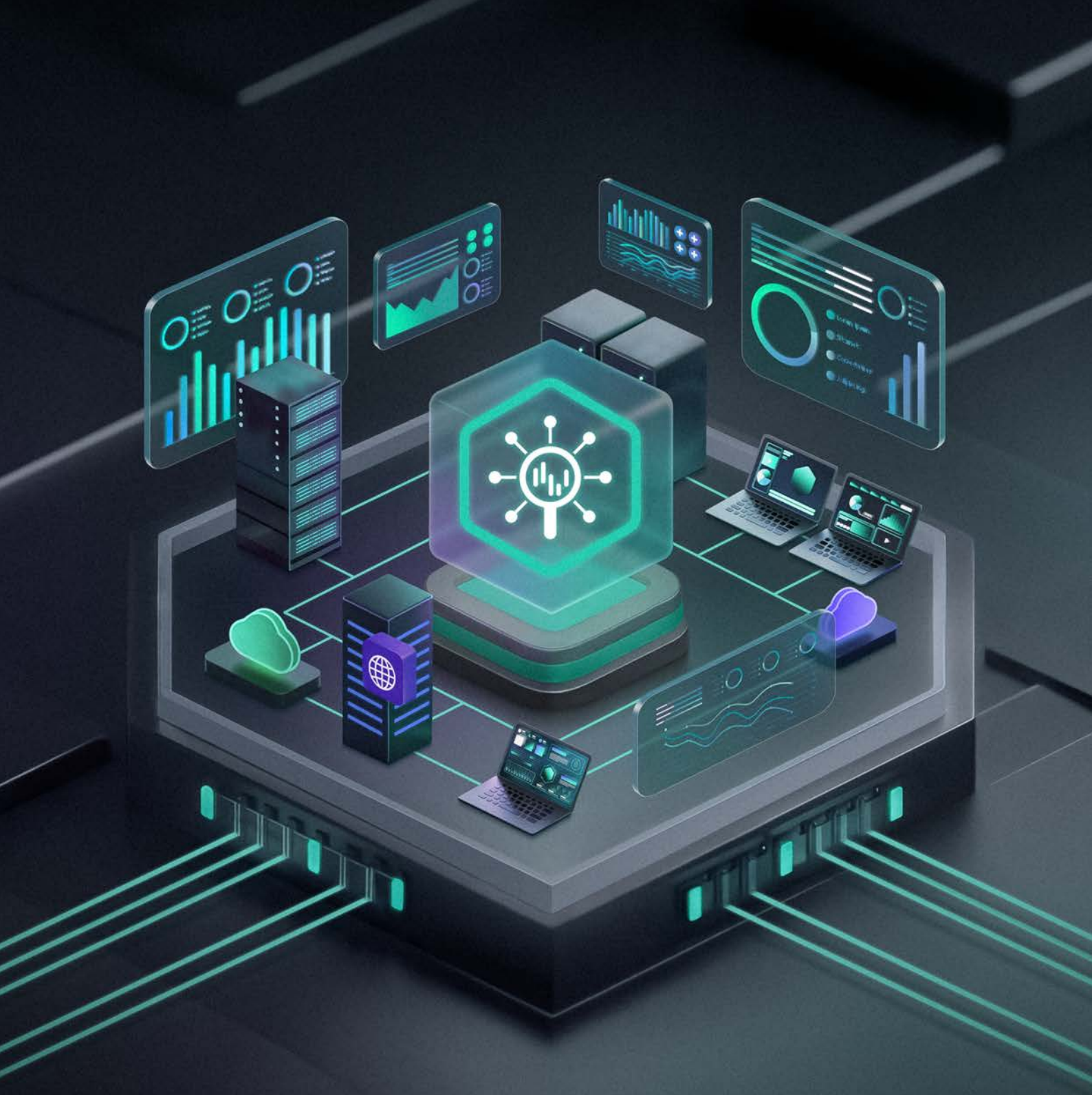


Scheda tecnica

Kaspersky SIEM

Trasformate le vostre operazioni di sicurezza con la nostra soluzione di nuova generazione, basata sull'intelligenza artificiale e potenziata con threat intelligence di livello mondiale

kaspersky bring on the future

Kaspersky SIEM è stato sviluppato appositamente per le organizzazioni con infrastrutture IT complesse, elevati volumi di dati e rigorosi requisiti normativi. Kaspersky SIEM supporta nativamente la multi-tenancy, venendo incontro alle esigenze degli MSSP.

