Whitepaper
sul prodotto

Kaspersky SIEM

kaspersky bring on the future

Sommario

Mercato Security Information and Event Management

I responsabili della cybersecurity delle organizzazioni devono affrontare molte sfide, tra cui un numero crescente di tentativi di attacco verso le loro infrastrutture, la carenza di personale addetto alla cybersecurity unite a tecniche, tattiche e procedure di attacco sempre più complessi.

Inoltre, le organizzazioni devono rispettare i requisiti normativi relativi alla conservazione dei dati, ai controlli e all'indagine sugli incidenti, e questo influisce sul mercato globale dei SIEM.

Le organizzazioni sono inoltre costrette a separare gli avvisi relativi ai cyberattacchi in base alla priorità e a classificarli in modo più efficiente dato che stanno diventando sempre più numerosi e complessi.

Inoltre, il lavoro da remoto ha portato le aziende ad adottare applicazioni SaaS e a consentire ai dipendenti di portare con sé i propri dispositivi (BYOD), obbligandole a estendere la visibilità della rete oltre il perimetro tradizionale.

Infine, trovare esperti di sicurezza qualificati è diventato molto difficile nel mercato odierno. Le aziende sono alla ricerca di modi per ottimizzare le proprie risorse e migliorare l'efficienza della cybersecurity. Di conseguenza, le organizzazioni vogliono che i dati di intelligence siano facilmente accessibili e utilizzabili per i team SOC.

Secondo il report Kaspersky Human Factor 360

77% delle aziende ha subito almeno una violazione della cybersecurity, e molte ne hanno subite fino a sei in quel periodo

41% delle aziende ritiene di avere gap nelle proprie infrastrutture di cybersecurity e prevede di aumentare gli investimenti in questo settore in futuro

Per saperne di più

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 ingresso. La piattaforma dispone anche di una funzionalità di ricerca, genera avvisi quando vengono rilevate potenziali minacce e supporta risposte automatizzate e 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.

Includendo 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 centralizzata dei log.

La soluzione riceve eventi di sicurezza da varie sorgenti, tra cui prodotti Kaspersky, sistemi operativi, applicazioni di terze parti, strumenti di sicurezza o 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 quelle precedentemente sconosciute, permettendo agli operatori di analizzare e correlare i dati storici, nonché di stabilire baseline statistiche per identificare le anomalie.

Kaspersky Unified Monitoring and Analysis Platform include i seguenti componenti

Un **core** con un'interfaccia utente grafica centralizzata per il controllo e il monitoraggio delle impostazioni dei componenti del sistema. La piattaforma è accessibile da soluzioni di terze parti tramite l'API.

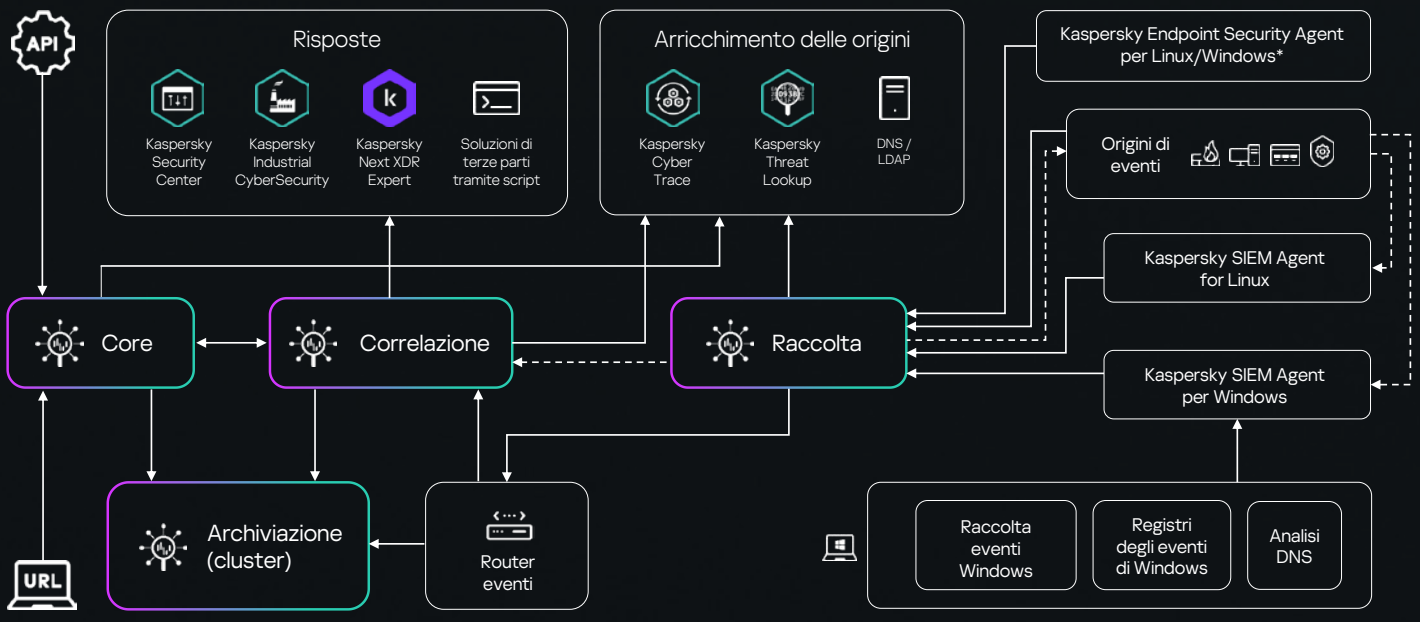
Le regole di correlazione vengono utilizzate per rilevare sequenze specifiche di eventi elaborati e per intraprendere determinate azioni dopo il riconoscimento, come la creazione di eventi/avvisi di correlazione o l'interazione con un elenco attivo. Il **correlatore** utilizza gli elenchi attivi per eseguire le azioni necessarie dopo aver analizzato gli eventi normalizzati ricevuti dai collettori e genera avvisi in base ai criteri di correlazione.

