Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

La sfida

Monitorare, analizzare, interpretare e ridurre le minacce alla sicurezza IT in continua evoluzione è un impegno di enorme portata. Le aziende in tutti i settori lamentano la mancanza dei dati rilevanti e aggiornati di cui hanno bisogno per poter gestire i rischi associati alle minacce alla sicurezza IT.

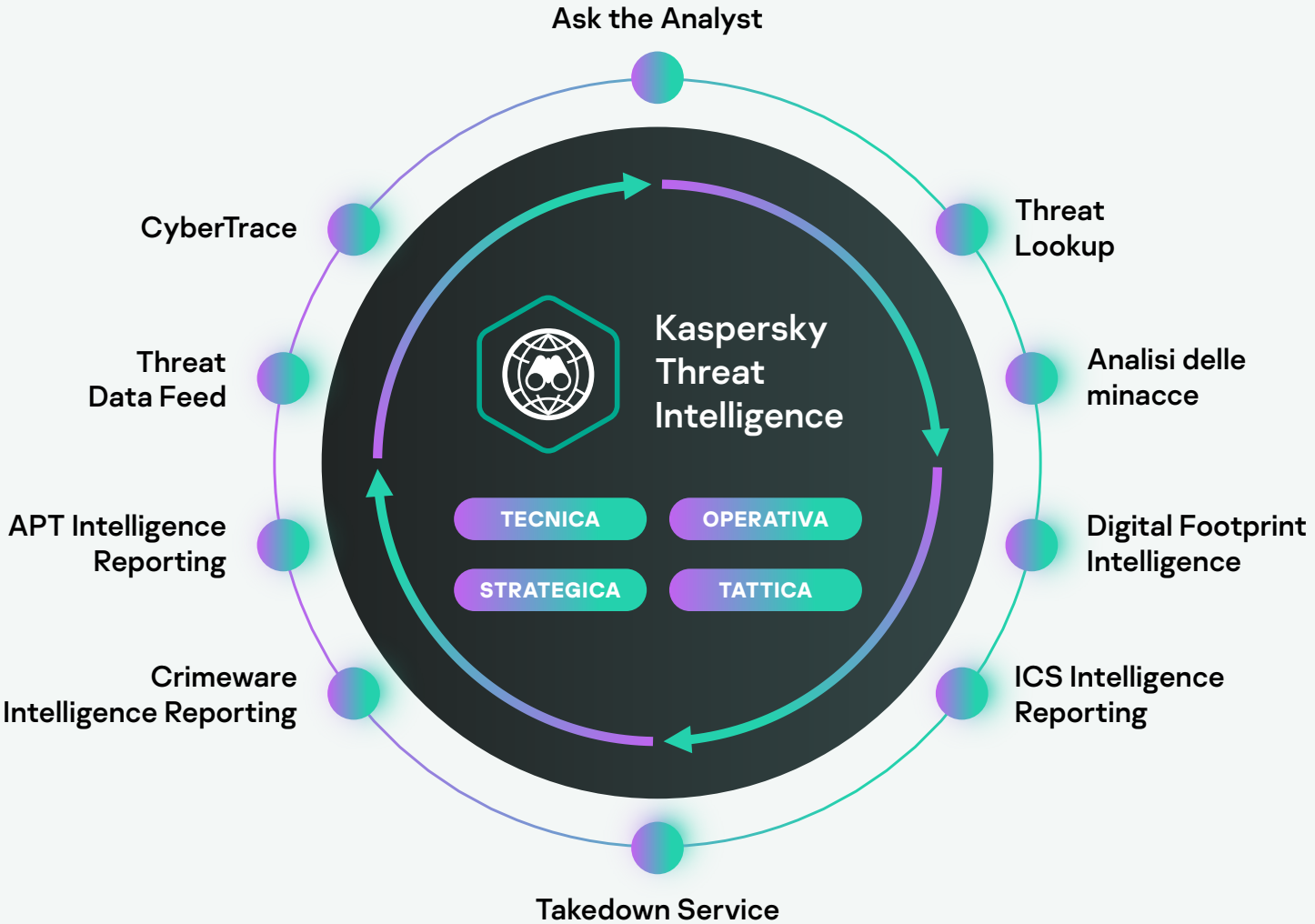
Kaspersky Threat Intelligence

La Threat Intelligence di Kaspersky, messa a disposizione dal nostro team composto dai migliori ricercatori e analisti del mondo, offre l'accesso alle informazioni necessarie per mitigare le minacce informatiche.

Le conoscenze, l'esperienza e le informazioni approfondite di Kaspersky su ogni aspetto della sicurezza informatica ne hanno fatto il partner di fiducia delle più importanti agenzie governative e forze dell'ordine, comprese Interpol e i principali CERT. Kaspersky Threat Intelligence vi dà accesso istantaneo a una Threat Intelligence tecnica, tattica, operativa e strategica.

Il portfolio Kaspersky Threat Intelligence include

Threat Data Feeds, CyberTrace (una piattaforma di Threat Intelligence), Threat Lookup, Threat Analysis (Cloud Sandbox e Cloud Threat Attribution Engine), una gamma di opzioni di reporting di Threat Intelligence e servizi che offrono competenze in ambito di Threat Intelligence su richiesta.