Queste organizzazioni riconoscono che una sicurezza efficace non dipende solo dalla prevenzione, ma anche dalla capacità di rilevare, analizzare e rispondere alle minacce in tempo reale su diversi sistemi.

Ottimizzate l'impatto delle vostre operazioni di sicurezza

Le grandi organizzazioni si trovano ad affrontare un numero crescente di minacce persistenti avanzate (APT). Nel 2024, sono stati rilevati APT in un'azienda su quattro e hanno rappresentato il 43% di tutti gli incidenti di elevata gravità[1]. Le conseguenze sono costose e vanno dall'interruzione dell'attività alle perdite finanziarie e ai danni reputazionali a lungo termine.

I team di sicurezza sono sottoposti a una pressione senza precedenti. I sistemi di protezione generano enormi volumi di dati, facendo aumentare i costi di archiviazione e rendendo costose le implementazioni SIEM. Gli analisti esperti non sono numerosi, ed i team esistenti sono sopraffatti: il 70% dei SOC (Security Operation Center) fa fatica a tenere il passo con il flusso eventi da analizzare[2]. Oltre a ciò, la complessità dell'amministrazione dei sistemi SIEM grava ulteriormente sulle risorse già limitate.

Anche i SOC più strutturati rischiano di perdere efficienza. Inoltre, senza gli strumenti basati sull'intelligenza artificiale si perde un valido aiuto alla qualificazione e a concentrarsi su ciò che conta di più.

Fornite al vostro team un SIEM basato sull'intelligenza artificiale supportato da threat intelligence di livello mondiale

Kaspersky SIEM è una soluzione di nuova generazione progettata per aiutare il vostro team di sicurezza a gestire e analizzare gli eventi di sicurezza. Eccelle in:

- Raccolta, elaborazione e archiviazione di eventi provenienti da diverse fonti, tra cui prodotti Kaspersky, sistemi operativi, applicazioni di terze parti, strumenti di sicurezza e database.
- Analizzando e correlando i dati in arrivo in tempo reale, arricchendoli con threat intelligence leader del settore per rilevare attività sospette.
- Fornire avvisi tempestivi per consentire indagini e risposte rapide agli incidenti.
- Archiviazione dei dati per un periodo prolungato senza sforare il budget per hardware di archiviazione costosi, grazie a diverse opzioni di archiviazione che permettono una con funzionalità di ricerca simultanea senza interruzioni.

