenzione, le norme di sicurezza saranno disciplinate dalla decisione 2015/44488 della Commissione e dalle relative norme di attuazione.

**Contributo finanziario:** I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno stabiliti nella Convenzione di sovvenzione (Scheda tecnica, punto 3 e art. 5). Budget del progetto (importo massimo della sovvenzione): si veda la sezione 6 di cui sopra. La sovvenzione sarà una sovvenzione mista a costi effettivi basata sul bilancio (costi effettivi, con costi unitari ed elementi forfettari). Ciò significa che rimborserà SOLO alcuni tipi di costi (costi ammissibili) e i costi effettivamente sostenuti per il progetto (NON i costi preventivati). Per quanto riguarda i costi unitari e gli elementi forfettari, è possibile addebitare gli importi calcolati come spiegato nella Convenzione di sovvenzione. I costi saranno rimborsati in base al tasso di finanziamento stabilito nella Convenzione di sovvenzione. Questo tasso dipende dal tipo di attività e dai partecipanti . In linea di principio, le sovvenzioni NON possono produrre un profitto (ossia un'eccedenza delle entrate + sovvenzione UE rispetto ai costi). Nel caso in cui la regola dell'assenza di profitto sia attivata nella Convenzione di sovvenzione, le organizzazioni

a scopo di lucro devono dichiarare le loro entrate e, se c'è un profitto, lo dedurremo dall'importo finale della sovvenzione.

**Scadenza:** 24 November 2022 17:00:00 Brussels time

**Ulteriori informazioni:**
**call-fiche_edf-2022-da_en.pdf (europa.eu)**