Kaspersky: oltre il 40% delle aziende italiane investirÃ in un SOC per rafforzare la cybersecurity

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Rafforzare la sicurezza informatica, individuare e rispondere piÃ¹ rapidamente alle minacce e ottenere un vantaggio competitivo sono tra i principali motivi che spingono le aziende a creare un Security Operations Center (SOC). Nonostante la crescente diffusione di soluzioni automatizzate per la cybersecurity, le organizzazioni continuano a fare affidamento su professionisti esperti per le decisioni strategiche, a conferma del fatto che le competenze umane restano un elemento chiave per una gestione efficace della sicurezza.

Un SOC Ã¨ unâ??unitÃ organizzativa dedicata al monitoraggio continuo e alla protezione dellâ??infrastruttura IT aziendale. La sua missione principale Ã¨ individuare, analizzare e rispondere in modo proattivo alle minacce informatiche. Per comprendere i principali fattori trainanti, le prioritÃ strategiche e le potenziali sfide legate alla pianificazione e allâ??implementazione dei SOC, Kaspersky ha condotto uno studio globale coinvolgendo specialisti senior della sicurezza IT, manager e direttori di aziende con almeno 500 dipendenti. Tutti i partecipanti operano attualmente senza un Security Operations Center, ma prevedono di crearne uno nel prossimo futuro. La ricerca ha preso in esame 16 Paesi tra APAC, META, LATAM, Europa e Russia, offrendo una panoramica completa sulle tendenze emergenti e sulle migliori pratiche nello sviluppo dei SOC a livello globale.

I risultati mostrano che in Italia il 44% delle aziende intende istituire un SOC principalmente per rafforzare la propria postura di sicurezza informatica, mentre il 28% Ã¨ spinto dalla necessitÃ di affrontare minacce sempre piÃ¹ sofisticate e pericolose. Tra le motivazioni secondarie emergono lâ??ottimizzazione del budget (36%), lâ??esigenza di un rilevamento e di una risposta piÃ¹ rapidi agli incidenti (27%) e lâ??espansione di software, endpoint e dispositivi utente (34%), che richiede misure

di sicurezza piÃ¹ articolate e stratificate. Inoltre, il 42% delle aziende punta a una migliore protezione delle informazioni riservate, il 27% mira alla conformitÃ normativa e il 40% si aspetta che le capacitÃ offerte da un SOC possano tradursi in un vantaggio competitivo. Le organizzazioni di dimensioni maggiori tendono a citare tutte queste ragioni con maggiore frequenza, riflettendo pressioni operative e normative piÃ¹ ampie.

Il monitoraggio continuo Ã¨ il requisito principale del SOC

La funzione principale affidata a un SOC dalle aziende italiane Ã¨ la rilevazione delle minacce, indicata dal 46% degli intervistati, seguita dal monitoraggio della sicurezza 24 ore su 24 (39%), che consente di individuare tempestivamente anomalie, prevenire lâ??escalation degli attacchi e mantenere la resilienza informatica in tempo reale. Questa prioritÃ evidenzia un approccio sempre piÃ¹ strategico e proattivo alla gestione del rischio, necessario per contrastare minacce persistenti che possono colpire in qualsiasi momento.

Le aziende che prevedono di esternalizzare completamente le operazioni SOC mostrano un maggiore interesse per lâ??applicazione di metodologie basate sulle â??lezioni appreseâ?•, mentre quelle che scelgono di sviluppare SOC interni pongono una maggiore attenzione sulla gestione degli accessi, al fine di mantenere un controllo piÃ¹ rigoroso.

Le competenze umane guidano le scelte tecnologie SOC

Sebbene i SOC facciano ampio uso di tecnologie avanzate, le scelte delle aziende italiane confermano il ruolo centrale degli analisti umani. Le tre tecnologie piÃ¹ adottate sono piattaforme di Threat Intelligence (48%), soluzioni di Endpoint Detection and Response (40%) e sistemi di Security Information and Event Management (31%) che permettono di automatizzare la raccolta dei dati e ridurre il carico operativo, ma richiedono competenze specialistiche per fornire il giusto contesto, interpretare risultati complessi e assumere decisioni critiche nelle fasi di risposta agli incidenti. Tra le altre soluzioni selezionate figurano Extended Detection and Response (43%), Network Detection and Response (28%) e Managed Detection and Response (32%).

A livello globale, le grandi aziende tendono a implementare un numero maggiore di tecnologie, con una media di 5,5 soluzioni per SOC, mentre le realtÃ piÃ¹ piccole ne integrano mediamente 3,8.

â??Per creare un SOC efficiente, le aziende devono dare prioritÃ non solo alla giusta combinazione di tecnologie, ma anche a una pianificazione accurata dei processi, alla definizione di obiettivi chiari e a unâ??efficace allocazione delle risorse. Flussi di lavoro ben strutturati e un miglioramento continuo sono fondamentali per consentire agli analisti umani di concentrarsi sulle attivitÃ critiche, rendendo il SOC una componente proattiva e adattabile della strategia di sicurezza informaticaâ?•, ha commentato Roman Nazarov, Head of SOC Consulting di Kaspersky.

Per creare e gestire in modo efficace il proprio SOC, Kaspersky consiglia di:

Ulteriori informazioni su soluzioni e servizi di Kaspersky per la creazione e il potenziamento del proprio SOC, sono disponibili al seguente 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
Gennaio 21, 2026
Autore
redazione