Uno o più **collettori** ricevono gli eventi da origini esterne e li pre-elaborano: normalizzano (convertono in un unico formato), filtrano, aggregano e arricchiscono i dati provenienti da origini esterne utilizzando dizionari, chiamate al servizio DNS e altri strumenti.

L'archivio viene utilizzato per memorizzare gli eventi normalizzati in modo da potervi accedere rapidamente e costantemente dal SIEM per estrarre dati analitici.

Gli agenti inoltrano gli eventi non elaborati da workstation e server ai collettori SIEM. L'invio degli eventi del registro di Windows direttamente al collettore è ora possibile in Kaspersky Endpoint Security for Windows 12.6 o Linux 12.2. Ciò riduce significativamente la quantità di lavoro necessaria per integrare le fonti degli eventi con il sistema SIEM di Kaspersky.

I router di eventi riducono il carico sui collegamenti e il numero di porte aperte sui firewall, ricevendo gli eventi in modo costante e senza ritardi quando i collettori sono installati in uffici remoti con scarsa larghezza di banda o collegamenti dati già occupati.



Funzionalità di Kaspersky SIEM

Connettori integrati e personalizzati per fonti Kaspersky e per sorgenti di terzi con aggiornamenti e regolari.

Integrazione di sorgenti esterne con la creazione gratuita di connettori aggiuntivi da parte del team Kaspersky Professional Services.

Query di ricerca rapide e report pronti sugli eventi di sicurezza.

Archiviazione locale sicura dei log per la conformità alle normative e le indagini sugli incidenti.

Kaspersky SIEM supporta la ricerca di eventi in più archivi per consentire agli operatori di trovare più velocemente e più facilmente gli eventi pertinenti nei cluster di archiviazione distribuiti.

Monitoraggio, elaborazione e archiviazione delle informazioni sugli eventi di sicurezza

Kaspersky Unified Monitoring and Analysis Platform riceve gli eventi dai log e normalizza i dati provenienti da sorgenti di eventi diverse per renderli coerenti. Questi eventi possono includere tentativi di accesso, interazioni con i database o informazioni provenienti da sensori presenti all'interno dell'infrastruttura IT. Anche se un singolo evento potrebbe non sembrare significativo, nel complesso, più eventi singoli disegnano un quadro più ampio di attività dannose che può essere utilizzato per individuare problemi di sicurezza.

Il data lake, il nostro repository locale centralizzato, fornisce una piattaforma per la raccolta, l'indicizzazione e l'analisi dei log provenienti da varie sorgenti, tra cui soluzioni di sicurezza (EPP, FW, IAM, ecc.), sistemi operativi, applicazioni aziendali (sistemi HR, strumenti per l'ufficio), sistemi di sicurezza fisica (sistemi di controllo degli accessi automatizzati) e molti altri dispositivi.

Gli eventi, una volta filtrati e aggregati, vengono trasmessi al correlatore per l'analisi e all'archivio per la conservazione. Per identificare gli avvisi, il collettore riceve gli eventi dalle sorgenti di dati, li elabora e li indirizza all'archivio, al correlatore e/o a servizi di terze parti. Gli eventi non elaborati vengono inoltrati da workstation e server ai collettori SIEM (in alcuni casi dagli agenti) e possono essere inviati ad altri sistemi per ulteriori analisi.

