Piattaforma di
Threat Intelligence

Kaspersky CyberTrace

kaspersky bring on the future

Kaspersky CyberTrace

Una piattaforma di Threat Intelligence che consente l'immediata integrazione dei feed di dati con le soluzioni SIEM. Gli analisti possono pertanto sfruttare in modo più efficace le capacità di Threat Intelligence nei flussi di lavoro delle attività di sicurezza già esistenti.

Massima efficacia nel processo di triage e nelle attività di analisi

Il numero di avvisi elaborati dagli analisti di cybersecurity cresce in modo esponenziale. Con una simile quantità di dati da analizzare diviene pressoché impossibile assegnare in modo efficiente le dovute priorità agli incidenti, classificarli e convalidarli.

Troppe notifiche, generate da una moltitudine di prodotti di sicurezza, portano a ignorare avvisi di fondamentale importanza e possono talvolta causare il burnout degli analisti stessi. I sistemi SIEM e altri strumenti di analisi della sicurezza correlano gli eventi e aiutano a ridurre il numero di avvisi, ma non riducono in modo significativo il carico di lavoro degli analisti della sicurezza.

Sistemi SIEM

Grazie all'integrazione delle informazioni di Threat Intelligence costantemente aggiornate nei controlli di sicurezza esistenti (come i sistemi SIEM), i professionisti della sicurezza possono agevolmente automatizzare il processo iniziale di triage e fornire il contesto necessario per identificare immediatamente gli avvisi che richiedono un'analisi approfondita o che vanno inoltrati ai team di incident response per ulteriori analisi.

Il progressivo aumento del numero di data feed e la crescente quantità di fonti di Threat Intelligence disponibili rendono alquanto problematico, per le aziende, poter determinare quali siano le informazioni effettivamente rilevanti. La Threat Intelligence viene fornita in vari formati e comprende un enorme numero di Indicatori di Compromissione (IoC): questo ne rende difficile l'integrazione di queste informazioni all'interno dei sistemi SIEM o dei controlli di sicurezza implementati a livello di rete.

Integrazioni

Kaspersky CyberTrace può essere integrato con qualsiasi feed di dati di threat intelligence nei formati JSON, STIX, XML e CSV:

1. Kaspersky Threat Intelligence Data Feeds
2. Feed di dati di altri vendor
3. Feed OSINT (Open Source INTelligence) o personalizzati

Per assicurare agli utenti una maggiore praticità, CyberTrace supporta anche l'integrazione rapida con numerose soluzioni SIEM e fonti di log.

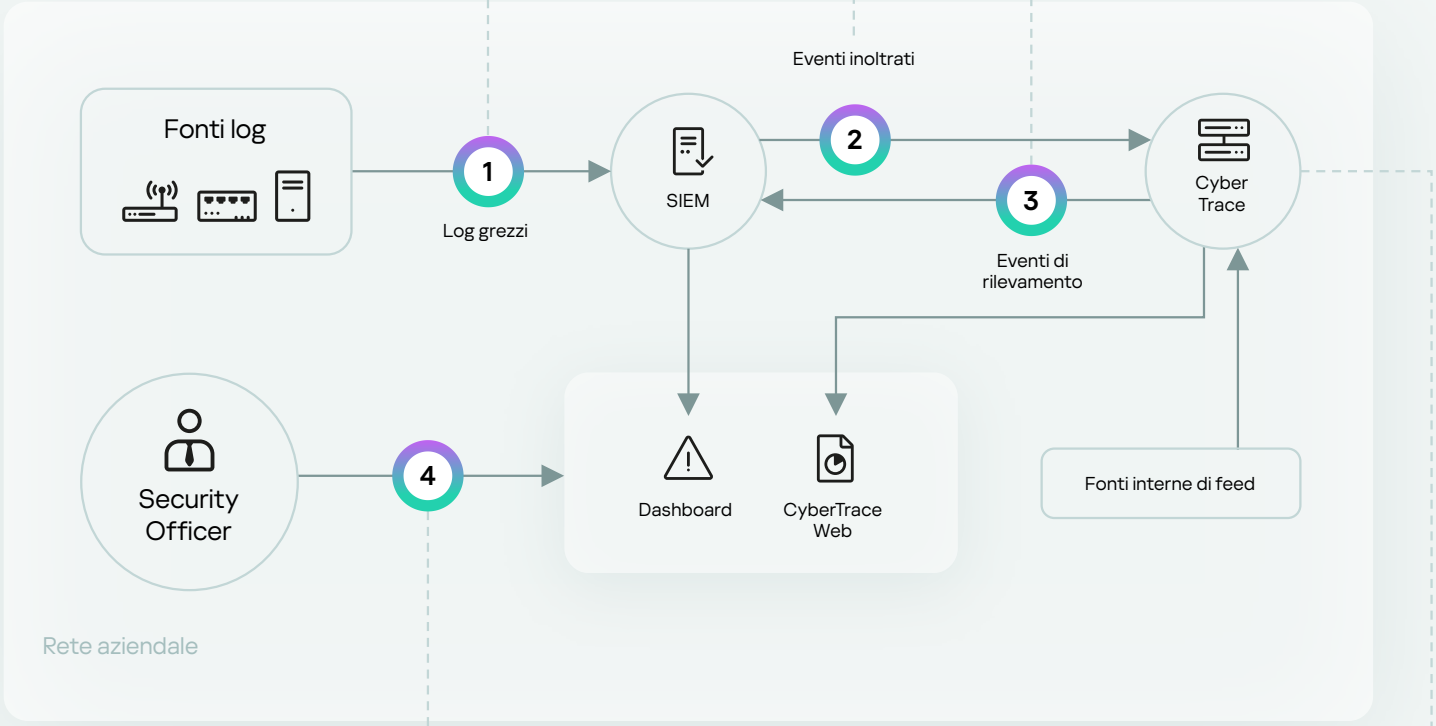
Schema di integrazione del tool Kaspersky CyberTrace