Kaspersky Threat Data Feeds

Gli attacchi informatici possono verificarsi ogni giorno. Le minacce informatiche continuano a crescere in termini di frequenza, complessità e livello di offuscamento, nel tentativo di compromettere le soluzioni di protezione. Gli avversari usano complicate intrusioni a catena, campagne e tattiche, tecniche e procedure (TTP) personalizzate per bloccare i processi aziendali o danneggiare i clienti. Emerge in tutta evidenza la necessità di adottare nuovi metodi di protezione, basati sulla Threat Intelligence.

Integrando nei sistemi di sicurezza esistenti, come ad esempio i sistemi SIEM, SOAR e le piattaforme di Threat Intelligence, feed di Threat Intelligence aggiornati, contenenti informazioni su IP, URL e hash di file sospetti e pericolosi, i team di sicurezza possono automatizzare il processo di triage iniziale e fornire ai relativi specialisti il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite, o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte.

- FEED SULLA REPUTAZIONE DEGLI IP
- FEED SUGLI HASH (WIN/*nix/ MacOS/AndroidOS/iOS)
- FEED SUGLI URL (dannosi, phishing e C&C)
- FEED SUGLI URL RANSOMWARE
- FEED IOC APT
- FEED SULLE VULNERABILITÀ
- FEDD SUL DNS PASSIVO (pDNS)
- FEED SUGLI URL IoT
- FEED SULLE LISTE CONSENTITI
- FEED SUGLI HASH ICS
- E MOLTO ALTRO

Kaspersky Threat Data Feeds

Dati contestuali

Tutti i record presenti nei feed di dati sono corredati da un accurato contesto finalizzato all'azione (denominazione delle minacce, timestamp, geolocalizzazione, risoluzione degli indirizzi IP relativi alle risorse Web infette, hash, livello di popolarità e così via). I dati contestuali consentono di delineare un ampio quadro della minaccia, favorendo e supportando ulteriormente l'utilizzo dei dati su larga scala. Grazie al processo di contestualizzazione, i dati si possono utilizzare in modo ancor più rapido ed efficace: ciò consente di fornire precise risposte alle consuete e indispensabili domande "chi, cosa, dove e quando" per identificare gli avversari, prendere decisioni tempestive e adottare le misure adeguate.

Caratteristiche principali

I feed di dati vengono generati in modo automatico e in tempo reale, sulla base dei risultati di elaborazioni condotte su scala globale (Kaspersky Security Network offre piena visibilità su una considerevole percentuale dell'intero traffico Internet, arrivando a coprire decine di milioni di utenti finali in oltre 213 paesi), garantendo la massima accuratezza e tassi di rilevamento elevati

Implementazione semplificata. La fornitura di documentazione supplementare e specifici esempi, un account manager tecnico dedicato e l'avanzato supporto tecnico di Kaspersky si combinano perfettamente tra loro, consentendo un'agevole e immediata integrazione.

Contribuiscono alla generazione dei feed centinaia di esperti: tra questi, analisti di sicurezza situati in ogni angolo del globo, i rinomati esperti di sicurezza dei team GReAT e dei team che operano in ambito R&S. I responsabili della sicurezza ricevono informazioni critiche e avvisi generati da dati di massima qualità, senza alcun rischio di essere travolti da una valanga di indicatori e avvisi superflui

Raccolta ed elaborazione

I feed di dati vengono aggregati da fonti altamente affidabili ed eterogenee, quali Kaspersky Security Network e i nostri Web crawler, il servizio di monitoraggio botnet (monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno di botnet e delle relative attività e obiettivi), spam trap, partner e team di ricerca.

In tempo reale, dunque, tutti i dati aggregati vengono accuratamente ispezionati e perfezionati tramite diverse tecniche di pre-elaborazione, quali criteri statistici, sandbox, motori di euristica, strumenti di similarità, profilatura del comportamento, convalida da parte degli analisti e verifica delle liste consentiti:

Formati di diffusione leggeri e semplici (JSON, CSV, OpenIoC, STIX) tramite HTTPS, TAXII o appositi meccanismi di distribuzione, supportano in modo efficiente l'agevole integrazione dei feed nelle soluzioni di sicurezza

I feed di dati costellati di falsi positivi sono sostanzialmente inutili. Per questo motivo, prima del rilascio dei feed, vengono applicati test estesi e appositi filtri, al fine di garantire la fornitura di dati controllati al 100%

Tutti i feed sono generati e monitorati da un'infrastruttura ad alta tolleranza di errore, assicurando disponibilità continua

Vantaggi

Rafforzamento delle soluzioni implementate per la difesa della rete aziendale, inclusi SIEM, firewall, IPS/IDS, proxy per la sicurezza, soluzioni DNS, anti-APT, con indicatori di compromissione continuamente aggiornati e contesto di applicabilità, per offrire informazioni approfondite sugli attacchi informatici e fornire una maggiore comprensione dell'intento, delle capacità e degli obiettivi degli avversari. I principali SIEM (inclusi HP ArcSight, IBM QRadar, Splunk e così via) e le piattaforme TI sono pienamente supportati

Miglioramento e accelerazione delle capacità di analisi forense e incident response automatizzando il processo di triage iniziale e offrendo al tempo stesso agli analisti di sicurezza un contesto sufficiente per identificare immediatamente gli avvisi da approfondire o inoltrare ai team di incident response per ulteriori analisi e risposte

