



SOC e intelligenza artificiale in Italia: il 100% delle aziende pronta all'adozione

Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

In Italia tutte le aziende che intendono istituire un Security Operation Center (SOC) considerano l'intelligenza artificiale (IA) una componente indispensabile. Tuttavia, nonostante le grandi aspettative, le organizzazioni devono affrontare sfide significative nell'implementazione e nell'utilizzo efficace dell'IA. Tra queste rientrano la mancanza di dati di formazione di alta qualità, la carenza di personale qualificato in materia di IA, i costi di integrazione sostanziali e le nuove minacce legate all'IA.

Per capire come le aziende creano e gestiscono i processi nei SOC, Kaspersky ha realizzato uno studio globale che mette in evidenza, tra le altre cose, le priorità, le aspettative e le sfide legate all'uso dell'IA per migliorare le prestazioni dei SOC. I risultati mostrano che in Italia il 100% degli intervistati ha intenzione di integrare l'IA nelle proprie operazioni di sicurezza. Tra questi, quasi due terzi (63%) affermano che probabilmente lo faranno e il 37% dichiara che lo farà sicuramente. Questo dato sottolinea la percezione diffusa dell'IA come fattore fondamentale per migliorare il rilevamento delle minacce, accelerare i processi di indagine e aumentare l'efficienza complessiva dei SOC.

Per quanto riguarda i casi d'uso pratici, le aziende si aspettano principalmente che l'IA rafforzi le capacità di rilevamento delle minacce attraverso l'analisi automatizzata dei dati per identificare anomalie e attività sospette (46%) e faciliti l'automazione della risposta, consentendo la rapida esecuzione di scenari di risposta agli incidenti predefiniti (40%). Queste aspettative sono strettamente in linea con le principali motivazioni che spingono all'adozione dell'IA nei SOC: migliorare l'efficacia complessiva del rilevamento delle minacce (36%), automatizzare le attività di routine (41%) e aumentare la precisione riducendo i falsi positivi (37%). Le grandi imprese riportano costantemente piani più ampi e ambiziosi per l'applicazione dell'IA in più funzioni SOC.

Tuttavia, quando si passa dall'intenzione all'implementazione concreta dell'IA, emerge un evidente divario nell'esecuzione, caratterizzato da diverse sfide critiche e diffuse. La principale è la mancanza di dati di formazione di alta qualità, un ostacolo citato dal 24% delle aziende come un impedimento fondamentale che compromette l'accuratezza e la pertinenza dei modelli di IA. Questo problema è ulteriormente aggravato da altre preoccupazioni rilevanti: la carenza di esperti qualificati in IA all'interno del team interno (15%), l'emergere di nuove minacce e vulnerabilità legate all'uso dell'IA (26%) e i costi elevati associati allo sviluppo e alla manutenzione di soluzioni basate sull'IA (35%). Nel loro insieme, questi fattori creano una barriera che impedisce alle aziende di trasformare la strategia di IA in un successo operativo, sottolineando la necessità di un approccio strutturato e adeguatamente supportato.

Le aziende riconoscono chiaramente il valore che l'IA può apportare ai SOC, ma il passaggio dalla sperimentazione all'impatto reale sui SOC rimane ancora una sfida. Data la carenza di talenti nel campo della sicurezza informatica, e anche la scarsità di competenze nel campo dell'IA, l'introduzione di capacità interne di IA in un SOC resta un obiettivo ambito ma difficile da raggiungere. Questo è il motivo per cui le aziende di sicurezza informatica stanno investendo in funzionalità basate sull'IA nei loro prodotti di punta. Nel corso dell'ultimo anno, Kaspersky ha introdotto una suite completa di strumenti basati sull'intelligenza artificiale nel proprio portfolio B2B per soddisfare la crescente domanda di rilevamento tempestivo delle minacce più avanzate, rendendo al contempo le nostre soluzioni più efficienti e intuitive, ha dichiarato Anton Ivanov, Chief Technology Officer di Kaspersky.

Per creare e gestire un SOC affidabile e di successo, Kaspersky raccomanda di:

Per scoprire altre soluzioni e servizi di Kaspersky per la creazione e il potenziamento del tuo SOC, segui questo link.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Responsabilità editoriale di Kaspersky

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Febbraio 19, 2026

Autore

redazione

default watermark