Strumenti, tecnologie e servizi di sicurezza informatica basati sull'intelligenza artificiale

Cybersecure tools, technologies and services relying on AI

TOPIC ID:
DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI

Ente finanziatore:
Commissione europea
Digital Europe Programme (DIGITAL)

Obiettivi ed impatto attesi:
Questo argomento riguarda le tecnologie basate sull'intelligenza artificiale (compresa la GenAI) per le autorità nazionali e competenti, compresi gli hub informatici nazionali e transfrontalieri, i CSIRT, gli enti pubblici e gli organismi privati della direttiva NIS 2, gli NCC1, ecc. Essi svolgono un ruolo fondamentale nel fornire capacità operative centrali agli ecosistemi europei di sicurezza informatica. Possono anche fornire dati primari per strumenti e soluzioni di sicurezza informatica basati sull'IA/ML, che possono rafforzare la capacità di tali autorità di analizzare, individuare e prevenire minacce e incidenti informatici e sostenere la produzione di informazioni di alta qualità sulle minacce informatiche. In particolare, l'adozione dell'IA generativa2 potrebbe rappresentare una sfida e un'opportunità per i processi e le applicazioni di sicurezza informatica3.

Queste tecnologie abilitanti dovrebbero consentire una creazione e un'analisi più efficaci delle informazioni sulle minacce informatiche (CTI), l'automazione di processi su larga scala, nonché un'elaborazione più rapida e scalabile delle CTI e l'identificazione di modelli che consentano un rilevamento e un processo decisionale rapidi.

È inoltre necessario affrontare la questione della sicurezza dell'IA stessa, in particolare per i sistemi in fase di apprendimento, compreso l'uso improprio dell'IA da parte di soggetti malintenzionati. Ciò comprende la valutazione e la mitigazione dei rischi di sicurezza informatica inerenti alle tecnologie di IA, l'attuazione della sicurezza della catena di approvvigionamento, ecc. e il rispetto della legge sull'IA, della legislazione sulla proprietà intellettuale e del GDPR.

Oltre ad essere sicure, le tecnologie di IA in fase di sviluppo dovrebbero funzionare bene ed essere robuste e affidabili. In particolare, disporre di soluzioni di IA affidabili sarà utile nella fase di implementazione, in cui l'accettazione sociale è essenziale.
Risultato atteso:

- Implementazione dell'intelligenza artificiale e di varie tecnologie basate sull'IA come strumenti abilitanti per Cyber Hub, CSIRT, NCSC, NIS SPOC e altri.
- Nuovi strumenti di sicurezza informatica basati sull'IA che sono stati sviluppati, testati e

convalidati in condizioni pertinenti e messi a disposizione di Cyber Hub, CSIRT, NCSC, NIS SPOC e altri.

- Miglioramento della condivisione delle informazioni e della collaborazione tra Cyber Hub nazionali e transfrontalieri, CSIRT, NCSC, NIS SPOC e altri soggetti interessati, con il supporto delle CTI prodotte da strumenti basati sull'intelligenza artificiale.
- Strumenti per l'automazione dei processi di sicurezza informatica, quali la creazione, l'analisi e l'elaborazione delle CTI, al fine di migliorare le operazioni dei Cyber Hub.
- Feed o servizi CTI europei originali.
- Garantire lo sviluppo e l'implementazione delle soluzioni di IA sicure più avanzate e innovative per i settori NIS.
- Soluzioni e strumenti di IA sicuri, conformi alla legislazione dell'UE. Promuovere la mitigazione dei rischi associati all'uso improprio dell'IA da parte di attori malintenzionati, con particolare attenzione all'etica dell'IA e alla sua implementazione sicura.
- Contributo alla standardizzazione e alla certificazione di tecnologie di IA sicure e affidabili.

Criteri di eleggibilità:
Le candidature saranno considerate ammissibili solo se il loro contenuto corrisponde in tutto (o almeno in parte) alla descrizione dell'argomento per il quale sono state presentate. Partecipanti ammissibili (paesi beneficiari potenziali) Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono: − essere persone giuridiche (enti pubblici o privati) − essere stabiliti in uno dei paesi ammissibili, ovvero: -
- 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 registro dei partecipanti — prima di presentare la proposta — e dovranno essere convalidati dal Servizio Centrale di Validazione (REA Validation). Per la convalida, verrà richiesto di caricare documenti che dimostrino lo status legale e l'origine.

Altri soggetti possono partecipare ad altri ruoli del consorzio, quali partner associati, subappaltatori, terzi che forniscono contributi in natura, ecc. (cfr. sezione 13). Si prega di notare tuttavia che tutti gli argomenti di questo bando sono soggetti a restrizioni per motivi di sicurezza, pertanto le entità non devono essere controllate direttamente o indirettamente da un paese che non è un paese ammissibile.

Tutti i soggetti dovranno compilare e presentare una dichiarazione sulla proprietà e sul 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 a entità stabilite e controllate da paesi ammissibili
− le attività del progetto (compreso il lavoro in subappalto) devono svolgersi in paesi ammissibili (cfr. la sezione Ubicazione geografica di seguito e la sezione 10)
− la Convenzione di sovvenzione può prevedere restrizioni in materia di diritti di proprietà intellettuale

Contributo finanziario:
Il budget stimato disponibile per la call è di € 15.000.000

I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno fissati nella Convenzione di sovvenzione (Scheda tecnica, punto 3 e art 5).

Budget del progetto

− per il tema DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI: indicativamente tra i 3 e i 5 milioni di euro per progetto ma non sono esclusi altri importi, se debitamente giustificati.

La sovvenzione concessa può essere inferiore all'importo richiesto. La sovvenzione consisterà in una sovvenzione per i costi effettivi misti basata sul budget (costi effettivi, con elementi di costo unitario e a tasso forfettario). Ciò significa che rimborserà SOLO alcuni tipi di costi (costi ammissibili) e costi che sono stati effettivamente sostenuti per il tuo progetto (NON i costi preventivati). Per i costi unitari e i tassi forfettari, è possibile addebitare gli importi calcolati come spiegato nella convenzione di sovvenzione (cfr. articolo 6 e allegati 2 e 2a). I costi saranno rimborsati al tasso di finanziamento fissato nella convenzione di sovvenzione. Questa percentuale dipende dal tipo di azione che si applica al tema (cfr. sezione 2). Le sovvenzioni NON possono produrre un profitto (ossia un'eccedenza di entrate + sovvenzione dell'UE rispetto ai costi). Le organizzazioni a scopo di lucro devono dichiarare i loro ricavi e, se c'è un profitto, lo detrarremo dall'importo finale della sovvenzione (vedi art 22.3). Inoltre, si prega di notare che l'importo finale della sovvenzione può essere ridotto in caso di mancato rispetto della convenzione di sovvenzione

Scadenza:
31 Marzo 2026

Ulteriori informazioni:
Call for proposals: DIGITAL-ECCC-2025-DEPLOY-CYBER-09 | European Cybersecurity Competence Centre and Network