Prevenzione dell'esfiltrazione delle risorse sensibili e della proprietà intellettuale dalle macchine infette all'esterno dell'organizzazione. Rilevamento rapido delle risorse infette per proteggere la reputazione del brand, mantenendo il vantaggio competitivo e tutelando le opportunità aziendali

In qualità di MSSP, è possibile far crescere l'azienda grazie a una Threat Intelligence leader di settore offerta ai clienti come servizio premium. Da parte loro, i CERT hanno l'opportunità di potenziare ed estendere considerevolmente le capacità di rilevamento e identificazione delle minacce informatiche

Kaspersky CyberTrace

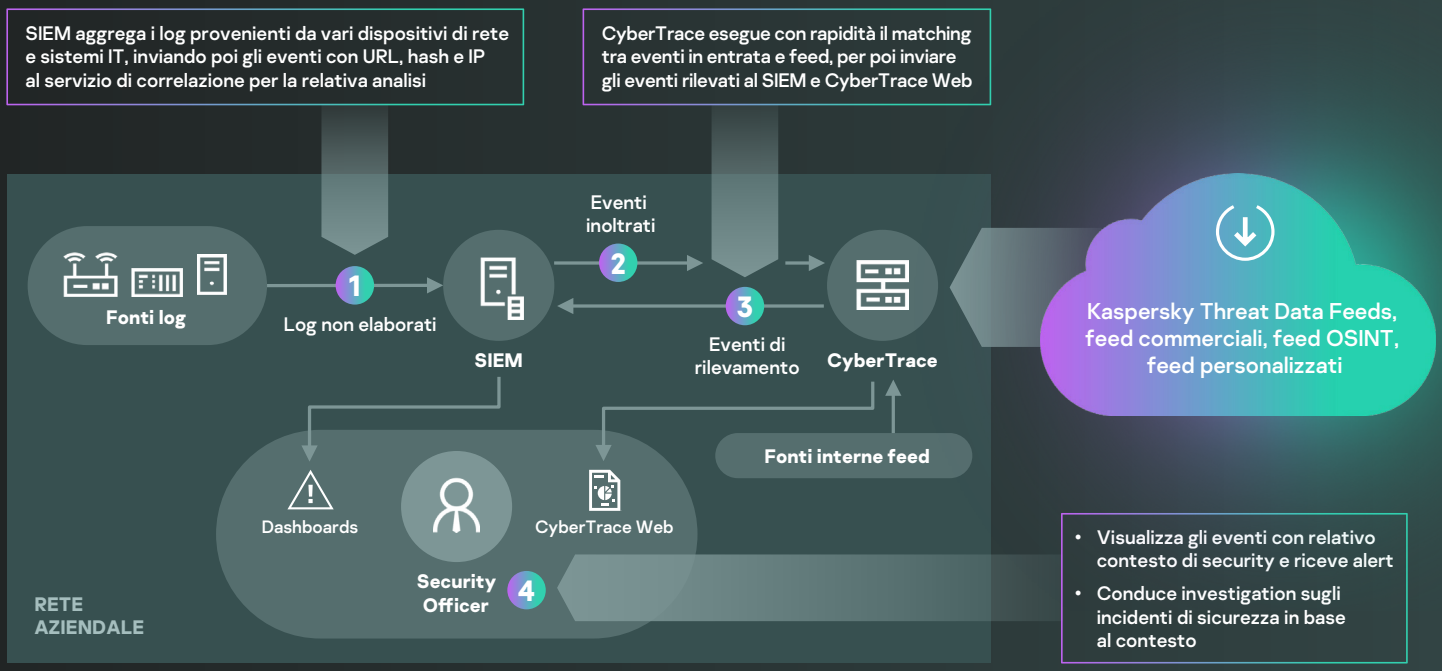
Integrando informazioni di Threat Intelligence costantemente aggiornate e machine-readable nei controlli di sicurezza esistenti, come i sistemi SIEM, i Security Operation Center possono automatizzare agevolmente il processo di triage iniziale e fornire agli analisti di sicurezza il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite o che vanno inoltrati ai team di incident response per ulteriori analisi 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: 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 feed di dati 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 con qualsiasi feed di Threat Intelligence (di Kaspersky, altri vendor, OSINT o feed dei clienti) nei formati JSON, STIX, XML e CSV e supporta l'integrazione immediata con numerose soluzioni SIEM e fonti di log.

Kaspersky CyberTrace offre un set di strumenti per rendere operativa la Threat Intelligence in modo efficiente:

- Un database di indicatori con ricerca full-text e la possibilità di effettuare ricerche complesse tramite query avanzate in tutti i campi degli indicatori, inclusi i campi contestuali
- 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
- Un grafico di ricerca consente di esplorare visivamente i dati e i rilevamenti archiviati in CyberTrace e di scoprire le relazioni tra le minacce
- 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
- 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
- La funzione di correlazione cronologica (scansione retroattiva) consente di analizzare gli elementi osservabili in eventi controllati in precedenza utilizzando i feed più recenti per individuare le minacce già scoperte
- Un filtro invia eventi di rilevamento alle soluzioni SIEM, riducendo il carico, anche sugli analisti
- La multi-tenancy supporta gli MSSP e gli use case delle grandi aziende
- 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
- Il protocollo REST API consente l'integrazione della Threat Intelligence