Gli eventi di correlazione vengono generati dalla soluzione quando viene riconosciuto un particolare evento o una serie di eventi correlati, e vengono anch'essi analizzati e conservati. Se un evento o una sequenza di eventi indica una potenziale minaccia alla sicurezza, Kaspersky SIEM genera un avviso con informazioni sulla minaccia e qualsiasi altra informazione pertinente che gli specialisti della sicurezza dovranno poi considerare.

Per trasferire gli eventi tra i componenti, si utilizzano protocolli di trasporto affidabili, con criptaggio opzionale. Il sistema può utilizzare un diodo dati per raccogliere dati da segmenti isolati.

Kaspersky SIEM consente la gestione centralizzata delle risorse fornendo un ampio inventario di server, workstation e dispositivi di rete. La piattaforma può raccogliere dati sulle vulnerabilità delle risorse da origini come gli scanner di vulnerabilità e correlarli con i dati relativi alle categorie di risorse per identificare le minacce. In questo modo i team di sicurezza hanno visibilità sull'intero panorama delle risorse.

A supporto degli analisti, viene visualizzata la copertura della matrice MITRE ATT&CK in base alle regole, per valutare meglio il livello di sicurezza.

Oltre 650 regole di correlazione preconfigurate per il rilevamento degli scenari di attacco, regolarmente aggiornati dai server Kaspersky con la mappatura MITRE e i consigli per la risposta.

Miglioramento della rilevanza dei dati grazie all'arricchimento con i dati analitici raccolti da Kaspersky Threat Intelligence Portal (utilizzando Kaspersky Threat Lookup e Kaspersky CyberTrace).

I dati sulle risorse e sull'infrastruttura vengono raccolti da Kaspersky Security Center o da origini di terze parti.

Gli utenti possono confrontare un evento con valori raggruppati, aggregati, medi, massimi e minimi per un periodo di tempo specifico, utilizzando la funzionalità di data mining di ClickHouse. Questo amplia notevolmente le capacità della logica di rilevamento senza richiedere la creazione di numerose regole di servizio.

Per facilitare la creazione e la modifica dei contenuti, consentiamo agli utenti di sapere in anticipo a quali regole di correlazione si applicherà la modifica prevista, prima di apportare qualsiasi cambiamento ai criteri di filtro.

Correlazione storica e in tempo reale degli eventi di sicurezza

Kaspersky SIEM esegue la correlazione incrociata praticamente in tempo reale utilizzando regole personalizzate per l'identificazione di attacchi e minacce e centinaia di regole predefinite sviluppate da Kaspersky SOC, uno dei team di threat hunting attivi di maggior successo ed esperienza del settore. Gli esperti di Kaspersky SOC hanno conseguito numerosi certificati che ne confermano l'elevato livello di competenze e conoscenze.

Gli eventi vengono **correlati in tempo reale**. Il correlatore analizza gli eventi normalizzati, crea avvisi in base alle regole di correlazione configurate e gestisce le attività o operazioni eventualmente specificate.

Il principio del funzionamento del correlatore si basa sull'analisi dell'evento, vale a dire che ogni evento viene gestito in base alle regole di correlazione specificate dall'utente. Il software genera un evento di correlazione e lo invia all'archivio quando trova una serie di eventi che soddisfano i requisiti della regola. L'utente può adattare le regole di correlazione in modo che siano attivate dai risultati di un'analisi precedente, inviando l'evento di correlazione al correlatore per un'analisi supplementare. I risultati delle regole di correlazione possono essere utilizzati da altre regole di correlazione. Ad esempio, più avvisi secondari possono generare un avviso più importante (più attacchi di forza bruta possono essere analizzati per scoprire un incidente di forza bruta di massa).

La piattaforma utilizza dati storici per identificare le tendenze, trovare minacce precedentemente non identificate e individuare attacchi ignorati da alcuni elementi di sicurezza, migliorando i processi complessivi di rilevamento delle minacce.

Soluzioni di terze parti o prodotti integrati come **Kaspersky Endpoint Detection and Response** eseguono il rilevamento lato endpoint. Regolando le impostazioni dei prodotti, gli utenti possono controllare questo processo e ottenere eventi e dati di telemetria che questi prodotti hanno già elaborato attraverso la propria logica di rilevamento.