Kaspersky CyberTrace è in grado di migliorare le funzionalità dei SIEM con un ulteriore livello di analisi e corrispondenza dei dati in entrata, riducendo significativamente il carico di lavoro del SIEM. La corrispondenza degli eventi con le informazioni dei feed di dati aiuta a identificare le minacce e a fornire un contesto prezioso agli incidenti rilevati. La figura riportata di seguito mostra un'architettura di alto livello relativamente all'integrazione della soluzione.

SIEM aggrega i log provenienti dai diversi dispositivi (apparati di rete e sistemi IT).

I log con URL, hash e IP vengono inviati a CyberTrace per ulteriori analisi

CyberTrace esegue con rapidità il matching tra eventi in entrata e i data feeds, per poi inviare gli eventi rilevati al SIEM e pubblicare le rilevazioni sull'interfaccia web di CyberTrace



- Consente di visualizzare gli eventi con il relativo contesto di sicurezza e di ricevere avvisi
- Consente di condurre indagini sugli incidenti di sicurezza in base al contesto

Kaspersky Threat Data Feeds, feed commerciali, feed OSINT, feed personalizzati

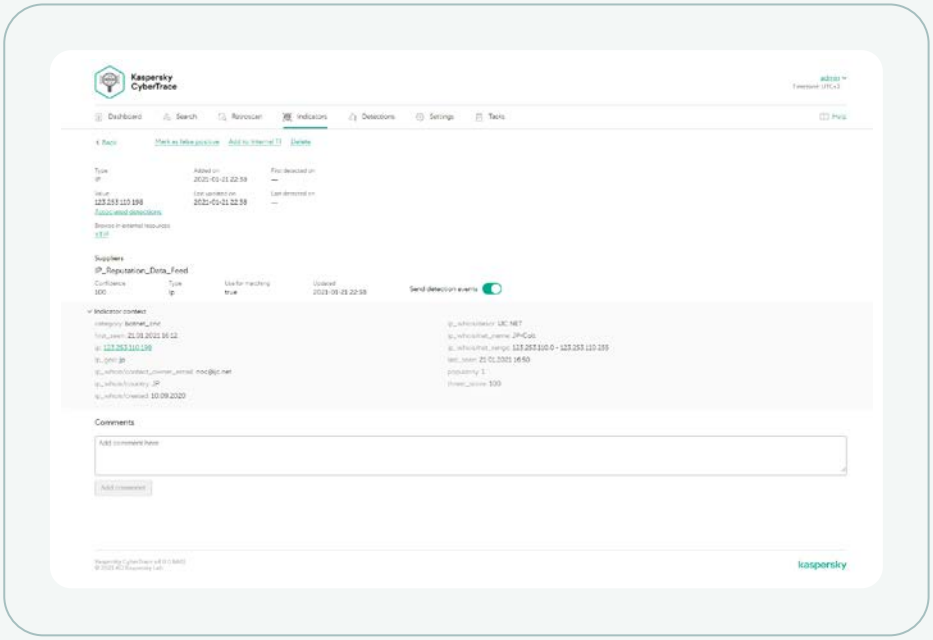
Funzionalità del prodotto

La soluzione Kaspersky CyberTrace fornisce una serie di strumenti atti a rendere pienamente operativa la Threat Intelligence, al fine di poter condurre con efficacia il processo di triage e le attività di risposta iniziali:

