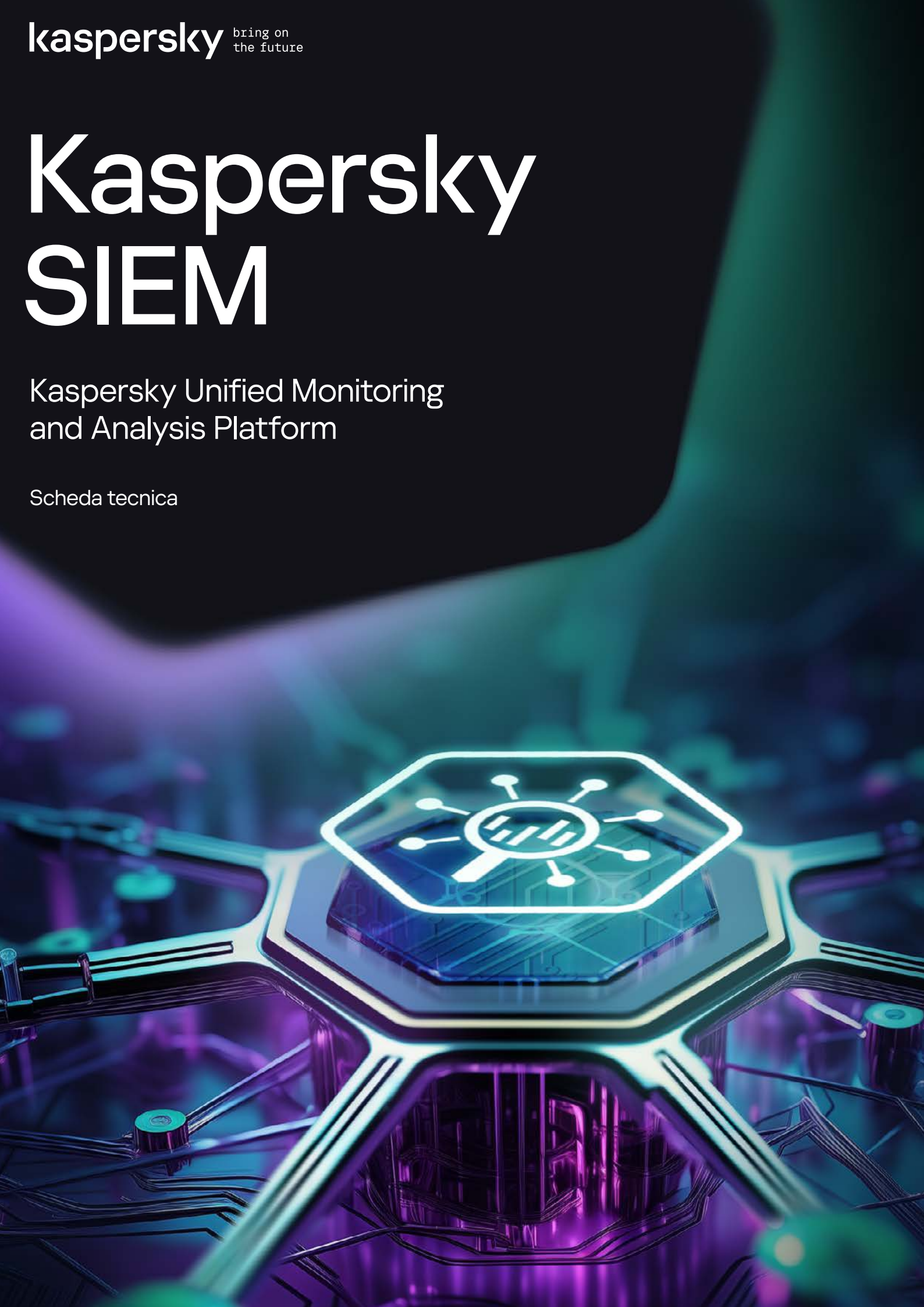
kaspersky bring on the future

Kaspersky SIEM

Kaspersky Unified Monitoring and Analysis Platform

Scheda tecnica



Informazioni su Kaspersky SIEM e sulla sua architettura

Kaspersky Unified Monitoring and Analysis Platform è una soluzione SIEM integrata di nuova generazione per la gestione di eventi e dati di sicurezza. Si distingue per la ricezione, l'elaborazione e l'archiviazione di eventi relativi a informazioni sulla sicurezza e per l'analisi e la correlazione dei dati in entrata. La piattaforma dispone anche di una funzionalità di ricerca, genera avvisi quando vengono rilevate potenziali minacce e supporta risposte automatizzate agli avvisi generati e il threat hunting.

L'architettura modulare ad alte prestazioni consente di elaborare centinaia di migliaia di eventi al secondo (EPS) in ogni istanza e di ridurre il costo di proprietà (TCO) ottimizzando i requisiti di sistema.