Il motore di correlazione della soluzione incorpora il rilevamento lato piattaforma. Grazie al potente motore di correlazione della piattaforma, gli utenti possono creare regole di correlazione adattabili. Sono inoltre disponibili pacchetti di regole e normalizzatori già pronti per supportare prodotti di terze parti in commercio, che vengono costantemente ampliati e aggiornati.

Il principio del funzionamento del correlatore si basa sull'analisi dell'evento, vale a dire che ogni evento viene gestito in base alle regole di correlazione specificate dall'utente. Il software genera un evento di correlazione e lo invia all'archivio quando trova una serie di eventi che soddisfano i requisiti della regola di correlazione.

Rilevamento delle anomalie per scoprire minacce precedentemente sconosciute, consentendo agli operatori di analizzare e correlare i dati storici utilizzando un potente database orientato a colonne.

Per individuare facilmente filtri, dizionari e regole unificati da un unico tag, gli utenti possono utilizzare la funzione di ricerca basata su tag. Il salvataggio della cronologia delle query di ricerca consente all'utente di accedere facilmente alle ricerche precedenti.

La piattaforma può archiviare i dati per un periodo prolungato senza sforare il budget per acquistare hardware di archiviazione costoso grazie alle opzioni di archiviazione cold e hot che utilizzano ClickHouse e Hadoop Distributed File System (HDFS) o i dischi locali.

Gli amministratori possono prevenire i problemi di spazio utilizzando impostazioni flessibili: la profondità dell'archiviazione degli eventi può essere impostata in gigabyte come percentuale dello spazio su disco, o in giorni.

Archiviazione dei dati degli eventi di sicurezza

Il componente di archiviazione di Kaspersky SIEM viene utilizzato per memorizzare gli eventi normalizzati al fine di accedere ai dati analitici in modo rapido e continuo da **Kaspersky Unified Monitoring and Analysis Platform**.

ClickHouse garantisce continuità e velocità di accesso. L'archivio è collegato a un servizio di archiviazione di Kaspersky SIEM tramite un cluster ClickHouse. Ai cluster ClickHouse si possono anche aggiungere dischi di archiviazione aggiuntivi per aumentare il periodo di conservazione del dato.

Gli utenti possono aggiungere spazi nei repository per raggruppare gli eventi archiviati in base a un attributo specifico. In questo modo, gli amministratori possono impostare tempi di archiviazione diversi per gli eventi in base alle loro caratteristiche specifiche.

Kaspersky Unified Monitoring and Analysis Platform gestisce anche la compressione dei dati per ridurre drasticamente l'utilizzo dello spazio su disco senza compromettere il recupero dei dati. La soluzione Kaspersky supporta due aree: una per il recupero rapido dei dati e l'altra per l'archiviazione di una grande quantità di dati.

La piattaforma ha due sezioni distinte: una per l'archiviazione a lungo termine, che può essere realizzata su Hadoop Distributed File System o su dischi locali e l'altra per l'archiviazione operativa attraverso ClickHouse. Questa separazione è trasparente per gli utenti.

Senza dover passare da un archivio all'altro, gli operatori possono creare query di ricerca in un'unica interfaccia e concentrarsi completamente sull'indagine. Questo **riduce il costo di proprietà del sistema**, assicurando al contempo un'esperienza utente eccellente. La piattaforma supporta la ricerca di eventi in più risorse di archiviazione per consentire agli operatori di trovare più velocemente e più facilmente gli eventi pertinenti nei cluster di archiviazione distribuiti.

Le organizzazioni possono essere conformi ai requisiti normativi per la conservazione dei dati, i controlli e l'indagine sugli incidenti raccogliendo e archiviando in modo sicuro i log da diverse origini. Inoltre, grazie all'archiviazione centralizzata e strutturata, le aziende possono facilmente recuperare e analizzare i log in base alle necessità.

Capacità di risposta integrate

Le funzionalità di risposta predefinite che utilizzano i prodotti Kaspersky aumentano l'affidabilità della soluzione di sicurezza. Ad esempio, per estendere le funzionalità di risposta a livello di endpoint, Kaspersky SIEM può essere abbinato a Kaspersky Endpoint Detection and Response per gestire l'isolamento di rete delle risorse e le regole di prevenzione o per eseguire applicazioni e script. Queste azioni di risposta possono essere eseguite manualmente o automaticamente sugli endpoint con l'agente di Kaspersky Endpoint Security.

La raccolta automatizzata di informazioni sull'inventario (software installato, vulnerabilità, apparecchiature, proprietari delle risorse e così via) consente di contestualizzare gli eventi di sicurezza delle informazioni e favorire le indagini sugli incidenti.

