MARIO FURORE
EUROPARLAMENTARE

# Intelligenza artificiale  per il rafforzamento della sicurezza informatica

## AI for cybersecurity reinforcement
## TOPIC ID: HORIZON-CL3-2021-CS-01-03

**Ente finanziatore:** Commissione europea
Programma Horizon Europe

**Obiettivi ed impatto attesi:** L'intelligenza artificiale (AI) è presente in quasi tutte le aree di applicazione in cui sono coinvolti massive data  Comprendere le implicazioni e i possibili effetti collaterali per la sicurezza informatica richiede tuttavia un'analisi approfondita, compresa ulteriore ricerca e innovazione. Da un lato, l'AI può essere utilizzata per migliorare la risposta e la resilienza, ad esempio per il rilevamento precoce di minacce e altre attività dannose con l'obiettivo di identificare, prevenire e fermare gli attacchi in modo più accurato. Dall'altro lato, gli aggressori stanno sempre più alimentando i loro strumenti utilizzando l'AI o manipolando i sistemi AI (compresi i sistemi AI utilizzati per rafforzare la sicurezza informatica).

Le azioni proposte dovrebbero sviluppare metodi e strumenti basati sull'AI per affrontare le seguenti capacità interconnesse:
(i) migliorare la solidità dei sistemi (cioè la capacità di un sistema di mantenere la sua configurazione iniziale stabile anche quando elabora input errati, grazie all'auto-testing e all'auto-riparazione);
(ii) migliorare la resilienza dei sistemi (cioè la capacità di un sistema di resistere e tollerare un attacco, anticipare, far fronte ed evolvere facilitando il rilevamento delle minacce e delle anomalie e permettendo agli analisti della sicurezza di recuperare informazioni sulle minacce informatiche);
(iii) migliorare la risposta dei sistemi (cioè la capacità di un sistema di rispondere autonomamente agli attacchi, grazie all'identificazione delle vulnerabilità in altre macchine e di operare in modo strategico decidendo quale sia il sistema più adatto); e
(iv) contrastare i modi in cui l'IA può essere usata per attaccare. Le soluzioni avanzate basate sull'IA, compresi gli strumenti di apprendimento automatico, così come i meccanismi difensivi per garantire l'integrità dei dati dovrebbero anche essere inclusi nelle azioni proposte. Le proposte dovrebbero cercare di facilitare, in ultima analisi, il lavoro degli esperti di cybersecurity pertinenti (ad esempio, riducendo i carichi di lavoro degli operatori della sicurezza).
I progetti dovrebbero contribuire ad alcuni dei seguenti risultati attesi:
- Rafforzamento della cybersicurezza usando componenti e strumenti tecnologici dell'IA in linea con la politica pertinente dell'UE, i requisiti legali ed etici.
- Maggiore conoscenza di come un attaccante potrebbe usare la tecnologia IA per attaccare i sistemi IT.
- Processi, prodotti e sistemi digitali resilienti contro i cyberattacchi basati sull'IA

La proposta dovrebbe fornire indicatori appropriati per misurarne i progressi e l'impatto specifico.

**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 1 ) può partecipare (indipendentemente dal fatto che sia ammissibile o meno al finanziamento), purché siano soddisfatte le condizioni stabilite nel regolamento del programma Horizon Europe, 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. Un PIC convalidato non è un prerequisito per la presentazione della domanda.

Si applicano le seguenti eccezioni: Alcune attività, risultanti da questo argomento, possono comportare l'uso di informazioni di base classificate e/o la produzione di risultati sensibili per la sicurezza (EUCI e SEN). Si prega di fare riferimento alle relative disposizioni nella sezione B Sicurezza - Informazioni classificate e sensibili dell'UE degli allegati generali.

**Schema di finanziamento:** Azioni di ricerca e innovazione HORIZON-RIA HORIZON
Il budget disponibile è di 11 milioni di euro
Le azioni sono cofinanziate al 100% del totale dei costi eleggibili
La Commissione stima che un contributo dell'UE compreso tra 3,00 e 4,00 milioni di euro consentirebbe di affrontare adeguatamente questi risultati. Ciò non esclude tuttavia la presentazione e la selezione di una proposta che richieda importi diversi.

**Scadenza:** 21 Ottobre 2021

**Ulteriori informazioni: wp-6-civil-security-for-society_horizon-2021-2022_en.pdf (europa.eu)**