Informazioni dettagliate su un indicatore da tutti i fornitori di Threat Intelligence

Un database di indicatori con ricerca full-text e la possibilità di effettuare ricerche complesse tramite query avanzate tra tutti i campi degli indicatori, inclusi i campi contestuali. Il filtro dei risultati provenienti dai fornitori di Threat Intelligence semplifica il processo di analisi delle informazioni.

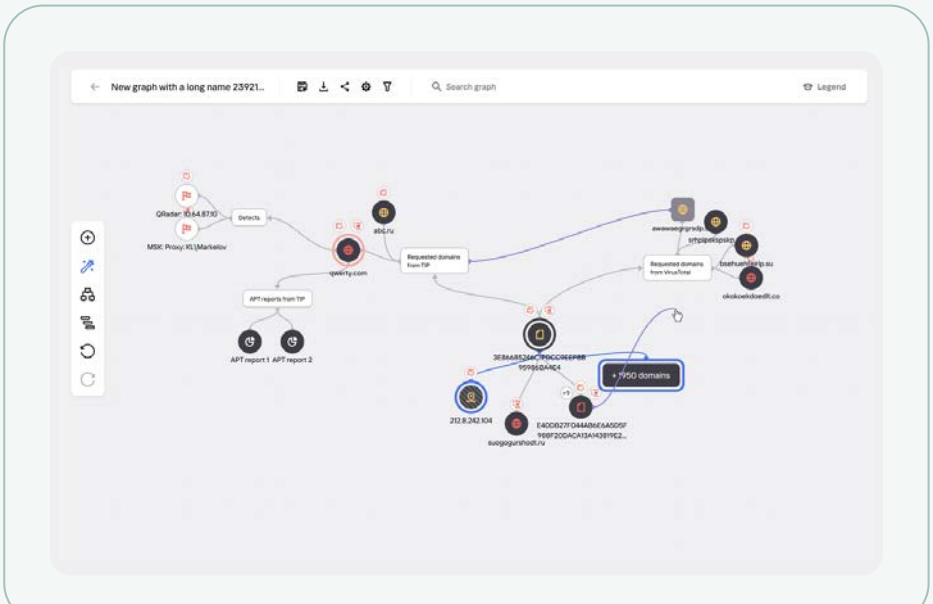
Sottoscrizioni e-mail e documenti PDF di Computer Emergency Response Team (CERT) nazionali/governativi/finanziari, vendor TI e community possono essere utilizzati come fonte di IoC all'interno di CyberTrace. L'estrazione degli IOC è possibile sia dal corpo dell'e-mail che dagli allegati (XML, CSV, JSON, PDF). I server IMAP/POP3 e le cartelle condivise/locali con una raccolta di file PDF possono essere utilizzati come fonte di feed.



Le pagine includono informazioni dettagliate su ciascun indicatore e sono in grado di fornire un'analisi ancora più approfondita. Ogni pagina riassume tutte le informazioni relative a un indicatore ricevute dai diversi fornitori di Threat Intelligence (deduplica) e consente agli analisti di avviare indagini sulle minacce e aggiungere informazioni di Threat Intelligence interne sull'indicatore. Qualora venga rilevato un indicatore, sono disponibili informazioni sulle date di rilevamento e link all'elenco dei rilevamenti.

