



COMUNICATO STAMPA SPONSORIZZATO â?? Kaspersky SIEM si arricchisce: lâ??AI contro il DLL hijacking

Descrizione

(Immediapress) â??

Milano, 24 settembre 2025. Lâ??aggiornamento di Kaspersky SIEM introduce la funzionalitÃ di AI per rilevare i segni di dirottamento delle DLL (Dynamic Link Library), offre lâ??integrazione con Kaspersky Digital Footprint Intelligence (DFI) e Kaspersky Managed Detection and Response (MDR) e garantisce migliori capacitÃ di lavoro con dashboard e report.

Secondo lâ??ultimo report degli analisti MDR di Kaspersky, nel 2024 le Advanced Persistent Threats (APT) hanno colpito in modo significativo unâ??azienda su quattro, con un incremento notevole del 74% rispetto al 2023. I risultati evidenziano che, nonostante i progressi nelle tecnologie di rilevamento automatico, i cybercriminali continuano a sfruttare le vulnerabilitÃ e ad aggirare le difese. Per affrontare queste sfide e migliorare le capacitÃ di rilevamento delle minacce, Kaspersky ha aggiornato la soluzione Kaspersky SIEM integrando nuove e significative funzionalitÃ progettate per migliorare lâ??efficienza complessiva dei sistemi di sicurezza informatica.

Kaspersky SIEM raccoglie, raggruppa, analizza e archivia i dati di log dellâ??intera infrastruttura IT, fornendo informazioni di threat intelligence contestualizzate e utilizzabili. Nellâ??ultimo aggiornamento, questa piattaforma Ã¨ stata migliorata con le seguenti funzionalitÃ :

Protezione avanzata contro il DLL hijacking

Il software legittimo carica numerose librerie durante il funzionamento, che possono essere sfruttate dagli aggressori per eludere il rilevamento ed eseguire attacchi informatici. Per affrontare questa minaccia, Kaspersky SIEM ha introdotto un sottosistema specializzato basato sullâ??intelligenza

artificiale che analizza continuamente le informazioni su tutte le librerie caricate. In caso di sospetta sostituzione, il sistema annota automaticamente l'evento, consentendo ai team di sicurezza di registrare gli incidenti per ulteriori approfondimenti. Per sfruttare questa nuova funzionalità, gli utenti possono semplicemente stabilire una regola di arricchimento DLL Hijacking al collettore o al correlatore, migliorando la capacità del sistema di rilevare e rispondere in modo efficace alle potenziali minacce di sostituzione delle librerie.

Integrazione con Digital Footprint Intelligence e Managed Detection and Response

Kaspersky SIEM offre ora una perfetta integrazione con Kaspersky Digital Footprint Intelligence, consentendo agli utenti di ricevere analisi complete relative ai dati del digital footprint. Questo miglioramento garantisce che le fughe di account utente e password vengano prontamente rilevate, con avvisi automatici generati per facilitare una risposta immediata. Gli incidenti identificati attraverso questa integrazione possono essere ulteriormente analizzati all'interno del sistema SIEM, migliorando la sicurezza complessiva.

Inoltre, la soluzione ora supporta l'importazione automatica degli incidenti dalla console Managed Detection and Response (MDR) direttamente nel SIEM, semplificando l'elaborazione e l'analisi degli incidenti per una gestione delle minacce più rapida ed efficiente.

Analisi comportamentale migliorata

Kaspersky SIEM è stato ulteriormente migliorato con l'integrazione di un set di regole dedicato all'User and Entity Behavior Analytics (UEBA), progettato specificamente per il rilevamento completo delle anomalie nei processi di autenticazione, nell'attività di rete e nell'esecuzione dei processi su workstation e server basati su Windows. Questa aggiunta consente a Kaspersky SIEM di analizzare in modo più efficace le deviazioni dai modelli comportamentali stabiliti, facilitando così l'identificazione tempestiva di APT, attacchi mirati e minacce interne.