Lo strumento si avvale di un processo interno per l'analisi e il matching dei dati in entrata: ciò riduce significativamente il workload dei SIEM. Kaspersky CyberTrace analizza log ed eventi in entrata, esegue con rapidità il matching tra dati ottenuti e feed; genera infine i propri avvisi in relazione al rilevamento delle minacce. Il diagramma di seguito mostra un'architettura di alto livello relativamente all'integrazione della soluzione:



Con Kaspersky CyberTrace e Kaspersky Threat Data Feeds, gli analisti di sicurezza ottengono i seguenti vantaggi:

- Efficace selezione di grandi quantità di avvisi di sicurezza e corretta assegnazione delle relative priorità
- Perfezionamento e accelerazione dei processi di triage e risposta iniziale
- Immediata identificazione degli avvisi di natura critica per l'azienda e possibilità di prendere decisioni rilevanti riguardo agli allarmi da inoltrare al team IR
- Creazione di difese proattive basate sull'intelligence

Kaspersky Threat Lookup

Il cybercrime non conosce confini e le capacità tecniche mostrano un rapido miglioramento: gli attacchi diventano sempre più sofisticati e i criminali informatici utilizzano le risorse del Dark Web per raggiungere i propri obiettivi. Le minacce informatiche registrano una costante crescita in termini di frequenza, complessità e tecniche di offuscamento, con un numero sempre maggiore di tentativi di compromissione delle soluzioni di protezione. I cybercriminali, nelle loro campagne, utilizzano complessi attacchi a catena, tattiche, tecniche e procedure personalizzate (TTP) mirate a interrompere le attività aziendali, carpire le risorse o danneggiare i clienti dell'impresa.

Kaspersky Threat Lookup fornisce tutte le conoscenze acquisite da Kaspersky sulle minacce informatiche e sulle relazioni tra di esse, riunite in un unico e potente servizio Web. L'obiettivo è fornire ai team di sicurezza la maggior quantità possibile di dati, per prevenire gli attacchi informatici prima che compromettano l'organizzazione. La piattaforma recupera le informazioni dettagliate più recenti in termini di Threat Intelligence riguardo a URL, domini, indirizzi IP, hash di file, denominazioni delle minacce, dati statistici/comportamentali, dati WHOIS/DNS, attributi di file, dati di geolocalizzazione, catene di download, timestamp e così via. Il risultato è una visibilità globale delle minacce nuove ed emergenti: ciò consente di proteggere al meglio la propria azienda, migliorando sensibilmente qualità ed efficienza delle attività di incident response.

Caratteristiche principali

Intelligence altamente affidabile: un elemento chiave di Kaspersky Threat Lookup è l'elevata affidabilità dei nostri dati di Threat Intelligence. Kaspersky si colloca in testa rispetto ai test condotti sulle soluzioni anti-malware[1], grazie all'impareggiabile qualità della nostra security intelligence e ai tassi di rilevamento estremamente elevati, con falsi positivi vicini allo zero

Ricerca delle minacce: massima proattività nella prevenzione, nel rilevamento e nella risposta agli attacchi, al fine di ridurne al minimo l'impatto e la frequenza. Monitoraggio e tempestiva eliminazione degli attacchi nel minor tempo possibile. Quanto prima viene rilevata la minaccia, tanto minore sarà il danno causato. Quanto più rapidamente vengono prese misure correttive, tanto prima potranno tornare al loro normale funzionamento le attività di rete

Indagini sugli incidenti: un grafico di ricerca ottimizza le indagini sugli incidenti consentendo di esplorare visivamente i dati e i rilevamenti archiviati in Threat Lookup. Offre una visualizzazione grafica della relazione tra URL, domini, file e altri contesti per comprendere meglio l'ambito completo di un incidente e identificarne le cause principali

Ricerca master: consente la ricerca di informazioni in tutte le fonti esterne e i prodotti di Threat Intelligence attivi (inclusi IoC OSINT, Dark Web e Surface Web) in un'interfaccia unica e potente.

Interfaccia Web o API RESTful facili da usare: si può utilizzare il servizio in modalità manuale attraverso un'apposita interfaccia Web (tramite browser Web) o accedervi tramite una semplice API RESTful, a seconda delle preferenze.

Ampia gamma di formati di esportazione: è possibile esportare gli IoC (Indicators of Compromise, indicatori di compromissione) o i dati relativi al contesto finalizzato all'azione nei formati di condivisione machine-readable maggiormente utilizzati e organizzati, come STIX, OpenIOC, JSON, Yara, Snort o addirittura CSV, per ottenere tutti i vantaggi offerti dalla Threat Intelligence, automatizzare il flusso di lavoro operativo o effettuare la relativa integrazione con controlli di sicurezza come SIEM