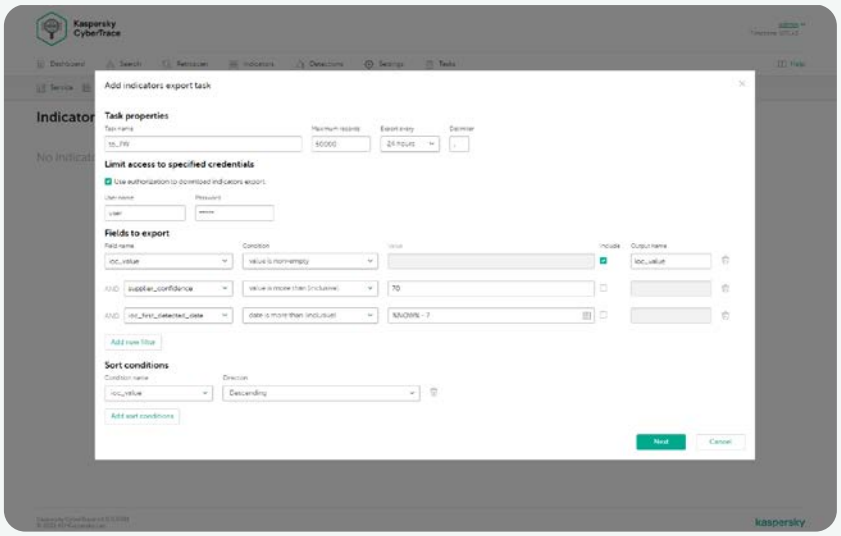
Grafico di ricerca

Un grafico di ricerca consente di esplorare visivamente i dati e i rilevamenti archiviati in CyberTrace e di scoprire le relazioni tra le minacce. Consente la visualizzazione grafica della relazione tra URL, domini, IP, file e altri contesti riscontrati durante le investigation. Il grafico include le seguenti funzionalità: trasformazioni, mini-grafico, raggruppamento di nodi, aggiunta manuale di collegamenti, aggiunta di indicatori e ricerca di nodi nel grafico. È supportata l'integrazione IoC nel grafico di ricerca di VirusTotal.



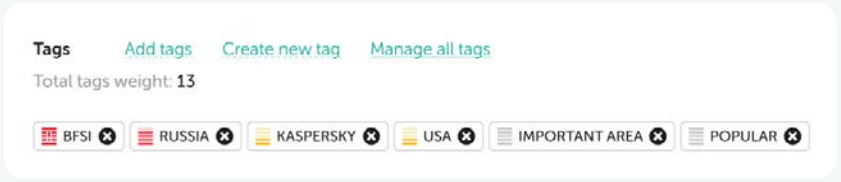
Task di esportazione degli indicatori

La funzione di esportazione degli indicatori supporta l'integrazione nativa degli IoC esportati con controlli di sicurezza di terze parti, ad esempio elenchi di criteri (elenchi di blocco), e avvia la condivisione dei dati sulle minacce tra le istanze di Kaspersky CyberTrace o con altre piattaforme TI.



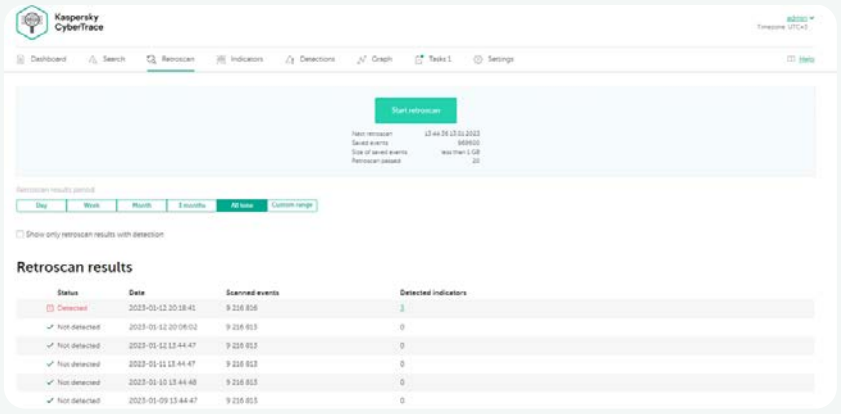
Tag IoC

L'assegnazione di tag agli IoC ne semplifica la gestione. È possibile creare qualsiasi tag, specificarne il peso (l'importanza) e utilizzarlo per assegnare manualmente tag agli IoC. È anche possibile ordinare e filtrare gli IoC in base a questi tag e al relativo peso.



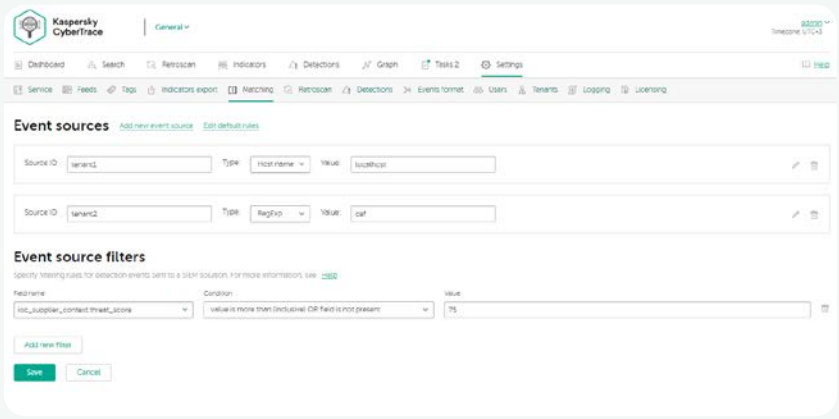
Funzionalità di scansione retroattiva

La funzione di correlazione cronologica (RETROSCAN) consente di analizzare gli eventi precedentemente già verificati utilizzando i feed più recenti per individuare nuove minacce precedentemente sconosciute. Nel report sono inclusi tutti i precedenti rilevamenti effettuati, per eventuali indagini future.