Kaspersky SIEM si avvale di Kaspersky CyberTrace, una piattaforma di threat intelligence completa che supporta decine di feed di dati sulle minacce (commerciali e pubblici) per l'arricchimento automatico degli eventi in tempo reale con informazioni contestuali sugli indicatori di compromissione.

Kaspersky Next XDR Expert

Con Kaspersky Next XDR Expert è disponibile un'ampia gamma di funzionalità di risposta tramite playbook.

Per saperne di più

I componenti di intelligenza artificiale di Kaspersky SIEM consentono di rilevare rapidamente le attività sospette nell'infrastruttura.

Strumenti di intelligenza artificiale e machine learning

Kaspersky utilizza algoritmi predittivi, tecniche di clustering, reti neurali, tecniche di modellazione statistica e algoritmi di esperti per aumentare l'efficacia dei nostri prodotti nel rilevare le minacce più rapidamente e nello stabilire in modo accurato la priorità dei rilevamenti.

I team di monitoraggio e risposta sono in grado di stabilire le priorità degli avvisi e di prevenire i potenziali danni, grazie ai big data e ai sistemi di intelligenza artificiale. Il modulo basato sull'IA agevola la classificazione analizzando i dati storici, dando priorità agli avvisi in entrata e fornendo punteggi di rischio basati sull'IA per le risorse. Questo approccio consente di formulare ipotesi valide che possono essere utilizzate per ricerche proattive.

La piattaforma utilizza le regole di correlazione definite dall'utente per collegare gli eventi in tempo reale. Il modulo di correlazione applica algoritmi di intelligenza artificiale per rilevare attività anomale, come picchi di traffico improvvisi o accessi multipli ai servizi, che denotano un potenziale incidente, consentendo un rilevamento tempestivo.

Kaspersky SIEM incorpora anche i dati di Kaspersky Threat Intelligence, generati utilizzando tecnologie di IA e big data. Il database viene continuamente arricchito con i risultati dell'analisi APT manuale, con i dati operativi della Darknet, con le informazioni di Kaspersky Security Network e con le conoscenze derivanti dall'analisi regolare di nuovi malware.

Tutte queste tecnologie consentono agli utenti di ridurre al minimo i danni potenziali causati dagli incidenti informatici e di aumentare i valori MTTR e MTTD.

L'eccellente visualizzazione con dashboard e report presenta i dati nei formati più utilizzabili per identificare tendenze, schemi ed eventi anomali.

Grazie ai widget personalizzabili che consentono di visualizzare facilmente gli indicatori, gli analisti possono stabilire la priorità degli incidenti, determinare le root cause e rispondere alle minacce in modo più efficiente, mentre le organizzazioni possono monitorare l'efficacia delle attività di sicurezza, identificare le tendenze e valutare lo stato generale del sistema di sicurezza.

Gli utenti possono arricchire i dati dei campi evento con i contenuti di dizionari, tabelle, risorse e attributi degli account e utilizzare questi dati per la ricerca e la visualizzazione. In questo modo, dashboard e report vengono creati con dati più contestuali.

Questa soluzione consente agli utenti di creare i propri widget con impostazioni personalizzate, nonché layout con **vari gruppi di widget:**

Metriche chiave degli avvisi

(gravità, priorità e stato)

- Risorse interessate
- Notifiche recenti
- Principali origini dati con il maggior numero di avvisi
- Avvisi allocati a operatori specifici
- Utenti e/o dispositivi interessati
- Avvisi in base ai criteri

