



Kaspersky SIEM si aggiorna con il rilevamento delle minacce basato su AI e personalizzazione avanzata

Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

La nuova versione 5.5 è dotata di un meccanismo basato sull'intelligenza artificiale per il rilevamento di potenziali compromissioni degli account e offre una maggiore integrità dei dati e funzionalità di personalizzazione avanzate, garantendo alle organizzazioni una sicurezza più solida e flessibile.

Secondo una recente ricerca globale condotta da Kaspersky, le piattaforme SIEM (Security Information and Event Management) rientrano tra le tre soluzioni di sicurezza informatica più richieste dalle aziende che intendono creare un Security Operations Center. Il 40% delle organizzazioni le considera infatti una componente tecnologica essenziale per la realizzazione di una divisione avanzata di sicurezza informatica.

In risposta a questa esigenza del mercato, Kaspersky ha aggiornato regolarmente la propria soluzione SIEM introducendo nuove e rilevanti funzionalità, progettate per abilitare capacità avanzate di rilevamento delle minacce e migliorare la conformità agli standard e alle normative di settore.

Con l'ultimo aggiornamento sono state introdotte le seguenti funzionalità chiave:

Modello flessibile personalizzabile

Il nuovo sistema consente agli utenti di creare, clonare e modificare i ruoli per allinearli in modo più efficace ai flussi di lavoro interni e alle esigenze organizzative. Questo miglioramento garantisce una

maggiore flessibilità , permettendo alle aziende di adattare il sistema alle proprie strutture specifiche.

Correlator 2.0 Beta e rilevamento dei furti di account basato sull'intelligenza artificiale

Il Correlator 2.0, tollerante ai guasti e scalabile orizzontalmente, è ora disponibile in versione beta. Questo aggiornamento introduce significativi miglioramenti in termini di prestazioni e riduce i requisiti hardware.

Integra inoltre funzionalità avanzate, come il rilevamento dei furti di account basato sull'intelligenza artificiale, che analizza le attività di accesso, definisce modelli di riferimento e individua comportamenti anomali, generando avvisi tempestivi in caso di potenziali compromissioni degli account. Questa funzionalità contribuisce a rafforzare la sicurezza e a migliorare l'efficienza operativa delle organizzazioni.

Backup e ripristino degli eventi per garantire l'integrità dei dati e la conformità

La nuova funzionalità supporta l'esportazione dei dati degli eventi in file di archivio sicuri e immutabili, proteggendo le informazioni durante le indagini, gli audit e i processi di conformità normativa e garantendo che i dati rimangano inalterati.

Ricerche di background per migliorare l'esperienza utente

L'elaborazione delle ricerche in background consente agli analisti di avviare query a bassa priorità che vengono eseguite silenziosamente. Questo permette agli utenti di continuare il proprio lavoro senza interruzioni, con i risultati della ricerca disponibili immediatamente al completamento dell'elaborazione, migliorando in modo significativo l'usabilità e l'efficienza operativa.

«In Kaspersky, il nostro impegno costante è quello di perfezionare e ampliare le funzionalità dei nostri prodotti per stare al passo con l'evoluzione delle minacce informatiche. Sfruttando le innovative tecnologie di intelligenza artificiale integrate in Kaspersky SIEM, siamo in grado di semplificare l'analisi di dati complessi e automatizzare i processi essenziali, consentendo ai professionisti della sicurezza informatica di concentrarsi sull'analisi di incidenti sofisticati e sull'implementazione di misure di sicurezza proattive. Questi miglioramenti rafforzano in modo significativo la resilienza organizzativa e garantiscono una protezione solida contro le minacce emergenti», ha dichiarato Ilya Markelov, Head of Unified Platform Product Line di Kaspersky.

Kaspersky SIEM raccoglie, aggrega, analizza e archivia i dati di log dell'intera infrastruttura IT, fornendo un arricchimento contestuale ai team di sicurezza informatica. La piattaforma sfrutta un set di regole dedicate all'analisi del comportamento di utenti ed entità (UEBA), che consente di identificare le deviazioni dai modelli comportamentali stabiliti e di facilitare il rilevamento tempestivo di APT, attacchi mirati e minacce interne. Inoltre, la mappatura delle regole sulla piattaforma viene aggiornata regolarmente per allinearsi alle versioni più recenti di MITRE ATT&ACK.

Per ulteriori informazioni su Kaspersky SIEM è possibile visitare il sito web al seguente link.

Contatti:

Kaspersky

kaspersky@noesis.net

COMUNICATO STAMPA a CONTENUTO PROMOZIONALE

Responsabilità editoriale di Kaspersky

â

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Gennaio 26, 2026

Autore

redazione