

Rafforzamento delle capacità di cibersecurity delle PMI europee mediante soluzioni di cibersecurity basate sull'intelligenza artificiale (IA)

Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions

TOPIC ID:

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME

Ente finanziatore:

Commissione europea
Programma Europa Digitale

Obiettivi ed impatto attesi:

Obiettivi

Sostenere l'adozione da parte del mercato e la diffusione di soluzioni innovative di cibersecurity basate sull'IA, in particolare nelle PMI, eventualmente utilizzando risultati derivanti da progetti Horizon Europe o analoghi, e migliorare le conoscenze e le attività di audit relative al livello di preparazione in materia di cibersecurity.

Le PMI spesso non dispongono delle risorse necessarie per valutare i rischi informatici, sviluppare strategie di cibersecurity e implementare soluzioni, risultando pertanto vulnerabili agli attacchi informatici. La resilienza delle organizzazioni che rientrano in questa categoria è fondamentale per la prosperità del mercato unico dell'UE.

La valutazione e la gestione dei rischi informatici possono essere significativamente migliorate e semplificate mediante l'applicazione di strumenti e soluzioni basati sull'IA. Tuttavia, ciò richiede una comprensione dell'evoluzione del panorama tecnologico, dei benefici derivanti dall'integrazione delle tecnologie e delle priorità di implementazione. Di fronte a vincoli organizzativi e finanziari, le PMI possono non riuscire a cogliere l'opportunità di sfruttare pienamente le soluzioni basate sull'IA per migliorare la propria cibersecurity e resilienza.

La cibersecurity costituisce una condizione preliminare per modelli e algoritmi di IA affidabili, sicuri e resilienti. La cibersecurity dell'IA non riguarda esclusivamente la protezione dei sistemi di IA contro minacce quali gli attacchi di poisoning ed evasion, ma implica anche la necessità di garantire caratteristiche di affidabilità, quali la supervisione umana e la robustezza, ossia la capacità di resistere agli attacchi informatici, come richiesto dall'AI Act dell'UE per i sistemi di IA ad alto rischio. La necessità di una supervisione umana dell'IA è stata inoltre sottolineata dagli esperti. L'utilizzo dell'IA a livello delle

PMI, a supporto dell'integrazione di algoritmi predittivi, può inoltre contribuire in misura significativa a un approccio bottom-up nella rilevazione delle vulnerabilità, nella mitigazione delle minacce e in una risposta coordinata agli incidenti più efficiente.

Ambito di applicazione

La presente azione mira ad aumentare il livello di maturità della gestione dei rischi informatici, migliorare la resilienza informatica e, in ultima analisi, promuovere una cultura della cibersicurezza tecnologicamente avanzata per le PMI nell'UE. Le azioni nell'ambito del presente topic dovrebbero sviluppare e implementare prodotti, strumenti e servizi basati sull'IA destinati alle PMI europee, consentendo anche il rilevamento e l'individuazione di modelli di attacco.

Le proposte dovrebbero comprendere lo sviluppo o l'adattamento del software/hardware e la validazione delle soluzioni.

L'azione prevede l'automazione dei processi fondamentali di cibersicurezza, in particolare nelle organizzazioni di piccole dimensioni operanti sul mercato, attraverso un toolkit SaaS adattato alle esigenze delle PMI. Tale toolkit dovrebbe consentire alle PMI di migliorare gli aspetti fondamentali della propria cibersicurezza, mettendo a disposizione strumenti di facile utilizzo per la gestione dei rischi, il rilevamento delle minacce, la risposta e la notifica degli incidenti, al fine di migliorare la loro igiene informatica e mitigare le potenziali minacce, proteggendo al contempo i dati personali. Il toolkit di cibersicurezza dovrebbe inoltre fornire funzionalità di previsione e risposta agli incidenti informatici per migliorare la resilienza delle PMI.

Le attività dovrebbero comprendere almeno una delle seguenti:

- Adozione/utilizzo di strumenti di cibersicurezza basati sull'IA nelle organizzazioni in cui tali strumenti non siano ancora stati adottati.
- Sviluppo di insiemi di strumenti di facile utilizzo, ad esempio toolkit, basati sull'IA per automatizzare i principali processi di cibersicurezza nelle PMI. Tale toolkit potrebbe fornire funzionalità automatizzate quali:
 - una funzione che supporti la valutazione e la gestione dei rischi di cibersicurezza di una PMI. Tale funzione dovrebbe effettuare una valutazione dei rischi, fornire raccomandazioni per la mitigazione dei rischi e individuare le possibili opzioni;
 - un'interfaccia con strumenti esistenti che supportino l'analisi e la valutazione dell'entità del rischio informatico di una PMI sulla base delle informazioni raccolte mediante la scansione delle infrastrutture digitali e dei dati forniti dagli utenti autorizzati;
 - una funzione che emetta avvisi relativi a vulnerabilità e minacce pertinenti sulla base delle informazioni raccolte dalla funzione di gestione dei rischi;
 - una funzione che colleghi le PMI a un Cyber Hub per segnalare un incidente e fornire, ove possibile, assistenza nelle attività di ripristino.
- Interfaccia utente per le PMI, associata al toolkit di cibersicurezza, per la segnalazione degli incidenti. Gli utenti possono segnalare un incidente, ricevere istruzioni sulle modalità di reazione e ottenere informazioni su come accedere al supporto per la risposta, mediante l'utilizzo di assistenti basati sull'IA.