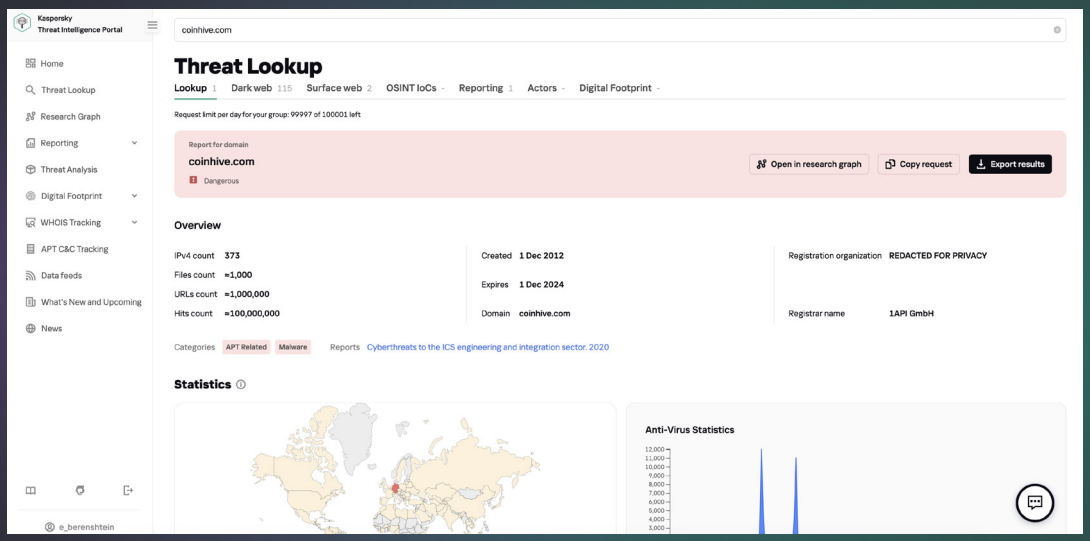
Vantaggi

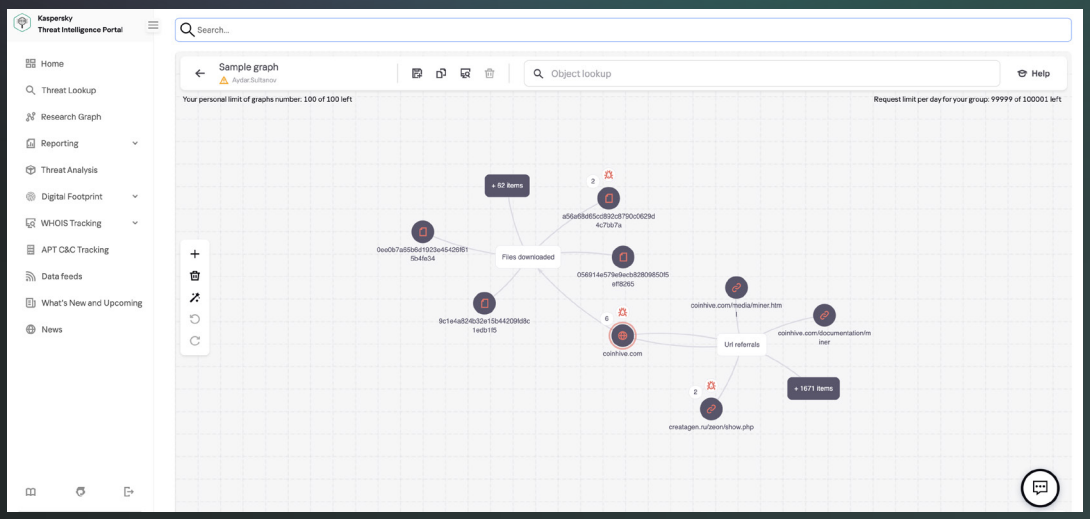
Ricerche approfondite sugli indicatori delle minacce con un contesto comprovato che consenta di assegnare la priorità agli attacchi e concentrarsi sulla mitigazione delle minacce più rischiose per l'azienda

Diagnosi e analisi degli incidenti di sicurezza negli host e nella rete in modo più efficace ed efficiente e assegnazione delle priorità ai segnali dei sistemi interni contro le minacce sconosciute

Ottimizzazione della risposta agli incidenti e delle funzionalità di ricerca delle minacce per interrompere la kill chain prima che vengano compromessi dati e sistemi critici

[1] kaspersky.com/top3





Adesso è possibile

Cercare gli indicatori delle minacce attraverso un'interfaccia basata sul Web o tramite l'API RESTful

Analizzare dettagli avanzati tra cui certificati, nomi comunemente utilizzati, percorsi di file o URL correlati per scoprire nuovi oggetti sospetti

