kaspersky BRING ON THE FUTURE

Kaspersky CyberTrace

Il numero degli avvisi elaborati ogni giorno dagli analisti di sicurezza informatica sta crescendo 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 luci lampeggianti, generate da una moltitudine di prodotti di sicurezza, portano a ignorare avvisi di fondamentale importanza e producono, talvolta, il burnout degli analisti stessi. I sistemi SIEM, al pari degli strumenti utilizzati per la gestione dei log e la conduzione delle necessarie analisi di sicurezza, estremamente utili per aggregare i dati e correlare i relativi allarmi, consentono di ridurre il numero di avvisi e garantiscono ulteriori controlli: in ogni caso, gli analisti di sicurezza continuano a essere sovraccarichi di lavoro.

La Threat Intelligence viene fornita in vari formati e comprende un enorme numero di Indicatori di Compromissione (IoC): questo ne rende difficile l'assimilazione da parte dei sistemi SIEM o dei controlli di sicurezza implementati a livello di rete.

Massima efficacia nel processo di triage e nelle attività di analisi

Integrando informazioni di Threat Intelligence costantemente aggiornate e machine-readable nei controlli di sicurezza esistenti, come i sistemi SIEM, i Security Operation Center possono automatizzare agevolmente il processo di triage iniziale e fornire agli analisti di sicurezza il contesto necessario per identificare immediatamente gli avvisi che richiedono investigation approfondite o che vanno inoltrati ai team di incident response per ulteriori investigation e risposte. Tuttavia, 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'assimilazione da parte dei sistemi SIEM o dei controlli di sicurezza implementati a livello di rete.

Kaspersky CyberTrace è una piattaforma di Threat Intelligence che consente l'immediata integrazione dei data feed con le soluzioni SIEM: in tal modo gli analisti possono sfruttare con maggiore efficacia la Threat Intelligence nei flussi di lavoro delle attività di sicurezza già esistenti. Si integra perfettamente con qualsiasi feed di Threat Intelligence (nei formati JSON, STIX, XML e CSV) che si desidera utilizzare (feed di intelligence sulle minacce elaborati da Kaspersky, altri vendor, OSINT o feed personalizzati), supportando l'integrazione immediata con numerose soluzioni SIEM e molteplici fonti di log.

Kaspersky CyberTrace si avvale di un processo interno per l'analisi e il matching dei dati in entrata, in grado di ridurre significativamente il workload dei SIEM. Analizza log ed eventi in entrata, esegue con rapidità il matching tra dati ottenuti e feed, generando infine i propri avvisi in relazione al rilevamento delle minacce. La Figura riportata sotto mostra un'architettura di alto livello relativamente all'integrazione della soluzione:

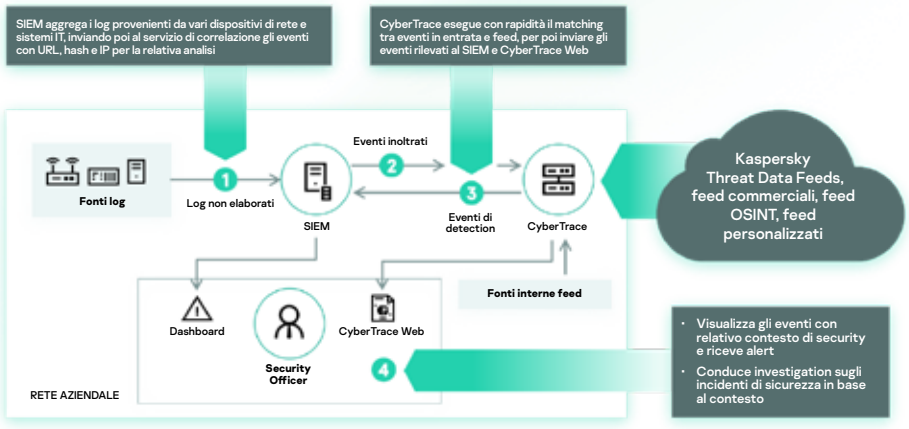

Figura 1. Schema di integrazione di Kaspersky CyberTrace

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:

- 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.
- 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 discussioni 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.