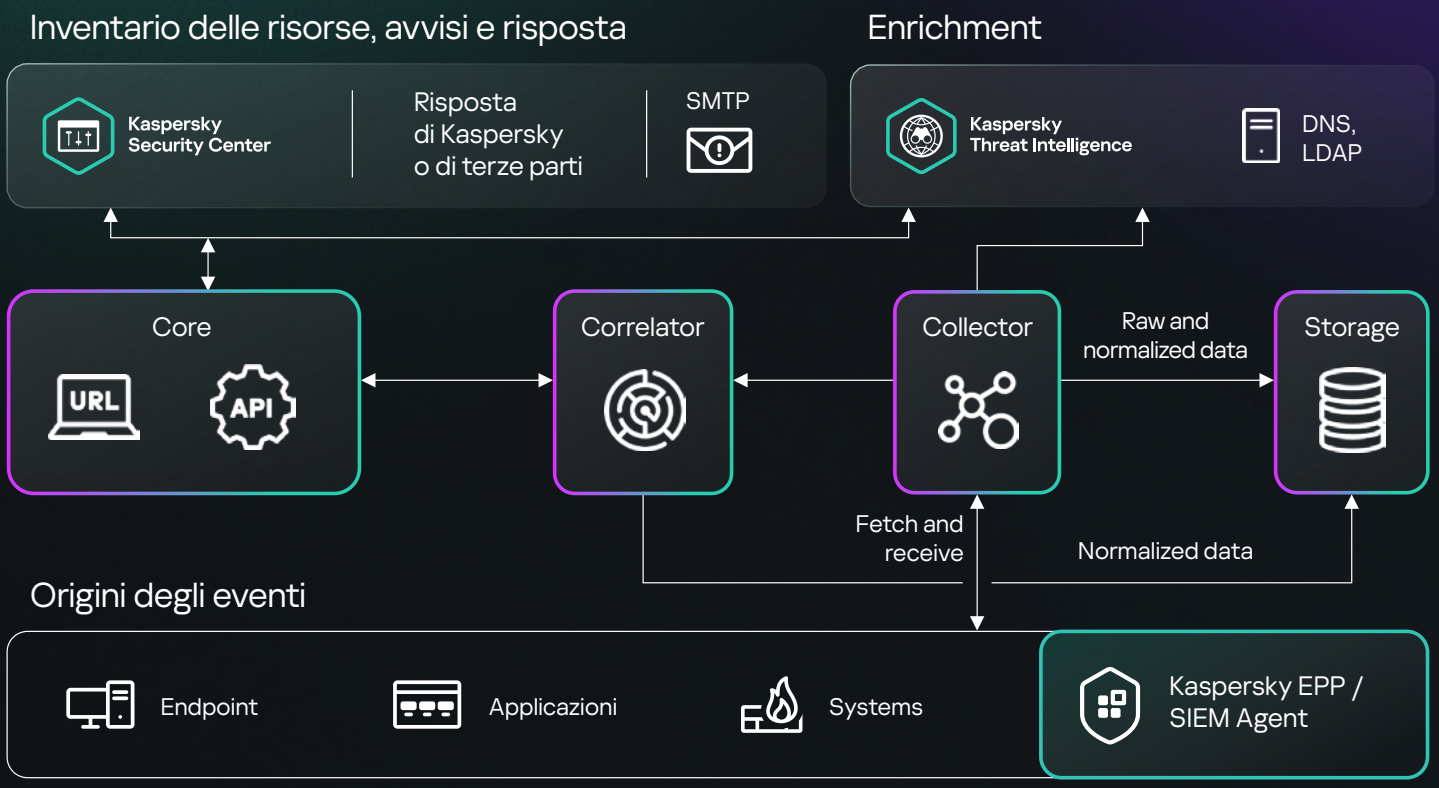
Unificando i log provenienti da diverse sorgenti di dato e correlandoli in tempo reale, Kaspersky SIEM fornisce agli analisti la visibilità completa e il contesto necessario per rispondere in modo efficiente.

Offre funzionalità di ricerca e analisi avanzate che consentono agli analisti di un SOC di individuare minacce precedentemente sconosciute. L'analisi dei dati storici e la baseline statistica con il set di regole di rilevamento UEBA aiutano il vostro team a identificare anomalie e a bloccare attacchi sofisticati.

Con Kaspersky SIEM, il SOC ottiene la visibilità, l'intelligence e l'efficienza di cui ha bisogno per trasformare dati enormi in informazioni di sicurezza fruibili. La soluzione può funzionare anche senza connettività Internet, garantendo la piena sovranità dei dati.

1 Report degli analisti Kaspersky Managed Detection and Response per il 2024
2 Kaspersky Report: The portrait of modern information security professional, 2024

Come funziona



Grazie all'architettura a microservizi della soluzione, gli amministratori possono creare e configurare i microservizi necessari per utilizzare Kaspersky SIEM come strumento completo o come sistema di gestione dei log.

Kaspersky SIEM è basato su una Open Single Management Platform[3], che integra sia i prodotti Kaspersky che quelli di terze parti in un sistema di sicurezza centralizzato. Costituisce una parte essenziale di una strategia di difesa completa, proteggendo gli ambienti aziendali e industriali e rilevando i cyberattacchi che si spostano dai sistemi IT a quelli OT.

Quali sono le caratteristiche distintive di Kaspersky SIEM

Ottimizza le prestazioni e riduce al minimo i costi

Riducete i costi di hardware e virtualizzazione fino al 50% e abbassate il TCO con un SIEM modulare ad alte prestazioni che supera le soluzioni legacy e gestisce centinaia di migliaia di EPS per singola instanza.

Un unico ecosistema Kaspersky integrato

Sfruttate oltre 200 integrazioni preconfigurate con Kaspersky e terze parti con opzioni di risposta integrate. Il nostro ecosistema offre un'unica interfaccia per threat intelligence, sensori endpoint come agenti SIEM fornendo funzionalità di integrazione ineguagliabili rispetto ad altri fornitori.

