kaspersky

Kaspersky
Managed Detection
and Response

Fermiamo gli incidenti prima che fermino la vostra attività

Aumentate la resilienza della sicurezza informatica con una protezione gestita 24 ore su 24, 7 giorni su 7

Kaspersky Managed Detection and Response è un servizio gestito da esperti che offre monitoraggio, rilevamento, indagine e una risposta rapida 24 ore su 24 agli attacchi informatici più sofisticati, potenziando i controlli di sicurezza esistenti con rilevamento guidato dall'uomo e intelligence sulle minacce globali. Il servizio rafforza immediatamente la vostra postura di sicurezza IT e OT, indipendentemente dalle dimensioni o dal settore della vostra organizzazione.

Vantaggi chiave

Protezione avanzata continua su tutta la superficie di attacco (endpoint, rete, cloud e oltre) fin dal primo giorno.

Un SOC pronto all'uso 24 ore su 24, 7 giorni su 7 con un team globale di esperti, che elimina la necessità di creare, gestire ed eseguire la manutenzione delle proprie operazioni di sicurezza interne.

Un carico di lavoro ridotto per il vostro team di sicurezza interna, delegando a noi il monitoraggio, il triage e le indagini.

Sicurezza orientata ai risultati che unisce competenza umana, threat intelligence e intelligenza artificiale per bloccare gli incidenti prima che possano avere ripercussioni sulla vostra attività.

Il lavoro da remoto, la rapida crescita dello scambio delle informazioni, il gap sempre maggiore di competenze a livello globale e il numero crescente di cyberminacce in grado di aggirare i controlli tradizionali automatizzati di prevenzione e rilevamento delle minacce stanno mettendo sempre più sotto pressione le organizzazioni di tutte le dimensioni. In questo contesto, è fondamentale rispondere in modo rapido ed efficace a ogni incidente.

Una panoramica delle minacce informatiche odierne[1]

1 Vettori di attacco iniziali

31% account validi

13% rapporto di fiducia

39% exploit di un'applicazione rivolta al pubblico

2 Operatività costante

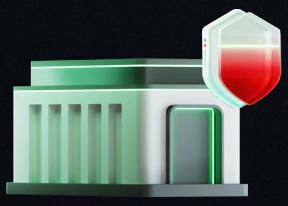
Gli autori degli attacchi spesso utilizzano strumenti legittimi (come Mimikatz, PsExec, SoftPerfect Network Scanner) in infrastrutture prive di adeguati controlli di configurazione del sistema.

3 Impatto

42% file criptati

17% fuga di dati

11% persistenza dell'installazione per l'impatto futuro



Le prove dimostrano che spesso gli attaccanti ritornano dopo un attacco andato a buon fine.

Durata dell'attacco

Rapida	Nella media	Di lunga durata
45%	20%	35%
fino a 1 giorno	13 giorni	253 giorni

> Kaspersky MDR ha rilevato e bloccato con successo un attacco zero-day che altrimenti avrebbe potuto causare gravi interruzioni alle nostre operazioni.

Daniel Huerta Santos
Cybersecurity Manager, Guanajuato State Government

Per saperne di più

1 Rapporto Kaspersky MDR and Incident Response

Cosa offre Kaspersky MDR

Protezione continua contro le minacce avanzate fin dal primo giorno

Kaspersky MDR si attiva in pochi minuti senza bisogno di infrastrutture aggiuntive, avvalendosi dei nostri analisti SOC e delle informazioni sulle minacce per fornire un rilevamento multilivello su più domini. Basato su miliardi di segnali di telemetria, consente la ricerca proattiva delle minacce, l'indagine sulla root cause e una correzione completa e rapida, proteggendo dalle minacce note e zero-day fin dal primo giorno.

Scenari di utilizzo

- Protezione pronta all'uso 24 ore su 24, 7 giorni su 7 per le organizzazioni senza SecOps
- SecOps co-gestito per potenziare i team interni di sicurezza informatica
- Protezione avanzata per l'infrastruttura OT
- Protezione continua dedicata dei sistemi integrati

Operazioni di sicurezza condotte da esperti, potenziate dall'intelligence

Con Kaspersky MDR, le operazioni di sicurezza sono gestite da esperti globali con una profonda esperienza in prima linea e certificazioni leader del settore. Il loro lavoro è amplificato dai meccanismi di threat intelligence e IA leader di mercato integrati nel servizio, che contribuiscono ad arricchire ogni avviso, ad accelerare il rilevamento e a ridurre il tempo medio di risposta (MTTR).

30-minuti
MTTR medio [2]

30%
di tutti gli avvisi ricevuti elaborati da AI Auto Analyst [1]

Efficienza operativa e prevedibilità dei costi

- Kaspersky MDR elimina la complessità e i costi di creazione di un SOC interno da zero, un processo che può prosciugare il budget e ritardare significativi miglioramenti della sicurezza per mesi o addirittura anni.
- Se disponete già di un SOC vostro, il servizio si fa carico del monitoraggio 24 ore su 24, 7 giorni su 7, della selezione degli avvisi e della classificazione degli incidenti, consentendo agli analisti di concentrarsi su lavori strategici di maggior valore.

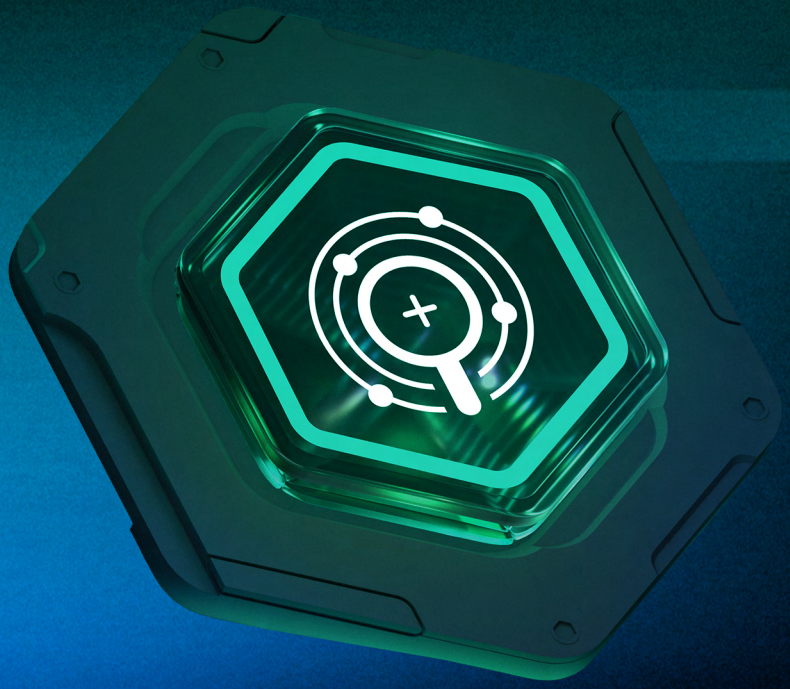
fino a 15 minuti
è il tempo necessario per attivare Kaspersky MDR

fino a 2 anni
è il tempo necessario per creare operazioni di sicurezza interne da zero

70%
dei team di sicurezza fatica a tenere il passo con il numero di avvisi generati dagli strumenti di sicurezza [3]

2 Secondo i nostri rapporti annuali degli analisti MDR

3 Ritratto del moderno professionista della sicurezza informatica, 2024



Kaspersky Managed Detection and Response

Pianificazione demo

www.kaspersky.it

#kaspersky
#bringonthefuture