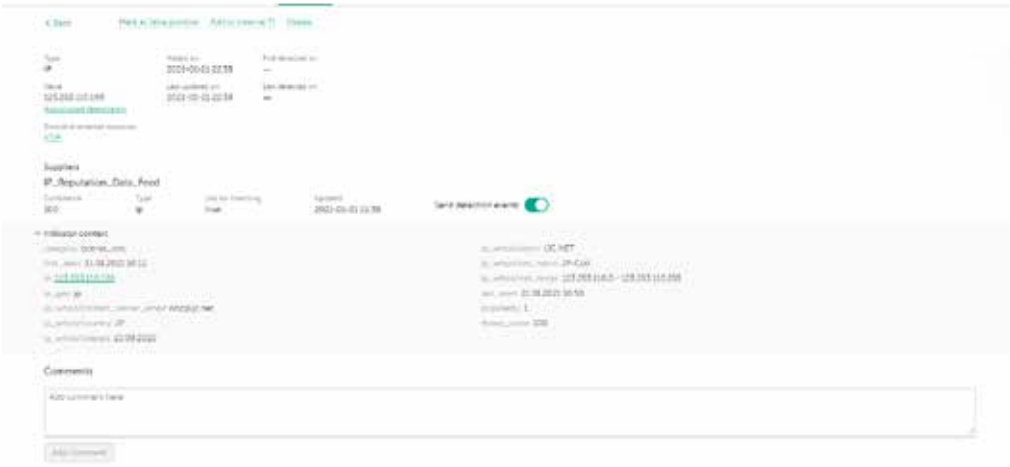

Figura 2. Informazioni dettagliate su un indicatore di tutti dai fornitori di Threat Intelligence

- 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.

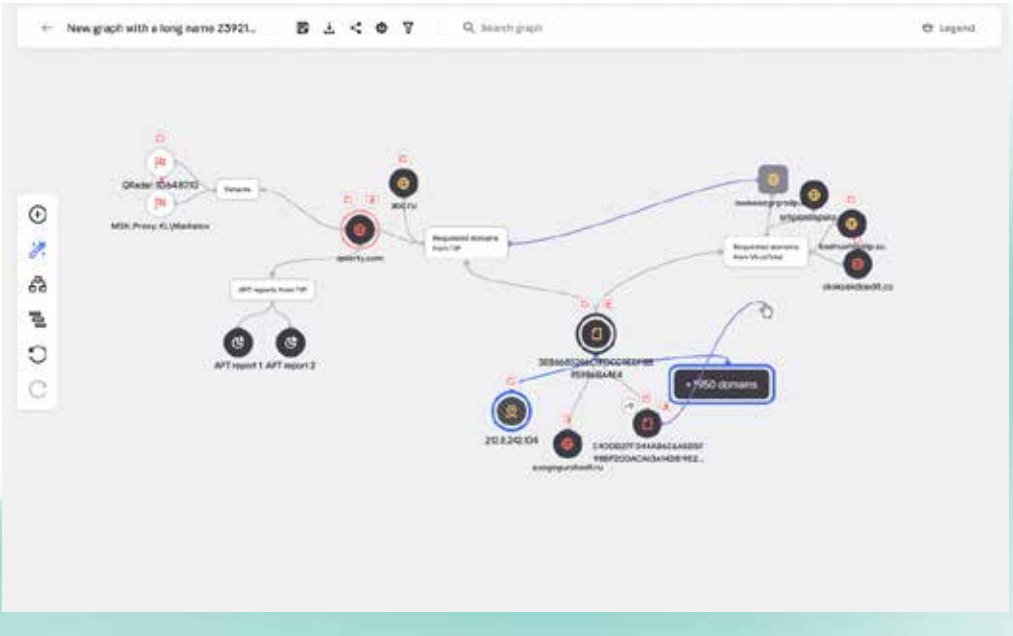

Figura 3. Grafico di ricerca

- La funzione di esportazione degli indicatori consente di esportare set di indicatori nei controlli di sicurezza, 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.