Indicatori chiave degli incidenti

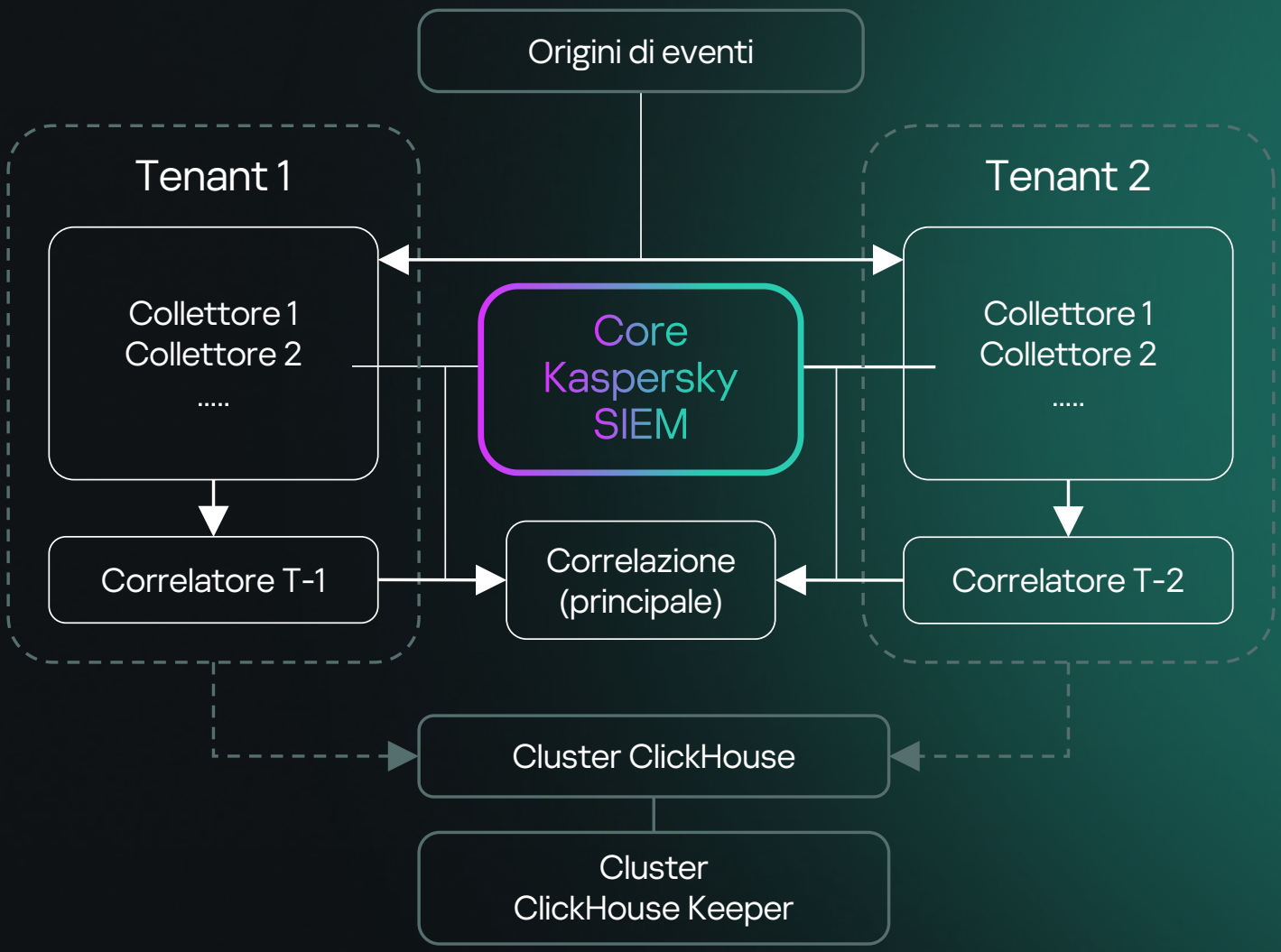
(gravità e assegnazione)

- Dispositivi interessati
- IP esterni e interni principali in base al Netflow Traffic Volume (BytesIn)
- Nodi principali per la gestione remota (porte 3389, 22)
- Byte NetFlow totali per le porte interne
- Origini principali in base al numero di eventi, categorie, risorse e utenti

Architettura multitenancy

Kaspersky SIEM offre supporto completo per i sistemi multi-tenant, vale a dire che gli utenti di un tenant non possono vedere i dati (eventi, avvisi, incidenti, ecc.) di un altro tenant. In modalità multitenancy, una singola istanza dell'applicazione Kaspersky SIEM distribuita nell'organizzazione principale consente l'isolamento delle filiali in modo che ricevano ed elaborino i propri eventi.

Il sistema è amministrato centralmente tramite l'interfaccia principale e i tenant operano in modo indipendente con accesso solo alle proprie risorse, servizi e impostazioni. Gli eventi relativi ai tenant vengono archiviati separatamente. Gli utenti possono accedere a più tenant contemporaneamente. L'amministratore generale può anche specificare quali dati del tenant saranno visualizzati nelle diverse parti dell'interfaccia Web.



La piattaforma offre un sistema basato su filtri per la distribuzione degli eventi negli spazi. L'accesso utente agli eventi ora viene impostato a livello di spazio, consentendo il controllo granulare dell'accesso agli eventi all'interno di un singolo tenant.

Il sistema è gestito centralmente attraverso l'interfaccia principale, mentre i tenant operano in modo indipendente l'uno dall'altro e hanno accesso solo alle proprie risorse, servizi e impostazioni. Gli eventi dei tenant vengono archiviati separatamente.