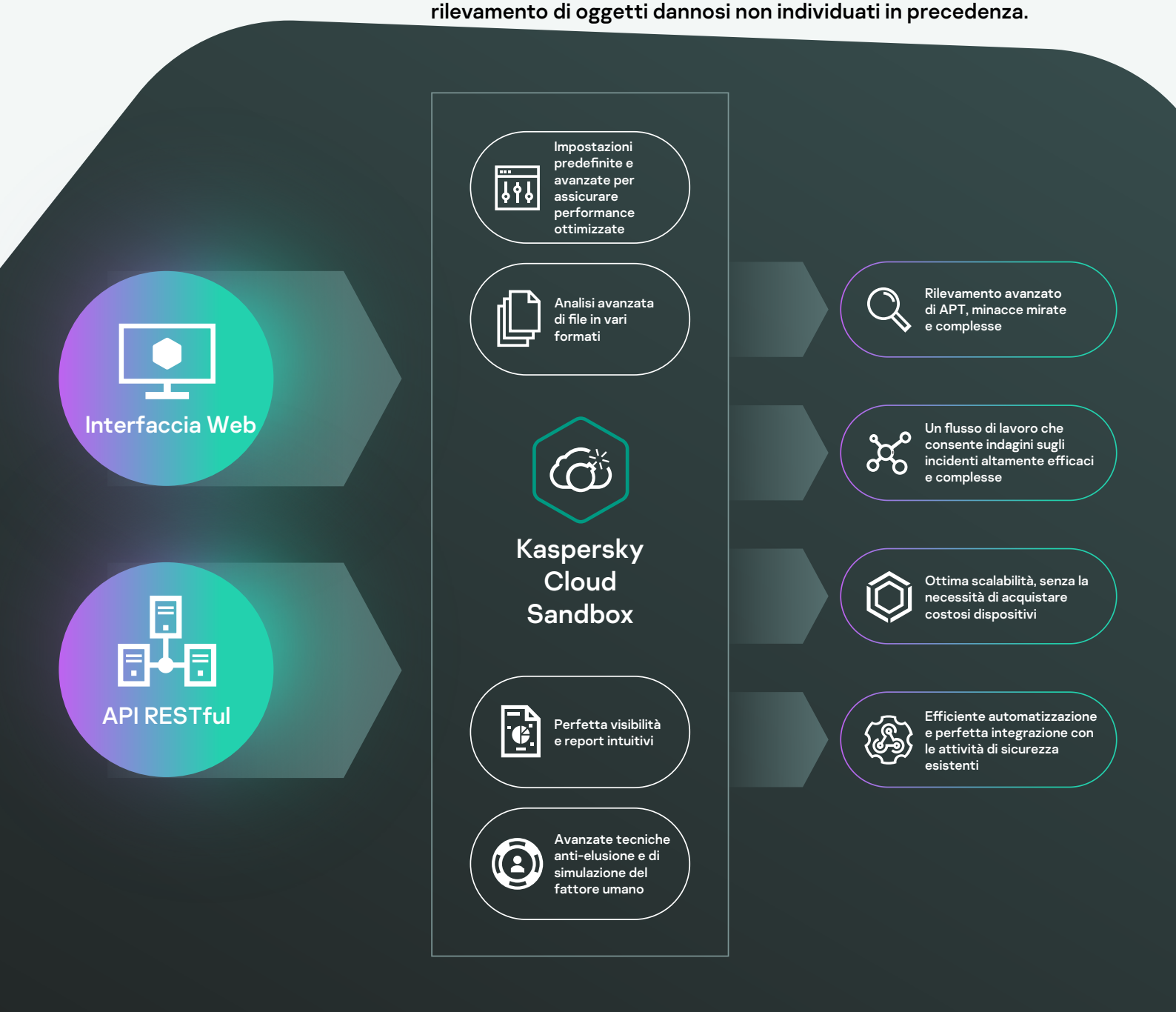
Controllare se l'oggetto rilevato è unico o ampiamente diffuso

Comprendere il motivo per cui un oggetto si deve considerare dannoso

Kaspersky Cloud Sandbox

È di fatto impossibile prevenire gli attuali attacchi di natura mirata avvalendosi esclusivamente dei tradizionali strumenti anti-virus. I motori anti-virus sono in grado di bloccare solo le minacce conosciute e le loro varianti, mentre i sofisticati threat actor fanno uso di tutti i mezzi a loro disposizione per eludere il rilevamento automatico. Le perdite derivanti da incidenti di sicurezza informatica continuano ad aumentare in modo esponenziale, evidenziando la crescente importanza delle capacità di rilevamento immediato degli attacchi, al fine di assicurare una risposta rapida alle minacce e contrastare le stesse prima che si verifichino danni significativi.

Prendere decisioni sulla base del comportamento di un file, analizzando contemporaneamente la memoria di processo, l'attività di rete e così via, rappresenta di sicuro l'approccio ottimale per comprendere al meglio le sofisticate minacce mirate e personalizzate più recenti. Mentre i dati statistici possono non comprendere le necessarie informazioni sui malware modificati di recente, le tecnologie di sandboxing consentono di condurre risolutive investigation sulle origini dei sample di file, eseguire la raccolta di preziosi IoC in base all'analisi comportamentale ed effettuare il rilevamento di oggetti dannosi non individuati in precedenza.



Reporting completo

- Caricamento ed esecuzione di DLL
- Connessioni esterne con nomi di dominio e indirizzi IP
- Creazione, modifica ed eliminazione di file
- Dettagliate informazioni di Threat Intelligence, corredate da contesto finalizzato all'azione, per ogni Indicatore di Compromissione (IoC) rivelato
- Dump della memoria di processo e dump del traffico di rete (PCAP)
- Richieste e risposte HTTP e DNS
- Creazione di esclusioni reciproche (mutex)
- API RESTful
- Modifica e creazione di chiavi di registro
- Creazione di processi attraverso il file eseguito
- Screenshot
- **e molto altro ancora**