Nuove funzionalità per la creazione di report

Le dashboard e i modelli di report possono ora essere condivisi e trasferiti tra le varie installazioni di Kaspersky SIEM, facilitando la collaborazione e garantendo la coerenza tra i diversi ambienti di sicurezza. Questa funzionalità consente inoltre agli utenti di ricevere aggiornamenti direttamente da Kaspersky, assicurando ai team di sicurezza l'accesso ai contenuti più recenti per un'analisi completa della sicurezza informatica aziendale.

Sono stati inoltre introdotti nuovi widget di visualizzazione dei dati che offrono funzionalità avanzate per la presentazione delle informazioni. Gli utenti possono ora visualizzare i dati con l'opzione trend,

combinare più grafici e illustrare le relazioni tra valori diversi, migliorando così la chiarezza e l'efficacia delle informazioni sulla sicurezza.

Inoltre, è stato aggiunto un nuovo widget preconfigurato, che offre la possibilità di creare query raffinate. A questo si aggiunge una funzionalità di drill-down, che consente agli utenti di passare da una dashboard a un'altra preconfigurata per un'analisi più dettagliata.

Maggiore disponibilità e scalabilità

Kaspersky ha introdotto un'architettura distribuita basata su Raft per il SIEM Core, progettata per garantire elevata disponibilità e resilienza. Questo approccio assicura il funzionamento continuo anche in condizioni di carico elevato e consente alle aziende di scalare orizzontalmente con facilità.

Kaspersky migliora continuamente la piattaforma SIEM per garantire che la capacità di rilevamento delle minacce sofisticate sia costantemente potenziata. Il nostro obiettivo è ridurre il carico di lavoro ai professionisti della sicurezza informatica, consentendo loro di dedicare più tempo all'analisi di incidenti informatici complessi e all'implementazione di misure preventive. Sfruttando tecnologie AI avanzate, automatizziamo numerosi processi e velocizziamo l'analisi di grandi volumi di dati. Questo progresso rafforza in modo significativo la sicurezza e la resilienza delle organizzazioni contro le minacce emergenti», ha commentato Ilya Markelov, Head of Unified Platform Product Line di Kaspersky.

Ulteriori informazioni su SIEM, sono disponibili al sito web.

Informazioni su Kaspersky

Kaspersky è un'azienda globale di cybersecurity e privacy digitale fondata nel 1997. Con oltre un miliardo di dispositivi protetti dalle minacce informatiche emergenti e dagli attacchi mirati, la profonda esperienza di Kaspersky in materia di sicurezza e di Threat Intelligence si trasforma costantemente in soluzioni e servizi innovativi per la sicurezza di aziende, infrastrutture critiche, governi e consumatori in tutto il mondo. Il portfolio completo dell'azienda comprende una protezione Endpoint leader, prodotti e servizi di sicurezza specializzati e soluzioni Cyber Immune per contrastare le minacce digitali sofisticate e in continua evoluzione. Aiutiamo oltre 200.000 aziende a proteggere ciò che conta per loro. Per ulteriori informazioni è possibile consultare <https://www.kaspersky.it/>

Seguici su:

[Tweets by KasperskyLabIT](#)

<http://www.facebook.com/kasperskylabitalia>

<https://www.linkedin.com/company/kaspersky-lab-italia>

<https://www.instagram.com/kasperskylabitalia/>

<https://t.me/KasperskyItalia>

Contatti:

Immediapress

Contatto di redazione:

NoesisKaspersky Italia

kaspersky@noesis.net

default watermark

COMUNICATO STAMPA SPONSORIZZATO: Immediapress Ã un servizio di diffusione di comunicati stampa in testo originale redatto direttamente dallâ??ente che lo emette. Lâ??Adnkronos e Immediapress non sono responsabili per i contenuti dei comunicati trasmessi

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Settembre 24, 2025

Autore

redazione