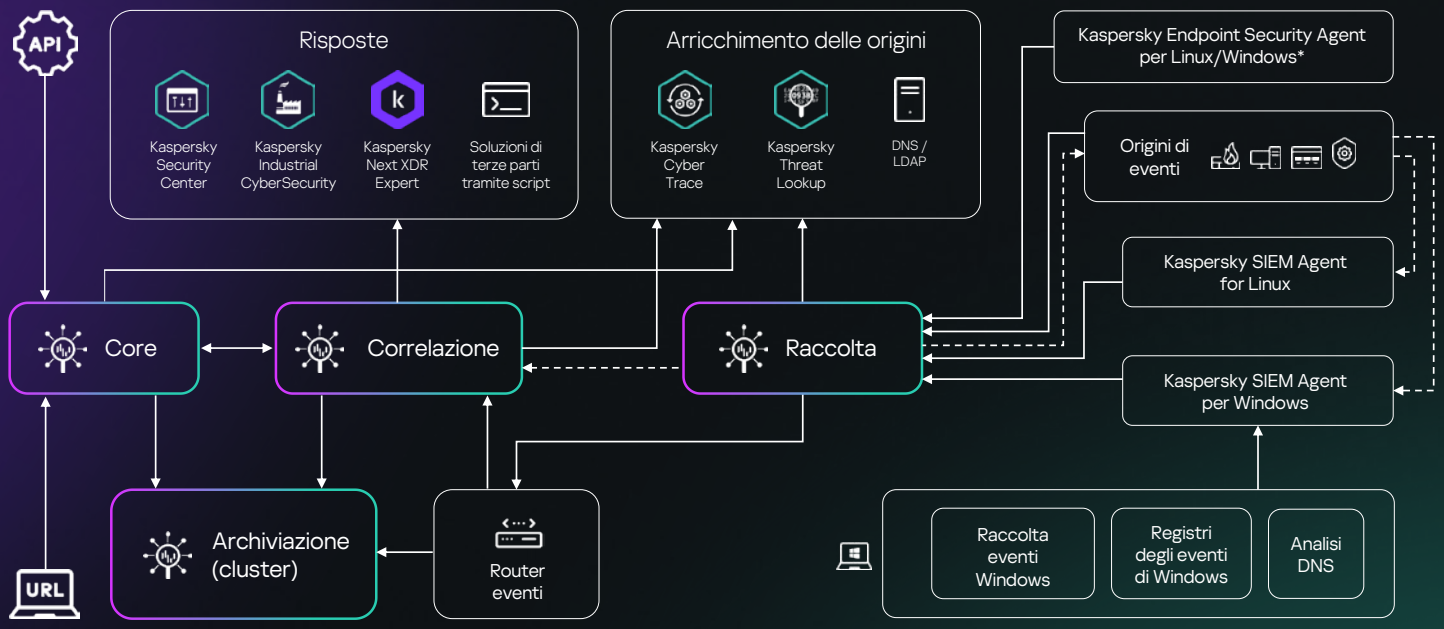
Incorporando prodotti di terze parti e di Kaspersky in un sistema di sicurezza informatico centralizzato, Kaspersky SIEM è una parte essenziale di una strategia di difesa completa in grado di proteggere gli ambienti aziendali e industriali, nonché di rilevare i cyberattacchi che partono dall'IT e passano ai sistemi OT.

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

La soluzione riceve eventi di sicurezza da varie origini, tra cui prodotti Kaspersky, sistemi operativi, applicazioni di terze parti, strumenti di sicurezza e diversi database, correla gli eventi tra loro e li arricchisce con i dati provenienti dai feed di threat intelligence per identificare le attività sospette nelle infrastrutture di rete aziendali e fornire una notifica tempestiva degli incidenti di sicurezza.

Raccogliendo i log di tutti i controlli di sicurezza e correlando i dati in tempo reale, **Kaspersky SIEM aggrega e fornisce tutte le informazioni necessarie per l'indagine e la risposta agli incidenti.**

Inoltre, Kaspersky SIEM consente ai rilevatori di minacce di scoprire minacce precedentemente sconosciute, permettendo agli operatori di analizzare e correlare i dati storici, nonché di stabilire baseline statistiche per identificare le anomalie.



Perché scegliere Kaspersky?

Risparmiate fino al 50% sui requisiti di installazione hardware o virtualizzazione e riducete il TCO con una soluzione modulare ad alte prestazioni, che supera costantemente i tradizionali fornitori SIEM in termini di efficienza dei costi e può gestire centinaia di migliaia di EPS per ogni istanza.

Flessibilità con le nostre opzioni di licenza. Monitoriamo anche il flusso medio di EPS al giorno dopo l'aggregazione e il filtro per limitare i superamenti e non limitare l'accesso a Kaspersky SIEM nel caso in cui si verifichino.

Vantaggi grazie a un'ampia gamma di integrazioni Kaspersky e di terze parti con opzioni di risposta integrate. Altri fornitori non possono eguagliare il nostro livello di integrazione continua con i nostri prodotti, che comprende un'unica interfaccia per l'integrazione di Threat Intelligence, la capacità di utilizzare i nostri sensori endpoint come agenti SIEM e molto altro.

