Agente AI autonomo distribuibile
Deployable Autonomous AI Agent

TOPIC ID: EDF-2023-DA-CYBER-DAAI

Ente finanziatore: Commissione europea, FONDO EUROPEO PER LA DIFESA

Obiettivi ed impatto attesi: L'intelligenza artificiale (AI) inizia a trasformare la sicurezza informatica. I recenti progressi nelle tecniche di apprendimento automatico (ML) potrebbero consentire in futuro capacità rivoluzionarie, tra cui difese che intercettano automaticamente gli aggressori e rimodellano le reti per attenuare le operazioni offensive. L'intelligenza artificiale, combinata con l'IA, potrebbe modellare le operazioni informatiche in modo tale da favorire impegni più aggressivi e destabilizzanti tra gli attori statali. È quindi importante prevedere come gli avversari potrebbero adattare le loro tattiche e strategie e determinare quali sfide potrebbero emergere per i difensori.
Il campo dell'IA si trova a un bivio critico. La globalizzazione e l'industrializzazione dell'IA si stanno intensificando, mentre si moltiplicano le questioni etiche e normative di queste tecnologie. L'IA è passata da una tecnologia emergente a una tecnologia matura, che non si occupa più di una parte speculativa della ricerca scientifica, ma di qualcosa che ha un impatto sul mondo reale, sia positivo che negativo. L'importanza dell'IA nelle operazioni informatiche è stata notata da molte nazioni. L'IA è una tecnologia strategica che potrebbe rivelarsi incredibilmente importante per la competitività dell'UE, dei suoi Stati membri e dei Paesi associati al FES (Norvegia).

Obiettivo specifico

Le conversazioni odierne sull'IA negli affari militari si concentrano su diverse varianti di intelligenza artificiale "stretta". Le attuali discussioni sull'IA spesso si concentrano principalmente sul ML, che è il processo di utilizzo di algoritmi per imparare dai dati. Gran parte dei progressi più interessanti degli ultimi anni hanno fatto leva sul deep learning, una tecnica che prevede l'uso di strati di reti neurali artificiali, ispirate alla struttura del cervello umano.

A livello di base, l'IA comporta un software che sfrutta i dati per l'apprendimento, ma richiede anche un hardware che sfrutti la potenza di capacità di calcolo significative per consentire questo processo. È intrinsecamente difficile definire cosa sia o possa essere l'IA quando il campo è così dinamico e si evolve così rapidamente. Per il momento, le tecniche di IA/ML sono spesso limitate dalla disponibilità di dati, anche se la situazione potrebbe cambiare con i progressi nell'uso di dati sintetici, esercitazioni cibernetiche reali, data lake e tecniche che sfruttano l'apprendimento per rinforzo, come la capacità di apprendere dal solo auto-gioco.

La sfida principale di questo argomento è quella di stabilire un approccio investigativo su un'area di creazione di IA autonoma dispiegabile, con l'intenzione di ampliare la prospettiva dell'intelligenza artificiale nella difesa informatica nell'UE.

Ambito di applicazione:
Le proposte devono concentrarsi sullo sviluppo di un agente di IA dispiegabile autonomo e adattivo. Tutte le attività proposte devono supportare in ultima analisi la creazione di un agente di intelligenza artificiale in grado di condurre una gestione automatizzata e semi-automatizzata degli incidenti su diversi sistemi di difesa informatica per l'intero processo del ciclo di gestione degli incidenti. Le soluzioni devono supportare gli operatori umani, gli analisti e i decisori a livello tecnico, tattico, operativo, strategico e politico. Inoltre, si prevede che le soluzioni contribuiscano a migliorare la consapevolezza della situazione informatica, ad aumentare la resilienza delle infrastrutture militari e a migliorare la protezione contro le minacce informatiche basate sull'intelligenza artificiale e altre minacce informatiche avanzate.

Il lavoro dovrebbe identificare le lacune per la realizzazione di un agente AI autonomo per i sistemi militari. Il risultato finale dovrebbe basarsi su un agente di intelligenza artificiale di uso generale che possa essere impiegato in diversi ambienti operativi.

Il lavoro dovrebbe anche affrontare la lacuna dell'apprendimento di set di dati attraverso l'uso di esercitazioni di fuoco dal vivo, concetti di data lake e algoritmi di autoapprendimento. L'accesso agli insiemi di dati dovrebbe essere pianificato in modo decentralizzato per consentire alla soluzione di essere distribuita. Ciò implica che si dovrebbero prendere in considerazione nuove architetture e soluzioni per raggiungere il decentramento, utilizzando e potenziando, ad esempio, l'edge computing alimentato dall'intelligenza artificiale.

La valutazione della soluzione proposta deve essere effettuata durante esercitazioni dal vivo con un metodo che consenta di confrontare l'agente AI sviluppato con le squadre di difesa effettive. Ciò significa utilizzare dati di apprendimento provenienti da esercitazioni diverse, ma anche dati provenienti dall'esercitazione stessa, in cui l'agente di intelligenza artificiale è in competizione.

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))
- Paesi non UE:
- Paesi SEE elencati ("Paesi associati al FES", cfr. elenco dei Paesi partecipanti
- avere la struttura di gestione esecutiva stabilita nei Paesi ammissibili
- non devono essere soggetti al controllo di un Paese terzo non associato o di un'entità di un Paese terzo non associato (a meno che non siano in grado di fornire garanzie - cfr. Allegato 2 - approvate dallo Stato membro o dal Paese associato al FES in cui sono stabiliti)

I beneficiari e gli enti affiliati devono iscriversi al 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. Altre entità possono partecipare in altri ruoli, come partner associati, subappaltatori, terzi che forniscono

contributi in natura, ecc. Si noti che, nel FES, anche i subappaltatori coinvolti nell'azione e i partner associati devono soddisfare le condizioni di stabilimento e controllo sopra elencate.
I partner associati che non sono stabiliti in uno dei Paesi ammissibili (o che sono soggetti al controllo di un Paese terzo non associato o di un'entità di un Paese terzo non associato) possono tuttavia partecipare in via eccezionale se sono soddisfatte alcune condizioni (non contravvenire agli interessi di sicurezza e difesa dell'UE e degli Stati membri;
- coerenza con gli obiettivi del FES;
- risultati non soggetti a controllo o restrizione da parte di Paesi terzi non associati o entità di Paesi terzi non associati;
- nessun accesso non autorizzato a informazioni classificate; nessun potenziale effetto negativo sulla sicurezza dell'approvvigionamento di fattori di produzione critici per il progetto), previo accordo dell'autorità concedente e senza alcun finanziamento nell'ambito della sovvenzione.
Le proposte devono essere presentati da minimo 3 candidati indipendenti (beneficiari; entità non affiliate) provenienti da 3 diversi paesi ammissibili.
I candidati devono possedere il know-how, le qualifiche e le risorse per attuare con successo i progetti e contribuire con la loro parte (compresa un'esperienza sufficiente in progetti di dimensioni e natura comparabili).

Contributo finanziario: I candidati devono disporre di risorse stabili e sufficienti per attuare con successo i progetti e contribuire con la loro parte. Le organizzazioni che partecipano a diversi progetti devono avere capacità sufficienti per attuare tutti questi progetti.
Il budget fissato per la call è di EUR 26 000 000
Il budget totale del progetto non potrà essere superiore al budget della call
I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc, ecc.) saranno fissati nella Convenzione di sovvenzione.

Scadenza: 22 Novembre 2023 17:00:00 Brussels time

Ulteriori informazioni:
call-fiche_edf-2023-da_en.pdf (europa.eu)