Forbes
ITALIA

Cogit AI lancia Leonydas, la piattaforma di intelligenza artificiale per la cybersecurity

2026-06-12 12:15:38 di Forbes.it

URL:https://forbes.it/2026/06/12/cogit-ai-lancia-leonydas-la-piattaforma-di-intelligenza-artificiale-per-la-cybersecurity/

La cybersecurity è diventata una delle grandi emergenze silenziose del nostro tempo. Non perché manchino tecnologie di difesa, ma perché gli attacchi continuano a crescere nonostante l'aumento degli investimenti, delle procedure e degli strumenti di protezione. Le aziende installano firewall più evoluti, adottano sistemi di autenticazione multifattore, rafforzano gli endpoint, migliorano backup e monitoraggio. Eppure la superficie d'attacco continua ad allargarsi. Il motivo è semplice: la sicurezza informatica non riguarda più soltanto macchine, reti e infrastrutture. Riguarda le persone. Secondo il Data Breach Investigations Report di Verizon, **il fattore umano continua a essere coinvolto in una quota rilevante delle violazioni informatiche.** Nelle ultime analisi, phishing, credenziali rubate, errori operativi e comportamenti non sufficientemente consapevoli restano tra i principali fattori di rischio. Il report 2026 evidenzia inoltre che il 31% delle violazioni parte oggi dallo sfruttamento di vulnerabilità software, mentre il ransomware compare nel 48% delle violazioni analizzate. Il quadro economico è altrettanto significativo. Ibm, nel Cost of a Data Breach Report 2025, stima il costo medio globale di una violazione dei dati in 4,4 milioni di dollari. Lo stesso report segnala che il 63% delle organizzazioni non dispone di policy di governance adeguate per gestire l'intelligenza artificiale o prevenire la diffusione dello shadow AI, cioè l'utilizzo non governato di strumenti AI all'interno dell'azienda. A livello europeo, Enisa ha analizzato 4.875 incidenti nel Threat Landscape 2025, relativi al periodo compreso tra luglio 2024 e giugno 2025, descrivendo un ecosistema di minacce sempre più complesso, caratterizzato da sfruttamento rapido delle vulnerabilità, attacchi ransomware, campagne di phishing, DDoS e pressione crescente su pubbliche amministrazioni, infrastrutture, servizi digitali, trasporti e settore finanziario. Questi dati raccontano un passaggio ormai evidente: **la cybersecurity non è più una funzione isolata del reparto IT**. È diventata una questione di continuità aziendale, reputazione, governance e cultura organizzativa.

L'attacco

La maggior parte degli attacchi informatici non inizia con una spettacolare violazione dei sistemi, ma con un gesto del tutto ordinario. Può essere un link aperto di fretta, una password riutilizzata su più account, un allegato scaricato per distrazione o una richiesta urgente accettata senza le dovute verifiche. Il phishing e il social engineering funzionano così bene perché, prima ancora delle falle tecnologiche, colpiscono i meccanismi della natura umana, come la fiducia, l'abitudine, la fretta e la pressione gerarchica.

È proprio in questo spazio vulnerabile, dove la tecnologia incontra il comportamento umano, che si inserisce **Leonydas**, la piattaforma di intelligenza artificiale sviluppata da **Cogit AI**.

Questa soluzione va ben oltre la semplice formazione aziendale tradizionale. Leonydas nasce per supportare le organizzazioni nella costruzione di una solida cultura della sicurezza digitale, agendo su prevenzione, responsabilità, conformità normativa e uso sicuro della stessa IA. L'obiettivo finale non è sostituire il fattore umano con le macchine, ma allearsi con l'intelligenza artificiale per rendere le persone la prima, vera linea di difesa dell'azienda.

Cosa può fare l'IA

Nel dibattito pubblico l’intelligenza artificiale viene spesso raccontata come un moltiplicatore di rischio. Ed è vero: gli attaccanti possono usarla per scrivere email più credibili, personalizzare campagne di phishing, simulare identità e rendere decisamente più sofisticati i tentativi di social engineering. Ma questa è solo una parte della storia. **Esiste infatti anche un’intelligenza artificiale utile**, capace di supportare concretamente le aziende nella prevenzione, nella formazione continua e nella valutazione del rischio.

Questo tipo di tecnologia permette di rendere comprensibili temi altrimenti complessi, adattando i percorsi di apprendimento al ruolo specifico di ogni lavoratore attraverso la simulazione di scenari realistici. In questo modo è possibile misurare con precisione il livello di consapevolezza interna, trasformando le rigide policy aziendali in esperienze concrete e guidando il personale verso un uso più responsabile degli strumenti digitali.

Il richiamo a Leonida

Il nome Leonydas si ispira al re spartano, simbolo di disciplina, preparazione e capacità di affrontare minacce superiori attraverso l’addestramento. Il parallelismo non riguarda la guerra, ma la cultura della prontezza: Leonida non vinse per il numero di risorse, ma perché guidava persone addestrate e consapevoli.

Questa metafora è cruciale per la cybersecurity. Le aziende non possono muoversi solo dopo un attacco, né limitarsi a una policy da firmare o a un corso annuale. Devono allenare le persone prima che il rischio si presenti, trasformando la sicurezza in un'abitudine quotidiana. È questo il senso profondo di Leonydas: portare in azienda il principio della preparazione continua, per rendere il fattore umano la prima linea di difesa e non la principale vulnerabilità.

Formazione, consapevolezza e compliance

La necessità di preparare le persone non nasce solo dall'aumento degli attacchi, ma anche da un quadro normativo europeo sempre più esigente.

Con l'**AI Act**, l'Unione Europea ha introdotto il principio di *AI literacy*: chiunque utilizzi o fornisca sistemi di intelligenza artificiale deve garantire che il proprio personale abbia competenze e consapevolezza adeguate. La compliance, quindi, non si ferma più a documenti e policy, ma richiede la capacità reale delle persone di comprendere rischi e responsabilità degli strumenti usati. In parallelo, la direttiva **NIS2** rafforza l'obbligo di resilienza cyber e gestione del rischio.

Per le aziende la sfida è concreta: non basta installare la tecnologia, serve dimostrare di aver formato le persone. Sviluppata da Cogit AI, **Leonydas** nasce proprio per questo: aiutare le imprese a trasformare formazione e conformità normativa in un percorso continuo, integrato nei comportamenti quotidiani e vicino alla realtà operativa.

Oltre l’anello debole

Per anni le persone sono state definite l’anello debole della cybersecurity. È una formula parziale: il fattore umano è vulnerabile solo se non è preparato. Se messe in condizione di riconoscere i rischi, le persone diventano una risorsa decisiva: un dipendente formato può bloccare un attacco di phishing, un manager consapevole può sventare una frode e un team allenato riduce drasticamente l'esposizione dei dati.

La sicurezza del futuro dipenderà dalla tecnologia, ma soprattutto dalla maturità culturale delle organizzazioni. In quest'ottica, Leonydas non è solo una piattaforma, ma il simbolo di una trasformazione: la cybersecurity diventa una disciplina quotidiana che unisce governance, responsabilità e preparazione continua. Perché nel digitale, come nella storia, resiste solo chi si prepara prima.