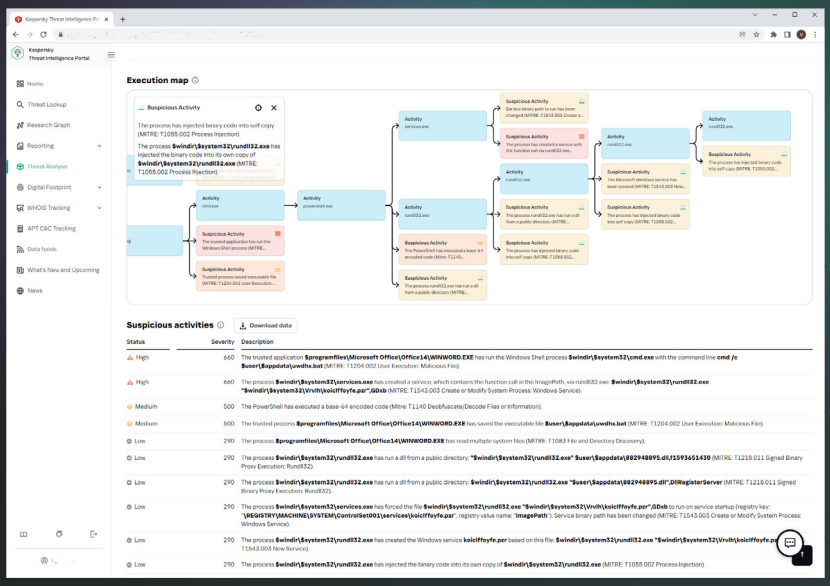
Rilevamento e mitigazione delle minacce proattivi

Il malware si avvale di tutta una serie di metodi per agire senza essere rilevato. Se il sistema non soddisfa i parametri richiesti, il programma dannoso quasi sicuramente si distruggerà da solo, senza lasciare alcuna traccia. Affinché il codice dannoso venga eseguito, l'ambiente di sandboxing dovrà essere in grado di imitare accuratamente il normale comportamento dell'utente finale.

Kaspersky Cloud Sandbox fornisce in tal senso un approccio ibrido, volto a combinare le informazioni di Threat Intelligence ricavate dall'analisi di petabyte di dati statistici (grazie al Kaspersky Security Network e altri sistemi proprietari), l'analisi comportamentale e sofisticate tecniche antievasione con tecnologie in grado di simulare il fattore umano, come il clicker automatico, lo scorrimento dei documenti e processi fittizi.

Questo prodotto è stato sviluppato nel nostro laboratorio di sandboxing interno, evolvendosi per oltre un decennio. La tecnologia unisce tutte le conoscenze relative al comportamento del malware acquisite in oltre 20 anni di ricerca continua sulle minacce. Questo ci consente di rilevare oltre 360.000 nuovi oggetti pericolosi al giorno per fornire ai nostri clienti soluzioni di sicurezza leader di settore.

Nell'ambito del nostro Threat Intelligence Portal, Cloud Sandbox rappresenta il componente principale nel flusso di lavoro in termini di Threat Intelligence. Mentre Threat Lookup recupera le più recenti e dettagliate informazioni di Threat Intelligence riguardo a URL, domini, indirizzi IP, hash di file, denominazioni delle minacce, dati statistici/comportamentali, dati WHOIS/DNS e via dicendo, Cloud Sandbox collega tali conoscenze agli IoC generati attraverso l'analisi dei campioni di malware.



Ora è possibile condurre con elevata efficacia complesse indagini sugli incidenti, per un'immediata comprensione della natura delle minacce: vengono in tal modo acquisite informazioni particolarmente dettagliate, in grado di rivelare le correlazioni esistenti tra i vari indicatori delle minacce.

In genere, quando si deve far fronte ad attacchi multilivello, il processo di ispezione può richiedere un uso estensivo di risorse. Kaspersky Cloud Research Sandbox ottimizza le attività di analisi forense e incident response, garantendo la scalabilità necessaria per l'elaborazione automatica dei file senza la necessità di acquistare costose apparecchiature o preoccuparsi delle risorse di sistema.

Kaspersky APT Intelligence Reporting

I clienti Kaspersky APT Intelligence Reporting usufruiscono dell'accesso costante ed esclusivo alle indagini e ai rilevamenti, inclusi i dati tecnici completi (in un'ampia gamma di formati) su ogni attacco APT rilevato, nonché sulle minacce che non verranno mai rese pubbliche. I report contengono una sintesi con informazioni immediate e rilevanti che illustrano l'APT oltre a offrire una descrizione tecnica dettagliata dell'APT con le relative regole YARA e IOC per offrire ai ricercatori di sicurezza, agli analisti malware, ai security engineer, agli analisti di sicurezza di rete e ai ricercatori APT dati applicabili che consentono una risposta accurata e veloce alle minacce.

I nostri esperti avvisano immediatamente di eventuali modifiche rilevate nelle tattiche dei gruppi di criminali informatici Sarà inoltre garantito l'accesso al database completo dei report APT, un altro potente strumento di analisi e ricerca in ambito di difese di sicurezza.

Vantaggi

MITRE ATT&CK
Tutte le TTP descritte nei report risultano mappate in MITRE ATT&CK: ciò consente la conduzione di attività di rilevamento e risposta ancor più efficaci, grazie allo sviluppo dei relativi use case in termini di monitoraggio della sicurezza, con assegnazione delle indispensabili priorità. La specifica metodologia consente inoltre di effettuare accurate analisi delle eventuali lacune di sicurezza e di testare le attuali difese informatiche in relazione a determinate TTP

Informazioni sugli APT non pubblici
Per diversi motivi, non tutte le minacce di alto profilo vengono rese note pubblicamente, ma vengono condivise con i nostri clienti

Accesso privilegiato
Ricezione di descrizioni tecniche sulle minacce più recenti durante le indagini in corso, prima del rilascio al pubblico

Analisi retrospettiva
Durante il periodo di validità dell'abbonamento, è disponibile l'accesso all'archivio dei report privati

Accesso ai dati tecnici
È incluso un ampio elenco di IoC, disponibile in formati standard quali OpenIOC o STIX, e l'accesso alle regole YARA