Ampia gamma di integrazioni pronte all'uso

Kaspersky Unified Monitoring and Analysis Platform è completamente integrato con le soluzioni e le tecnologie Kaspersky per un uso coordinato dei prodotti con una maggiore efficienza. Altri competitor 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.

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response *

Kaspersky Security Center

Kaspersky Secure Mail Gateway

Kaspersky Web Traffic Security

Kaspersky Threat Lookup

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Automated Security Awareness Platform

e molto altro

L'integrazione con il ricco portfolio di servizi di **Kaspersky Threat Intelligence** consente di identificare le minacce e di stabilirne la priorità accedendo rapidamente a informazioni contestuali su nuovi attacchi, indicatori di compromissione assieme alle tecniche e tattiche messe in campo dagli aggressori.

* Include possibili integrazioni con Kaspersky Endpoint Detection and Response Expert, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Next EDR Foundations, Kaspersky Next EDR Optimum, Kaspersky Next EDR Expert

Kaspersky SIEM si distingue per la ricezione di dati (log) da altri sistemi e dispositivi. Per consentire un'implementazione rapida e semplice senza i costi aggiuntivi dovuti alla configurazione di regole per ciascuna sorgente di dato, la piattaforma è dotata di un'ampia gamma di integrazioni immediate per i prodotti Kaspersky e di terze parti:

Per dominio di sicurezza

- Protezione degli endpoint (soluzioni EPP ed EDR)
- Protezione di e-mail e traffico Web (protezione e-mail, NDR, FW/NGFW, UTM, IDS)
- Security Awareness
- Carico di lavoro cloud (CASB, CWPP)
- Threat Intelligence (CTI)
- Protezione dell'identità (IAM, PAM)
- Sicurezza OT/IoT
- Data Loss Prevention (DLP)

Per tipo di dati

- XML
- SysLog
- CSV
- JSON
- SQL
- CEF
- Valore chiave
- RegExp
- NetFlow v5
- NetFlow v9
- IPFIX

Per tipo di trasporto

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse, Elasticsearch)
- File
- Diode
- FTP
- NFS
- WMI
- WEC
- ETW (analisi DNS)
- SNMP
- SNMP Traps
- VMware API
- MS Office 365

Ulteriori integrazioni possono essere sviluppate dal team Kaspersky Professional Services o dai partner, anche utilizzando le API dei prodotti connettibili. Visualizzate l'elenco completo delle origini eventi supportate.

Elenco completo

Per vendor

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMware
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- e così via

Kaspersky Premium Support

Assistenza premium per Kaspersky SIEM

Kaspersky Premium Support per Kaspersky SIEM è disponibile con le licenze Premium e Premium Plus, assicurando una risposta rapida e un'assistenza di alta qualità per qualsiasi problema, per garantire un funzionamento regolare di Kaspersky SIEM

Comunicazione	Assistenza standard	Licenza Premium	Licenza Premium Plus
Account aziendale (portale Web)	●	●	●
Telefono		●	●
E-mail		●	●

Servizio			
Parser personalizzati per Kaspersky SIEM		5	10
Assistenza remota per diagnosticare il problema		●	●
Aumento della priorità delle richieste di assistenza		Alto	Massimo
Applicazione di patch private			●
Servizi TAM (Technical Account Manager) dedicati			●
Report sullo stato da TAM			Rapporto trimestrale

Tempi di risposta			
Problemi critici	Nessuno SLA	2 ore (24/7)	30 min (24/7)
Problemi di alto livello	Nessuno SLA	6 ore (8/5)	4 ore (24/7)
Problemi di medio livello	Nessuno SLA	8 ore (8/5)	6 ore (8/5)
Problemi di basso livello	Nessuno SLA	10 ore (8/5)	8 ore (8/5)

Risposta rapida

La priorità delle richieste viene assegnata in base a SLA rigorosi per una risoluzione dei problemi più rapida e affidabile

Parser personalizzati

I parser personalizzati consentono al SIEM di elaborare formati di log univoci provenienti da sorgenti specifiche

TAM dedicato

Con la licenza Premium Plus, un TAM gestisce tutti i problemi con grande responsabilità

Patch private

La licenza Premium Plus assicura correzioni e patch personalizzate, studiate per problemi specifici

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. Viene preso in considerazione il flusso medio di EPS al giorno dopo l'aggregazione e il filtro per limitare al massimo eventuali sforamenti. Inoltre, non viene limitato 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 il rilevamento e il 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.

Le aziende di tutto il mondo si affidano a Kaspersky Unified Monitoring and Analysis Platform per sviluppare processi di sicurezza delle informazioni completi che migliorano l'efficienza della cybersecurity.