Esperienza SOC integrata

Sfruttate le oltre 700 regole di rilevamento preconfigurate, aggiornate trimestralmente con mappatura MITRE e indicazioni di risposta, tutte sviluppate direttamente dal SOC Kaspersky, uno dei team di ricerca delle minacce più esperti del settore.

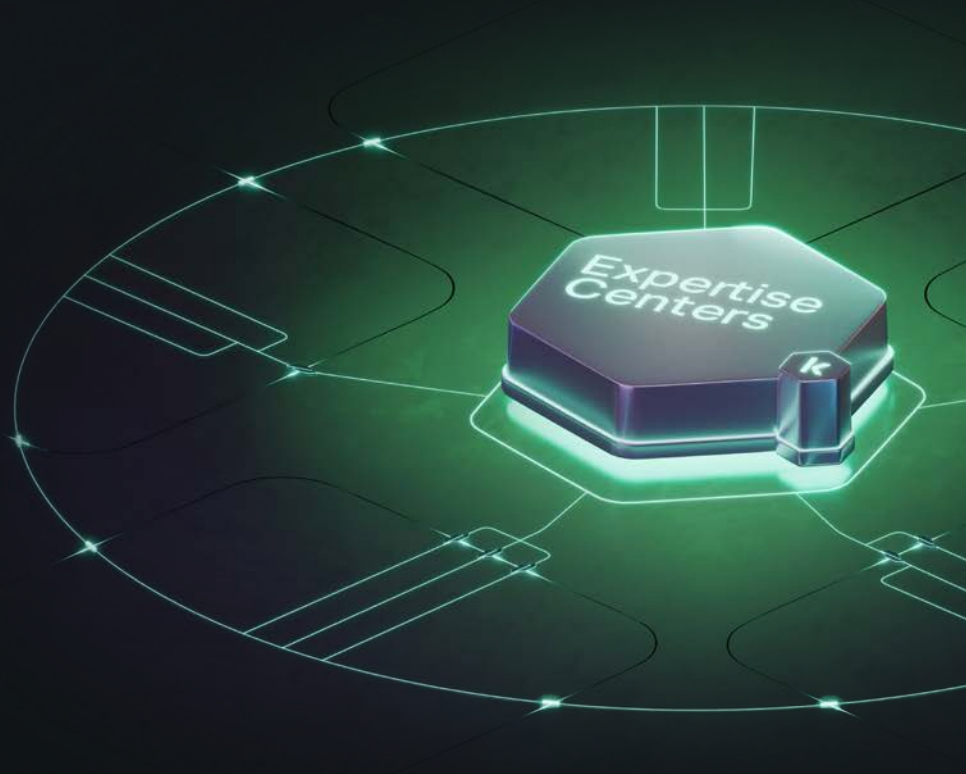
Rilevamento delle minacce basato su AI

Grazie all'utilizzo di componenti che sfruttano l'Intelligenza Artificiale, è possibile identificare rapidamente le attività sospette nella vostra infrastruttura, con rilevamento AI del hijacking di DLL, punteggio di rischio delle risorse e altro ancora. Queste funzionalità migliorano la precisione del rilevamento, riducendo sia i falsi positivi che l'impatto degli incidenti informatici, contribuendo a migliorare MTTD e MTTR.

3 Kaspersky Next XDR Expert, basato su questa piattaforma, amplia le capacità con funzionalità avanzate di ricerca delle minacce, playbook automatizzati e gestione semplificata dei casi.

Kaspersky SIEM sfrutta anni di conoscenze accumulate e competenze affinate dei Kaspersky Expertise Center, cinque hub specializzati in cybersecurity.

Per saperne di più



Kaspersky SIEM fornisce supporto e servizi Premium H24/7, incluse integrazioni personalizzate realizzate da Kaspersky Professional Services o partner fidati, sfruttando le API esposte dai prodotti integrati.

Forniamo implementazione completa, supporto per la migrazione senza interruzioni e competenza continua per garantire di ottenere il massimo valore dalla implementazione SIEM.

Kaspersky SIEM

www.kaspersky.it

Per saperne di più

#kaspersky
#bringonthefuture