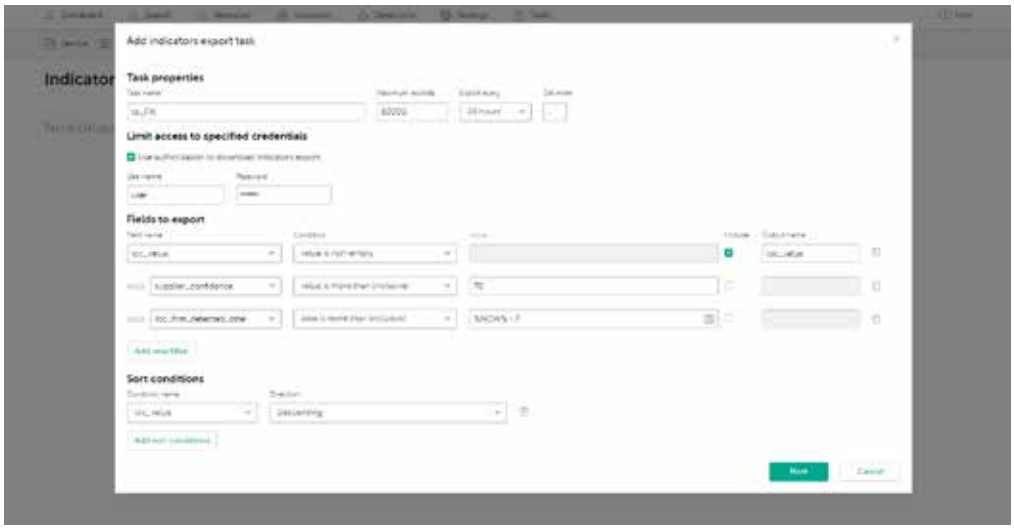

Figura 4. Task di esportazione degli indicatori

- 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.

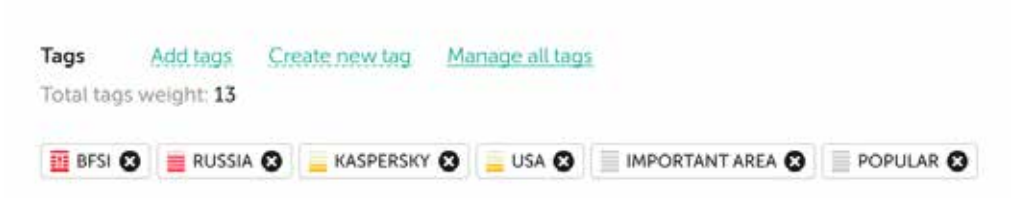

Figura 5. Tag IoC

- La funzione di correlazione cronologica (retrospan) consente di analizzare gli elementi osservabili da eventi controllati in precedenza utilizzando i feed più recenti per individuare le minacce già scoperte. Nel report sono inclusi tutti i rilevamenti cronologici per eventuali investigation future.
- 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 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 threat hunting.
- 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.

