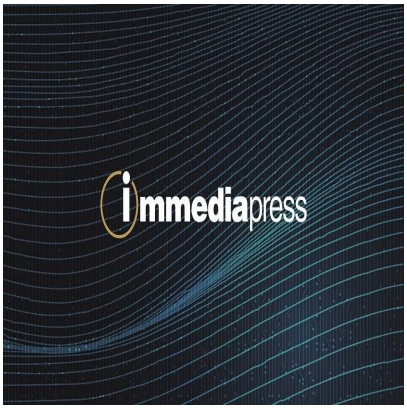

SOC e intelligenza artificiale in Italia: il 100% delle aziende pronta allâ??adozione

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

In Italia tutte le aziende che intendono istituire un Security Operation Center (SOC) considerano lâ??intelligenza artificiale (IA) una componente indispensabile. Tuttavia, nonostante le grandi aspettative, le organizzazioni devono affrontare sfide significative nellâ??implementazione e nellâ??utilizzo efficace dellâ??IA. Tra queste rientrano la mancanza di dati di formazione di alta qualitÃ , la carenza di personale qualificato in materia di IA, i costi di integrazione sostanziali e le nuove minacce legate allâ??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 prioritÃ , le aspettative e le sfide legate allâ??uso dellâ??IA per migliorare le prestazioni dei SOC. I risultati mostrano che in Italia il 100% degli intervistati ha intenzione di integrare lâ??IA nelle proprie operazioni di sicurezza. Tra questi, quasi due terzi (63%) affermano che probabilmente lo faranno e il 37% dichiara che lo farÃ sicuramente. Questo dato sottolinea la percezione diffusa dellâ??IA come fattore fondamentale per migliorare il rilevamento delle minacce, accelerare i processi di indagine e aumentare lâ??efficienza complessiva dei SOC.

Per quanto riguarda i casi dâ??uso pratici, le aziende si aspettano principalmente che lâ??IA rafforzi le capacitÃ di rilevamento delle minacce attraverso lâ??analisi automatizzata dei dati per identificare anomalie e attivitÃ sospette (46%) e faciliti lâ??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 allâ??adozione dellâ??IA nei SOC: migliorare lâ??efficacia complessiva del rilevamento delle minacce (36%), automatizzare le attivitÃ di routine (41%) e aumentare la precisione riducendo i falsi positivi (37%). Le grandi imprese riportano costantemente piani piÃ¹ ampi e ambiziosi per lâ??applicazione dellâ??IA in piÃ¹ funzioni SOC.

Tuttavia, quando si passa dallâ??intenzione allâ??implementazione concreta dellâ??IA, emerge un evidente divario nellâ??esecuzione, caratterizzato da diverse sfide critiche e diffuse. La principale Ã¨ la mancanza di dati di formazione di alta qualitÃ , un ostacolo citato dal 24% delle aziende come un impedimento fondamentale che compromette lâ??accuratezza e la pertinenza dei modelli di IA. Questo problema Ã¨ ulteriormente aggravato da altre preoccupazioni rilevanti: la carenza di esperti qualificati in IA allâ??interno del team interno (15%), lâ??emergere di nuove minacce e vulnerabilitÃ legate allâ??uso dellâ??IA (26%) e i costi elevati associati allo sviluppo e alla manutenzione di soluzioni basate sullâ??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 necessitÃ di un approccio strutturato e adeguatamente supportato.

â??Le aziende riconoscono chiaramente il valore che lâ??IA puÃ² apportare ai SOC, ma il passaggio dalla sperimentazione allâ??impatto reale sui SOC rimane ancora una sfida. Data la carenza di talenti nel campo della sicurezza informatica, e anche la scarsitÃ di competenze nel campo dellâ??IA, lâ??introduzione di capacitÃ interne di IA in un SOC resta un obiettivo ambito ma difficile da raggiungere. Questo Ã¨ il motivo per cui le aziende di sicurezza informatica stanno investendo in funzionalitÃ basate sullâ??IA nei loro prodotti di punta. Nel corso dellâ??ultimo anno, Kaspersky ha introdotto una suite completa di strumenti basati sullâ??intelligenza artificiale nel proprio portfolio B2B per soddisfare la crescente domanda di rilevamento tempestivo delle minacce piÃ¹ avanzate, rendendo al contempo le nostre soluzioni piÃ¹ efficienti e intuitiveâ•, 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 â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Febbraio 19, 2026
Autore
redazione