Risultati attesi

- Sostenere l'adozione di soluzioni innovative di cibersicurezza basate sull'IA pronte per il mercato, comprese le soluzioni sviluppate nell'ambito di progetti di ricerca e innovazione sostenuti dall'UE.
- Fornire e implementare strumenti e servizi aggiornati basati sull'IA presso le organizzazioni, in particolare le PMI, al fine di prepararsi, proteggersi e rispondere alle minacce alla cibersicurezza.
- Integrare le tecnologie di IA nei processi di cibersicurezza per migliorare la sicurezza delle soluzioni ICT, anche mediante approcci innovativi alla formazione dei dipendenti sull'utilizzo di soluzioni di IA per la cibersicurezza.
- Implementazione di strumenti e tecnologie cibersicuri basati su un'IA affidabile; strumenti di cibersicurezza basati sull'IA; integrazione di strumenti per la protezione e la messa in sicurezza delle soluzioni di IA.

Criteri di eleggibilità:

Ammissibilità delle candidature

Le candidature saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del topic per il quale sono presentate.

Partecipanti ammissibili (Paesi ammissibili)

Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:

- essere entità giuridiche (organismi pubblici o privati);
- essere stabiliti in uno dei Paesi ammissibili, vale a dire:
 - Stati membri dell'UE (compresi i Paesi e territori d'oltremare – PTOM);
 - Paesi SEE (Norvegia, Islanda, Liechtenstein).

I beneficiari e le entità affiliate devono registrarsi nel Participant Register — prima della presentazione della proposta — e dovranno essere convalidati dal Central Validation Service (REA Validation). Ai fini della convalida, sarà loro richiesto di caricare documenti attestanti lo status giuridico e l'origine.

Altre entità possono partecipare ricoprendo altri ruoli all'interno del consorzio, quali partner associati, subappaltatori, terzi che forniscono contributi in natura, ecc. (cfr. sezione 13).

Si tenga presente che tutti i topic del presente invito sono soggetti a restrizioni per motivi di sicurezza; pertanto, le entità non devono essere direttamente o indirettamente controllate da un Paese che non sia un Paese ammissibile. Tutte le entità¹⁷ dovranno compilare e presentare una dichiarazione relativa alla proprietà e al controllo.

Inoltre

- la partecipazione a qualsiasi titolo (in qualità di beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità stabilite e controllate da Paesi ammissibili;
- le attività del progetto (compresi i lavori subappaltati) devono svolgersi nei Paesi ammissibili (cfr. la sezione relativa alla localizzazione geografica di seguito e la sezione 10);
- il Grant Agreement può prevedere restrizioni in materia di diritti di proprietà intellettuale (IPR) (cfr. sezione 10).

Contributo finanziario:

Budget disponibile

Budget del topic

15.000.000 EUR

La disponibilità del budget della call dipende ancora dall'adozione definitiva della modifica del Programma di lavoro 2025-2027.

Forma della sovvenzione, tasso di finanziamento e importo massimo della sovvenzione

I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi ammissibili totali, ecc.) saranno stabiliti nella Convenzione di sovvenzione (Grant Agreement) (Scheda dati, punto 3 e articolo 5).

Budget del progetto (importo della sovvenzione richiesta)

Importo della sovvenzione richiesta

Il contributo UE richiesto dovrebbe essere pari a 1,5 milioni di EUR per progetto. Tuttavia, potranno essere prese in considerazione anche proposte che richiedano importi diversi, purché ciò sia debitamente giustificato.

La sovvenzione concessa potrà essere inferiore all'importo richiesto.

Forma della sovvenzione e costi ammissibili

La sovvenzione assumerà la forma di una sovvenzione basata sul budget a costi effettivi misti (budget-based mixed actual cost grant: costi effettivi, con elementi basati su costi unitari e tassi forfettari).

Ciò significa che saranno rimborsate ESCLUSIVAMENTE determinate tipologie di costi (costi ammissibili) e i costi effettivamente sostenuti per il progetto (NON i costi preventivati).

Per i costi unitari e i tassi forfettari, potranno essere imputati gli importi calcolati secondo le modalità indicate nella Convenzione di sovvenzione (cfr. articolo 6 e Allegati 2 e 2a).

Tipologia di azione e tasso di finanziamento

Azioni di sostegno alle PMI (SME Support Actions) — tasso di finanziamento del 50% e del 75% per le PMI.

Divieto di profitto

Le sovvenzioni NON possono generare un profitto, vale a dire un'eccedenza dei ricavi + sovvenzione UE rispetto ai costi.

Le organizzazioni a scopo di lucro devono dichiarare i propri ricavi e, qualora si realizzi un profitto, questo sarà dedotto dall'importo finale della sovvenzione (cfr. articolo 22.3).

Riduzione dell'importo finale della sovvenzione

Si tenga inoltre presente che l'importo finale della sovvenzione potrà essere ridotto in caso di mancato rispetto della Convenzione di sovvenzione, ad esempio in caso di attuazione non corretta, violazione degli obblighi, ecc.

Scadenza:

14 Gennaio 2027 17:00:00 Brussels time

Ulteriori informazioni:

[8e1d6074-95ed-4b23-8bd3-2ca42b096411_en](#)