Archiviate i dati in locale in modo conveniente e senza compromessi, senza sforare il budget per un periodo prolungato, grazie alle opzioni di archiviazione hot e cold, che utilizzano ClickHouse e HDFS (Hadoop Distributed File System) o i dischi locali, con la possibilità di effettuare ricerche rapide in entrambe le aree contemporaneamente.

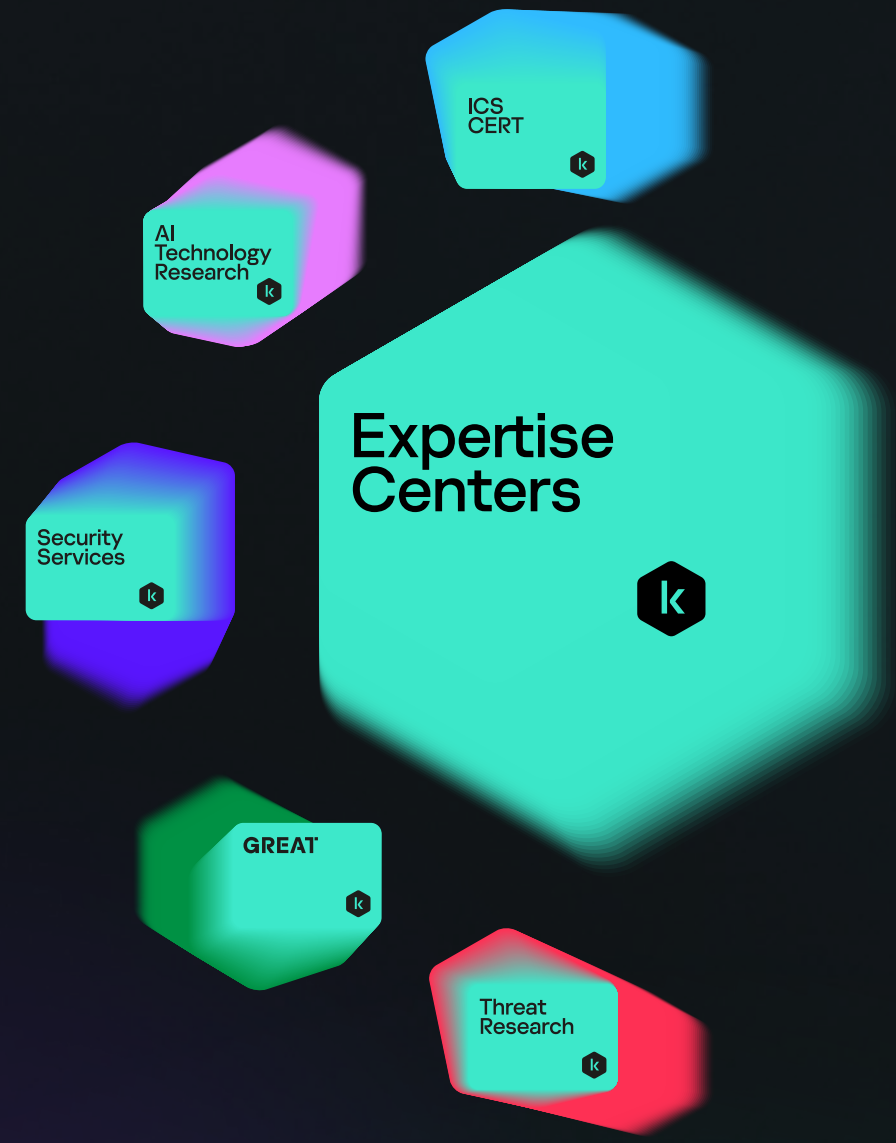
Migliorate la pertinenza dei dati e accelerate rilevamento e triage grazie all'arricchimento con la threat intelligence tattica, operativa e strategica resa disponibile dal nostro team di ricercatori e analisti leader a livello mondiale tramite Kaspersky Threat Intelligence Portal.

Sfruttate la multitenancy integrata con una soluzione adatta per MSSP e grandi imprese, che offre supporto multi-tenant nativo in cui una singola installazione SIEM nell'infrastruttura principale delle organizzazioni consente la creazione di SIEM isolati per tenant che ricevono ed elaborano i propri eventi.

Perché Kaspersky?

Kaspersky SIEM si avvale delle conoscenze e delle competenze accumulate e perfezionate nel corso degli anni dai 5 centri di competenza.

Per saperne di più



27

Da **più di 27 anni** creiamo strumenti e forniamo servizi per tenervi al sicuro con le nostre tecnologie più testate e premiate.

Per saperne di più

Siamo un'**azienda di cybersecurity globale privata** con migliaia di clienti e partner in tutto il mondo, che opera nell'ottica della trasparenza e dell'indipendenza.

Per saperne di più

Kaspersky Unified Monitoring and Analysis Platform

Per saperne di più

www.kaspersky.it

#kaspersky
#bringonthefuture