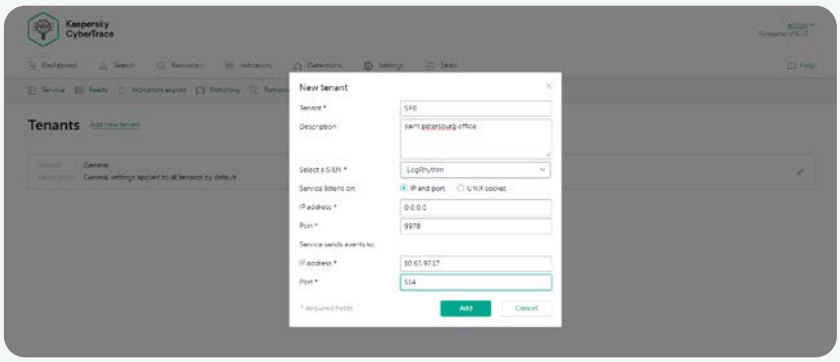
Filtri per le fonti di eventi

Un filtro per l'invio di eventi di rilevamento alle soluzioni SIEM riduce il carico di lavoro sui sistemi e sugli analisti stessi. Consente di inviare al sistema SIEM solo i rilevamenti più pericolosi, ossia quelli da trattare come incidenti. Tutti gli altri rilevamenti vengono salvati nel database interno e possono essere utilizzati durante la Root-Cause Analysis o le attività di ricerca delle minacce.



Supporto multitenancy

La funzionalità multitenancy è stata realizzata per gli MSSP o le aziende Enterprise, nel caso in cui un provider di servizi (sede centrale) abbia necessità di gestire gli eventi provenienti da diverse filiali (tenant) separatamente. In questo modo una singola istanza di Kaspersky CyberTrace può essere connessa a diverse soluzioni SIEM di tenant differenti, ed è possibile configurare i feed da utilizzare per ciascun tenant.



Statistiche sugli indicatori e matrice di intersezione dei feed

Le statistiche sull'utilizzo dei feed, utili per misurare il livello di efficacia dei feed integrati, e la matrice di intersezione dei feed consentono di scegliere i fornitori di Threat Intelligence più appropriati.

L'API REST basata su HTTP consente di cercare e controllare le informazioni sulle minacce

Utilizzando l'API REST, Kaspersky CyberTrace può essere facilmente integrato in ambienti complessi per l'automazione e l'orchestrazione. Integrazione con la piattaforma di monitoraggio, analisi e risposta agli incidenti di Kaspersky.

Altre funzionalità del prodotto

- Connettori per un'ampia gamma di soluzioni SIEM
- Ricerca on-demand di indicatori (hash, indirizzi IP, domini, URL) per indagini approfondite sulle minacce
- Filtro avanzato per i feed
- Scansione di massa per log e file
- Interfaccia grafica o via riga di comando per piattaforme Windows e Linux
- Modalità standalone: Kaspersky CyberTrace riceve e analizza i log provenienti da varie fonti, come i dispositivi di rete
- E molto altro ancora

Kaspersky CyberTrace e Kaspersky Threat Data Feeds si possono utilizzare separatamente, tuttavia il loro impiego congiunto consente di rafforzare sensibilmente la capacità di rilevamento delle minacce. Le attività di sicurezza vengono infatti potenziate grazie all'ottenimento di una visibilità globale sulle cyberminacce.

Con Kaspersky CyberTrace e Kaspersky Threat Data Feeds, le organizzazioni possono:

Selezionare efficacemente gli avvisi di sicurezza e assegnare le corrette priorità.

Ridurre il carico di lavoro degli analisti ed evitare il burnout.

Identificare immediatamente gli eventi di natura critica e decidere in modo più consapevole quali inoltrare o meno ai team di incident response.

Creare difese informatiche proattive basate sulla Threat Intelligence.

Kaspersky CyberTrace

Ulteriori informazioni

www.kaspersky.it

#kaspersky
#bringonthefuture