Adattare la consapevolezza della situazione cibernetica agli ambienti informatici in evoluzione

Adapting cyber situational awareness for evolving computing environments

TOPIC ID: EDF-2022-RA-CYBER-CSACE

Ente finanziatore: Commissione europea, EDF European Defence Fund

Obiettivi ed impatto attesi: Un numero crescente di azioni dannose che prendono di mira sistemi governativi e strategici avviene nel cyber-spazio. Per contrastare queste minacce sono essenziali soluzioni, tecnologie e applicazioni nuove o migliorate per una maggiore consapevolezza della situazione cibernetica (CSA). Per affrontare attività in evoluzione e più complicate nel cyberspazio, comprese le sfide che sorgono a causa della continua evoluzione delle reti e dei sistemi del campo di battaglia, i decisori e gli operatori del Centro operativo di sicurezza (SOC) hanno bisogno di una CSA più aggiornata relativa alle minacce informatiche, in tempo reale, raccogliendo informazioni informatiche interne ed esterne. La CSA indica la capacità di un decisore di sapere cosa sta accadendo nel dominio cibernetico per poter prendere decisioni informate e rispondere adeguatamente agli incidenti.

Obiettivo specifico

La CSA deve essere supportata dalla tecnologia per raccogliere, correlare e fondere le diverse fonti di dati e la loro diversa natura (ad esempio, rete, missione, open-source intelligence, consapevolezza delle minacce strutturate e non strutturate) per fornire le informazioni necessarie affinché i decisori umani possano assimilare la situazione. Le minacce informatiche continuano a crescere in complessità e portata, con minacce nuove e in evoluzione derivanti dall'avanzamento delle campagne e delle tattiche avversarie e, allo stesso tempo, il volume e la diversità delle informazioni sulle minacce informatiche aumentano costantemente. Per gli operatori umani è una sfida visualizzare e comprendere la varietà e il volume di informazioni prodotte da reti e sistemi dinamici e frammentati in un contesto di campo di battaglia. L'evoluzione delle sfide informatiche richiederà migliori capacità di consapevolezza della missione attraverso la Cyber Threat Intelligence (CTI) che stabilisce interfacce con le fonti di informazione considerate rilevanti per le fasi di pianificazione e condotta di un'operazione, al fine di fornire informazioni in tempo reale sulla missione al corretto livello di granularità del quadro operativo comune (COP).

Ambito di applicazione

L'obiettivo generale è quello di esplorare nuovi concetti e opportunità operative per fornire al comandante informazioni essenziali sull'avversario, le sue capacità e i suoi obiettivi mentre opera nel e attraverso il cyberspazio. Il CTI, potenziato con un modulo di arricchimento semantico delle

minacce in grado di analizzare i dati provenienti da archivi pubblici e dal dark web per generare Indicatori di compromissione (IoC) e Indicatori di attacco (IoA), supporterà le operazioni nel cyberspazio.

Si prevede che le proposte sviluppino soluzioni innovative facendo leva sulla difesa informatica a tutto spettro (fisica, logica, cyber persona) in una prospettiva incentrata sull'avversario. Le proposte devono puntare alla tecnologia di supporto alla CSA, con l'obiettivo di fornire gli elementi tecnici informativi necessari per elaborare le vaste quantità di informazioni al fine di produrre dalla tattica alla COP, nonché altri artefatti tecnici da utilizzare dai decisori che necessitano di CSA. Ciò include la creazione di grafici come linee temporali, istogrammi o grafici di relazione, cruscotti personalizzati e rapporti in base alle responsabilità di ciascun utente. Particolare attenzione dovrà essere prestata all'interoperabilità e alla collaborazione con le soluzioni esistenti a livello di Security Operations Centre (SOC), Network Operations Centre (NOC) e Computer Emergency Response Team (CERT), evitando la duplicazione degli sforzi.

Le proposte devono riguardare tecnologie all'avanguardia. I sistemi di gestione e visualizzazione delle informazioni di consapevolezza situazionale dovrebbero essere in grado di presentare una visione globale dell'ambiente del campo di battaglia attraverso i COP tramite moduli esportabili di informazioni logiche per essere interoperabili con altri quadri operativi a terra, in mare, in aria o nello spazio, tenendo conto dell'evoluzione in corso dei sistemi militari C2 verso lo scenario dell'Internet delle cose militari (IOMT) che pone una complessità aggiuntiva, e di sostenere contro un attacco massiccio al sistema critico del campo di battaglia.

Requisiti funzionali

Le proposte devono soddisfare i seguenti requisiti funzionali:

- Definizione di una serie di scenari d'uso per testare il concetto.
- Sviluppo di implementazioni di prova per verificare il funzionamento.
- Progettazione di un ambiente di simulazione basato sul cyber-range per generare serie di dati rappresentativi per convalidare i modelli di intelligenza artificiale e fornire un banco di prova per valutare il concetto generale.

Impatto previsto:

- una migliore comprensione del modo in cui la CTI, insieme alla tecnologia futura, sarà in grado di supportare la creazione e la conservazione di un alto livello di CSA da parte dell'analista.
- Miglioramento delle metafore di visualizzazione e dei processi di gestione delle informazioni derivanti dagli scenari IOMT.
- Miglioramento della gestione della CSA attraverso le capacità di simulazione fornite dai gemelli digitali.

- Miglioramento della consapevolezza della missione per le infrastrutture di missione supportate dall'IOMT.
- Maggiore condivisione di CTI grazie all'uso dell'apprendimento federato per evitare perdite o la necessità di condividere informazioni sensibili.
- Migliore comprensione dell'uso del rilevamento distribuito delle anomalie sia nelle singole organizzazioni che nell'efficacia delle intrusioni collaborative per migliorare il rilevamento degli attacchi.

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)