Per saperne di più

Kaspersky ha utilizzato il proprio SIEM per scoprire un malware precedentemente sconosciuto che prende di mira i dispositivi iOS

Durante il monitoraggio del traffico della nostra rete Wi-Fi aziendale dedicata ai dispositivi mobili con Kaspersky Unified Monitoring and Analysis Platform, abbiamo rilevato attività sospette provenienti da diversi telefoni basati su iOS.

Poiché è impossibile esaminare i moderni dispositivi iOS dall'interno, abbiamo creato backup offline dei dispositivi in questione, li abbiamo esaminati con il comando mvt-ios di Mobile Verification Toolkit e abbiamo scoperto tracce di compromissione.

Apple ha risposto rilasciando aggiornamenti di sicurezza per risolvere quattro vulnerabilità zero-day identificate dai ricercatori di Kaspersky:

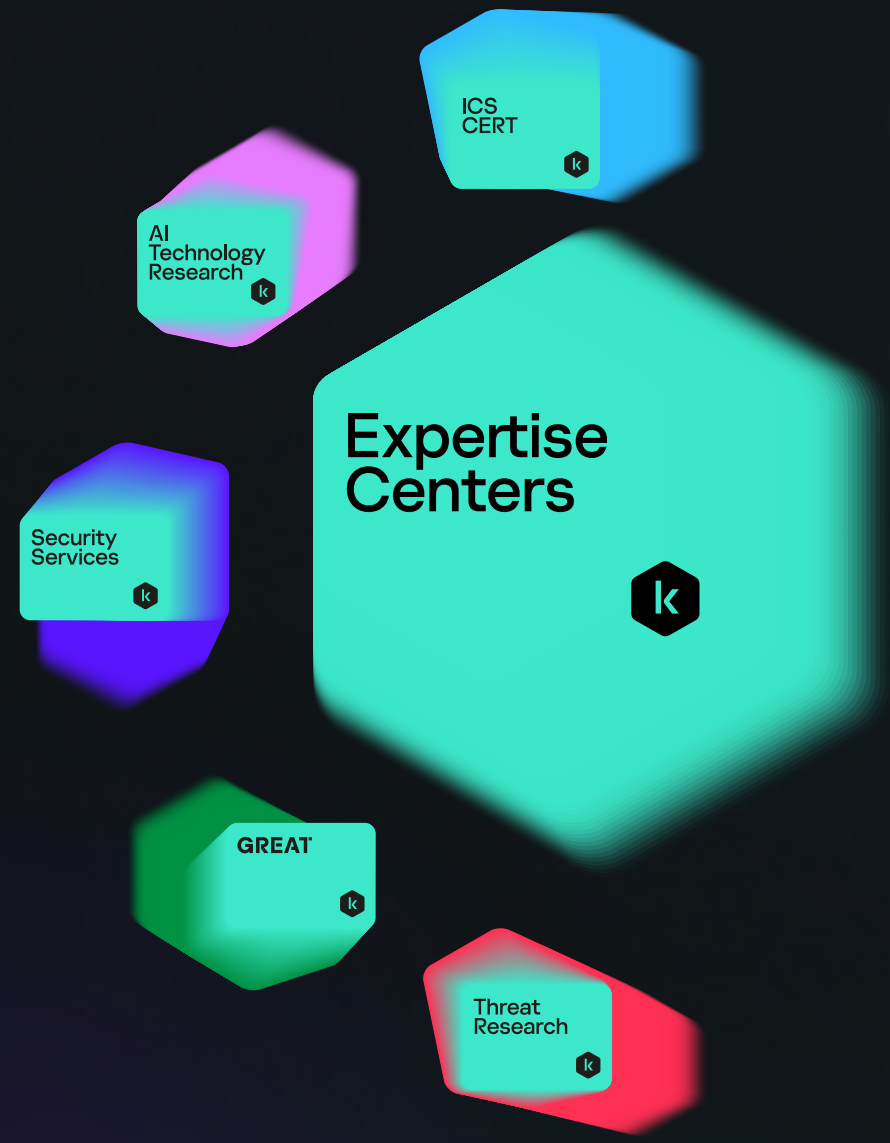
CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990

Queste vulnerabilità riguardano un'ampia gamma di prodotti Apple, tra cui iPhone, iPod, iPad, dispositivi macOS, Apple TV e Apple Watch. Kaspersky ha inoltre informato Apple dell'exploit di una funzionalità hardware, che l'azienda ha successivamente mitigato.

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



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

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

Kaspersky Unified Monitoring and Analysis Platform

Per saperne di più

www.kaspersky.it

#kaspersky
#bringonthefuture