

Nell'era dell'AI Engineering lancia piattaforma agentica EngSure

Descrizione

(Adnkronos) – In occasione della partecipazione al Digital Innovation Forum 2026, Engineering lancia EngSure, la nuova piattaforma agentica di cybersecurity che utilizza l'Intelligenza Artificiale per rafforzare la difesa degli asset digitali delle organizzazioni e proteggere l'ecosistema AI lungo tutto il suo ciclo di vita.

L'Intelligenza Artificiale sta trasformando profondamente lo scenario della sicurezza informatica. Da una parte rende gli attacchi più rapidi, credibili e scalabili, dall'altra introduce nuovi elementi da proteggere, come modelli, dati, prompt, agenti, applicazioni e workflow integrati nei processi aziendali. La crescente autonomia dei sistemi AI, capaci di accedere a informazioni, utilizzare strumenti e avviare operazioni, apre poi una nuova sfida. Non soltanto assicurarne le performance e proteggerli dalle minacce, ma anche mantenerne il controllo, garantendo che l'AI operi entro limiti definiti, sotto supervisione e in condizioni di sicurezza.

EngSure risponde a questa evoluzione integrando in un'unica piattaforma due esigenze complementari. Utilizzare l'AI per aumentare la velocità e l'efficacia della difesa informatica e, allo stesso tempo, proteggere e governare l'AI stessa. La soluzione crea infatti le condizioni di fiducia necessarie per affidare agli agenti AI attività rilevanti e accompagnarne l'adozione nei processi operativi di imprese e Pubbliche Amministrazioni. In concreto, la piattaforma può correlare segnali provenienti da fonti diverse per riconoscere e contenere rapidamente un attacco esterno, come un accesso anomalo o un tentativo di compromissione dei dati (phishing o furti di credenziali). Allo stesso modo, può rilevare se un agente AI prova a consultare dati o attivare operazioni fuori dal proprio perimetro autorizzato, bloccandolo o richiedendo l'intervento umano. Combinando automazione e competenze specialistiche, EngSure rende così modelli, dati e agenti AI sicuri, osservabili e governabili, prevedendo livelli di supervisione coerenti con il rischio e mantenendo le decisioni sotto la responsabilità delle persone.

Durante il suo intervento al panel dedicato ad AI, cybersecurity e crittografia post-quantum, l'Ad di Engineering Aldo Bisio ha spiegato: «La cybersicurezza è una condizione imprescindibile per la competitività e per la fiducia nell'innovazione digitale. Con Is-la abbiamo definito il nostro approccio a un'Intelligenza Artificiale governabile, trasparente e sicura, che consente alle organizzazioni di mantenere il controllo su dati, modelli, infrastrutture e processi. EngSure completa questa strategia, estendendone i principi alla cybersicurezza e proteggendo l'AI quando entra concretamente nei processi aziendali». EngSure si inserisce nella strategia Is-la, l'architettura di Engineering che consente a imprese e Pubbliche Amministrazioni di orchestrare e governare l'intero ciclo di vita dell'AI, integrando EngGpt 2 e mantenendo l'interoperabilità con modelli e piattaforme differenti.

EngSure completa questa architettura estendendone i principi alla cybersicurezza attraverso un framework di agenti AI proprietari, coordinati in quattro moduli specializzati. Il primo è Shield.

Monitora continuamente modelli, agenti e applicazioni AI in produzione, rileva anomalie e attacchi specifici e supporta le attività di risposta e contenimento. Il secondo Ã âProbeâ. Simula attacchi e comportamenti avversari per individuare vulnerabilitÃ e verificare la resilienza dei sistemi prima e durante il loro utilizzo. Il terzo Ã âCertisâ. Trasforma controlli, test ed evidenze tecniche in informazioni utilizzabili per governance, audit e compliance. âProvenanceâ analizza invece provenienza, qualitÃ e affidabilitÃ di dati e modelli, supportandone la valutazione del rischio nei diversi contesti applicativi.

EngSure porta questi controlli direttamente nei processi operativi dei clienti e trasforma test ed evidenze tecniche in informazioni utilizzabili per governance, audit e compliance. La piattaforma consente inoltre di definire e verificare il perimetro operativo degli agenti Ai, assicurando che agiscano entro autorizzazioni e livelli di supervisione prestabiliti. EngSure accompagna cosÃ¬ lâAi dalla sperimentazione allâimpiego operativo, con responsabilitÃ definite e condizioni di sicurezza che ne rendono possibile lâadozione su scala. Se Is-la permette di costruire, orchestrare e governare lâecosistema Ai dellâorganizzazione, EngSure ne orchestra la difesa. Engineering porta sicurezza e governance dentro i processi concreti delle organizzazioni. Dalla progettazione dei sistemi AI alla verifica prima del rilascio, fino alla sorveglianza continua durante il loro utilizzo. In linea con Is-la, EngSure abilita inoltre un approccio alla cybersecurity modulare, interoperabile e proporzionato. La piattaforma puÃ² essere adottata progressivamente e operare con modelli, framework e infrastrutture differenti, applicando livelli di sicurezza, governance e controllo coerenti con il caso dâuso, i requisiti normativi e il profilo di rischio dellâorganizzazione.

â

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Ottobre 15, 2026

Autore

redazione