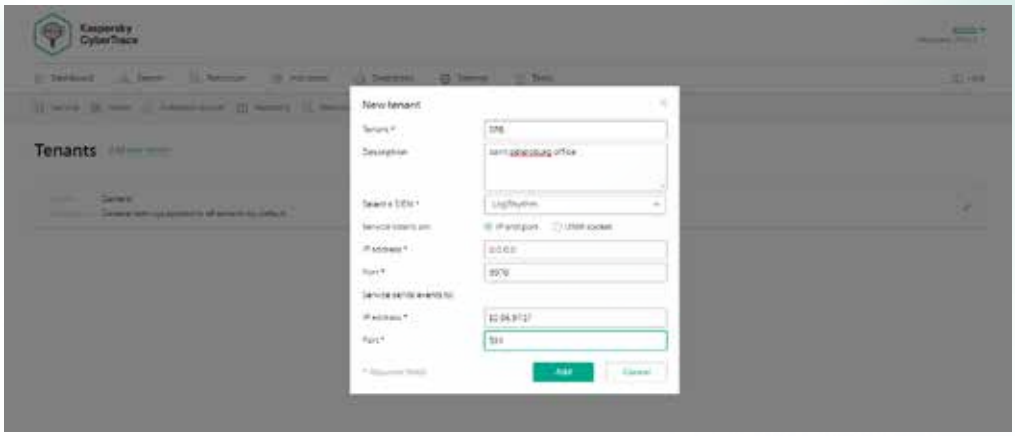

Figura 6. Creazione di nuovi tenant

- 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.

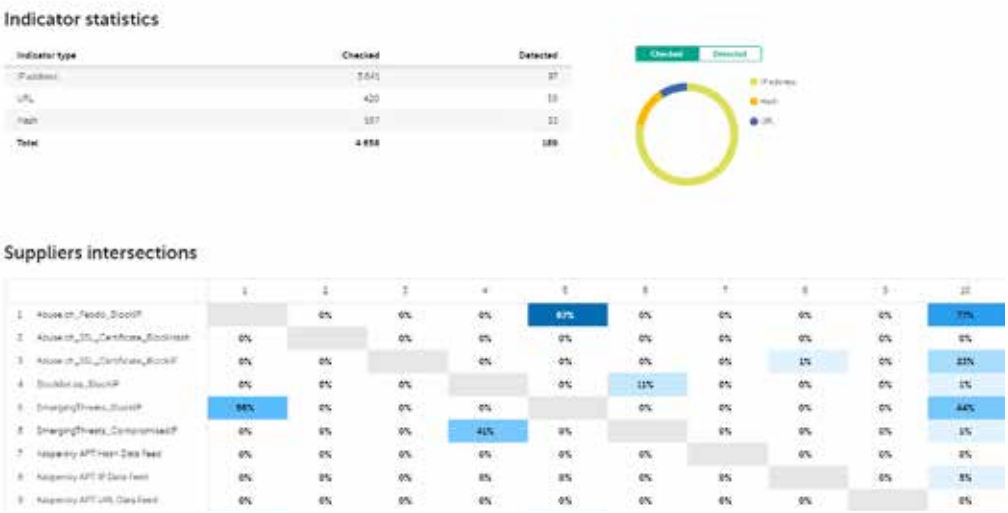

Figura 7. Statistiche sugli indicatori e matrice di intersezione dei feed

Altre funzionalità del prodotto:

- Connettori per un'ampia gamma di soluzioni SIEM, in modo da visualizzare e gestire al meglio i dati inerenti al rilevamento delle minacce
- Ricerca on-demand di indicatori (hash, indirizzi IP, domini, URL) per investigation approfondite sulle minacce
- Filtro avanzato per i feed
- Scansione di massa per log e file
- Interfaccia della 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

- L'API REST basata su HTTP consente di cercare e gestire la Threat Intelligence. Tramite questa API, Kaspersky CyberTrace può essere facilmente integrato in ambienti complessi per la massima automazione e orchestration.
- Supporto dell'integrazione con la piattaforma Kaspersky Unified Monitoring and Analysis (KUMA), compresa l'integrazione della UI web (UI singola).

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 avvisi di natura critica e decidere in modo più consapevole quali inoltrare ai team di incident response
- Creare difese informatiche proattive basate sull'intelligence.

News sulle minacce informatiche: www.securelist.it
IT Security News: business.kaspersky.com
Sicurezza IT per le PMI: www.kaspersky.it/small-to-medium-business-security
Sicurezza IT per le aziende Enterprise: kaspersky.it/enterprise-security
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.it

We are proven. We are independent. We are transparent. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia migliori le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Affidatevi alla cybersecurity per un futuro più sicuro.

Maggiori informazioni sono disponibili all'indirizzo kaspersky.com/transparency

Proven.
Transparent.
Independent.