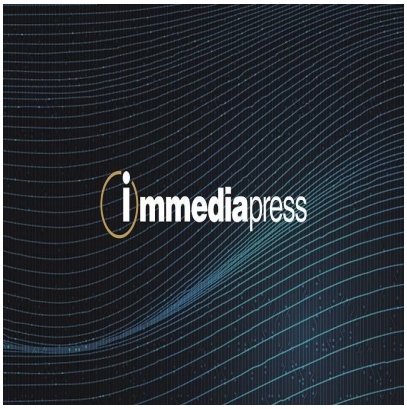

Kaspersky: in Italia quasi il 67% delle aziende sceglie di esternalizzare parte del proprio SOC

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Secondo una ricerca condotta da Kaspersky, la maggior parte delle aziende sceglie di esternalizzare almeno una parte del proprio Security Operations Center (SOC) e un numero significativo adotta il modello SOC-as-a-Service (SOCaaS). Questa scelta strategica consente alle organizzazioni di beneficiare di una protezione attiva 24 ore su 24, di garantire la conformitÃ agli standard normativi e di accedere a soluzioni avanzate di cybersecurity e a competenze specialistiche che spesso superano le capacitÃ interne.

Con lâ??aumento della sofisticazione delle minacce informatiche, le aziende stanno ripensando il modo in cui progettano e gestiscono i propri Security Operations Center[1]. In questo contesto, Kaspersky ha condotto una ricerca globale approfondita per identificare le principali motivazioni, gli obiettivi strategici e le sfide legate alla pianificazione e allâ??implementazione dei SOC. I risultati mostrano chiaramente che anche in Italia questa tendenza Ã¨ ormai consolidata: il 67% delle aziende italiane prevede di esternalizzare parte del proprio SOC, combinando risorse interne con competenze esterne, mentre il 22% Ã¨ pronto ad adottare un modello completamente SOC-as-a-Service (SOCaaS). Al contrario, solo lâ??11% delle aziende in Italia prevede di costruire un SOC interamente in-house, a conferma delle difficoltÃ crescenti nel garantire un monitoraggio continuo 24/7 e nellâ??attrarre e trattenere professionisti altamente qualificati.

Lâ??outsourcing del SOC consente alle aziende di delegare singole funzioni o lâ??intero ciclo operativo a un fornitore esterno di fiducia. Questo approccio puÃ² includere diversi servizi, tra cui:

Dai dati emerge che la maggior parte delle aziende preferisce mantenere internamente le attivitÃ strategiche, affidandosi invece a team esterni e tecnologie avanzate per i carichi di lavoro piÃ¹ operativi e altamente tecnici. Tra le aziende italiane che intendono esternalizzare le funzioni SOC, le attivitÃ piÃ¹ frequentemente delegate a fornitori terzi sono lâ??installazione e lâ??implementazione delle soluzioni (45%), la progettazione del SOC (43%) e lo sviluppo e la fornitura di soluzioni (34%).

Quando si rivolgono a specialisti SOC esterni, le aziende in Italia mostrano inoltre una chiara preferenza per il rafforzamento di ruoli specifici: gli analisti di seconda linea risultano i piÃ¹ richiesti (62%), seguiti dagli analisti di prima linea (35%). Questi dati evidenziano come le organizzazioni italiane si concentrino soprattutto sulle attivitÃ di sicurezza operative e intermedie, come il monitoraggio continuo e la risposta alle minacce.

PerchÃ© le aziende scelgono lâ??outsourcing SOC?

Il principale fattore che spinge verso lâ??outsourcing del SOC in Italia Ã¨ la necessitÃ di garantire una protezione continua 24 ore su 24, 7 giorni su 7 (39%), un requisito che molti team interni faticano a sostenere autonomamente. Un altro vantaggio chiave Ã¨ la riduzione del carico di lavoro per gli specialisti interni della sicurezza IT (38%), che possono cosÃ¬ concentrarsi su attivitÃ a maggiore valore strategico.

A ciÃ² si aggiungono lâ??accesso a soluzioni e tecnologie avanzate (36%) e il supporto esterno per assicurare la conformitÃ ai requisiti normativi e agli standard di settore (28%). Questi elementi rafforzano ulteriormente la scelta dellâ??outsourcing, sottolineando il valore delle competenze specialistiche e di strumenti evoluti come XDR, MDR, MXDR e altre tecnologie avanzate.

Lâ??ottimizzazione del budget Ã¨ considerata una prioritÃ solo dal 36% delle aziende italiane, a dimostrazione del fatto che il valore principale dellâ??outsourcing del SOC risiede soprattutto in una protezione piÃ¹ efficace, e non esclusivamente nella riduzione dei costi.

â??La tendenza allâ??esternalizzazione, totale o parziale, delle funzioni SOC Ã¨ guidata principalmente dalla necessitÃ di maggiore focalizzazione operativa e agilitÃ strategica. Affidando a partner esterni le attivitÃ tecniche e di routine, le aziende possono concentrarsi su iniziative ad alto valore, come il processo decisionale strategico e il coordinamento delle risposte alle minacce piÃ¹ sofisticate. Inoltre, questo approccio consente spesso di ottenere significative efficienze economiche, favorendo unâ??allocazione piÃ¹ efficace delle risorse. In definitiva, questo modello trasforma il SOC in una capacitÃ strategica fondamentale, contribuendo direttamente alla continuitÃ operativaâ?•, ha commentato Sergey Soldatov, Head of Security Operations Center di Kaspersky.

Per le aziende che intendono realizzare un SOC, Kaspersky raccomanda di:

Per scoprire altre soluzioni e servizi di Kaspersky per la creazione e il potenziamento del tuo SOC, Ã¨ possibile consultare il seguente link.

[1] Alla ricerca hanno partecipato professionisti senior della sicurezza IT, manager e direttori di organizzazioni con almeno 500 dipendenti, con particolare attenzione alle aziende che non dispongono ancora di un Security Operations Center (SOC) ma che intendono crearne uno nel prossimo futuro. Gli intervistati in questo studio provengono da 16 paesi, tra cui Germania, Spagna, Italia, Brasile, Messico, Colombia, Singapore, Vietnam, Cina, India, Indonesia, Arabia Saudita, Turchia, Egitto, Emirati Arabi Uniti e Russia.

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
Gennaio 27, 2026
Autore
redazione