Profili degli autori delle minacce
Sono inclusi il presunto paese di origine e l'attività principale, le famiglie di malware utilizzate, i settori e le aree geografiche colpite e le descrizioni di tutte le TTP utilizzate, con mappatura in MITRE ATT&CK

Monitoraggio continuo delle campagne APT
Accesso all'intelligence applicabile durante le indagini con informazioni sulla distribuzione APT, IOC, infrastrutture di controllo e comando e così via

API RESTful
Automatizzazione e integrazione immediate con i flussi di lavoro di sicurezza esistenti

Kaspersky Digital Footprint Intelligence

Parallelamente alla crescita del business aziendale si registra un aumento della complessità e della distribuzione degli ambienti IT. Tale situazione pone di fronte a una sfida particolarmente impegnativa: come proteggere efficacemente un'ampia presenza digitale senza il controllo diretto o l'effettiva proprietà. Gli ambienti dinamici e interconnessi consentono alle aziende di trarre vantaggi significativi. Tuttavia, la crescente interconnessione contribuisce ugualmente ad aumentare la superficie di attacco. Gli autori degli attacchi dimostrano un'abilità sempre maggiore: si rivela quindi di fondamentale importanza disporre di un quadro ampio e dettagliato riguardo alla presenza online dell'azienda. Allo stesso tempo, è essenziale monitorarne i progressivi cambiamenti e saper reagire prontamente alle informazioni costantemente aggiornate in relazione agli asset digitali esposti alle minacce.

Anche se le organizzazioni fanno uso di una vasta gamma di strumenti di sicurezza nelle proprie attività di sicurezza informatica, persistono numerose minacce digitali, associate all'effettiva capacità di rilevare e mitigare le attività di possibili insider, oppure i piani e gli insidiosi schemi di attacco dei criminali informatici che popolano i forum del Dark Web. Per aiutare gli analisti di sicurezza a scoprire in che modo l'avversario intende compromettere le risorse dell'azienda, consentendo loro di individuare prontamente i potenziali vettori di attacco di cui dispongono i criminali informatici e adeguare di conseguenza le difese, Kaspersky ha creato la soluzione Kaspersky Digital Footprint Intelligence.

Qual è il miglior modo per lanciare un attacco alla vostra organizzazione? Qual è il metodo di attacco più efficiente e vantaggioso in termini di costi? Quali sono le informazioni di cui dispone un criminale informatico che intende prendere di mira la vostra azienda? La vostra infrastruttura è già stata compromessa a vostra insaputa?

Kaspersky Digital Footprint Intelligence risponde a queste e a molte altre domande. I nostri esperti creano un quadro completo sullo stato dell'attacco, identificando i punti deboli da migliorare e mettendo in luce le prove relative agli attacchi avvenuti in passato, agli assalti attuali e a quelli pianificati per il futuro.

Il prodotto fornisce:

- Inventario a livello di perimetro di rete, mediante l'utilizzo di metodi non intrusivi, per identificare le risorse di rete e i servizi del cliente esposti al rischio informatico, ovvero i potenziali entry point per eventuali attacchi: interfacce di gestione inavvertitamente lasciate nell'area perimetrale, servizi dalla configurazione errata, interfacce di dispositivi, ecc.
- Analisi su misura delle vulnerabilità esistenti, con assegnazione del relativo punteggio e valutazione completa del rischio in base al punteggio CVSS; eventuale presenza di exploit pubblici, esperienza a livello di penetration test e posizione delle risorse di rete (hosting/infrastruttura).
- Identificazione, monitoraggio e analisi di eventuali attacchi mirati attivi o assalti in fase di pianificazione, campagne APT volte a colpire l'azienda o il settore e l'area geografica in cui l'impresa svolge le proprie attività di business.
- Identificazione delle minacce IT indirizzate a clienti, partner e abbonati, i cui sistemi infetti potrebbero essere utilizzati per un attacco diretto alla vostra azienda.
- Monitoraggio discreto di siti pastebin, forum pubblici, blog, canali di messaggistica istantanea, forum e community segreti con accesso limitato, per scoprire account compromessi, fughe di informazioni o l'eventuale discussione e pianificazione di attacchi rivolti alla vostra azienda.

Caratteristiche principali

Kaspersky Digital Footprint Intelligence si avvale di tecniche OSINT unite ad analisi manuali e automatizzate di Surface, Deep e Dark Web, oltre che della Knowledge Base interna di Kaspersky da cui estrapolare informazioni e suggerimenti applicabili.

Il prodotto è disponibile nel portale Kaspersky Threat Intelligence. Potete acquistare quattro rapporti trimestrali con avvisi annuali per le minacce in tempo reale o acquistare un singolo rapporto con avvisi attivo per sei mesi.

Cercate nel Surface Web e nel Dark Web informazioni pressoché in tempo reale su eventi di sicurezza globale che minacciano le vostre risorse, nonché dati sensibili esposti su community e forum segreti con accesso limitato. La licenza annuale include 50 ricerche al giorno in fonti esterne e nella Knowledge Base Kaspersky.

Kaspersky Digital Footprint Intelligence costituisce un'unica soluzione con il servizio Kaspersky Takedown Service. La licenza annuale include 10 richieste di rimozione di domini dannosi e di phishing all'anno.

Inventario del perimetro di rete (incluso il cloud)

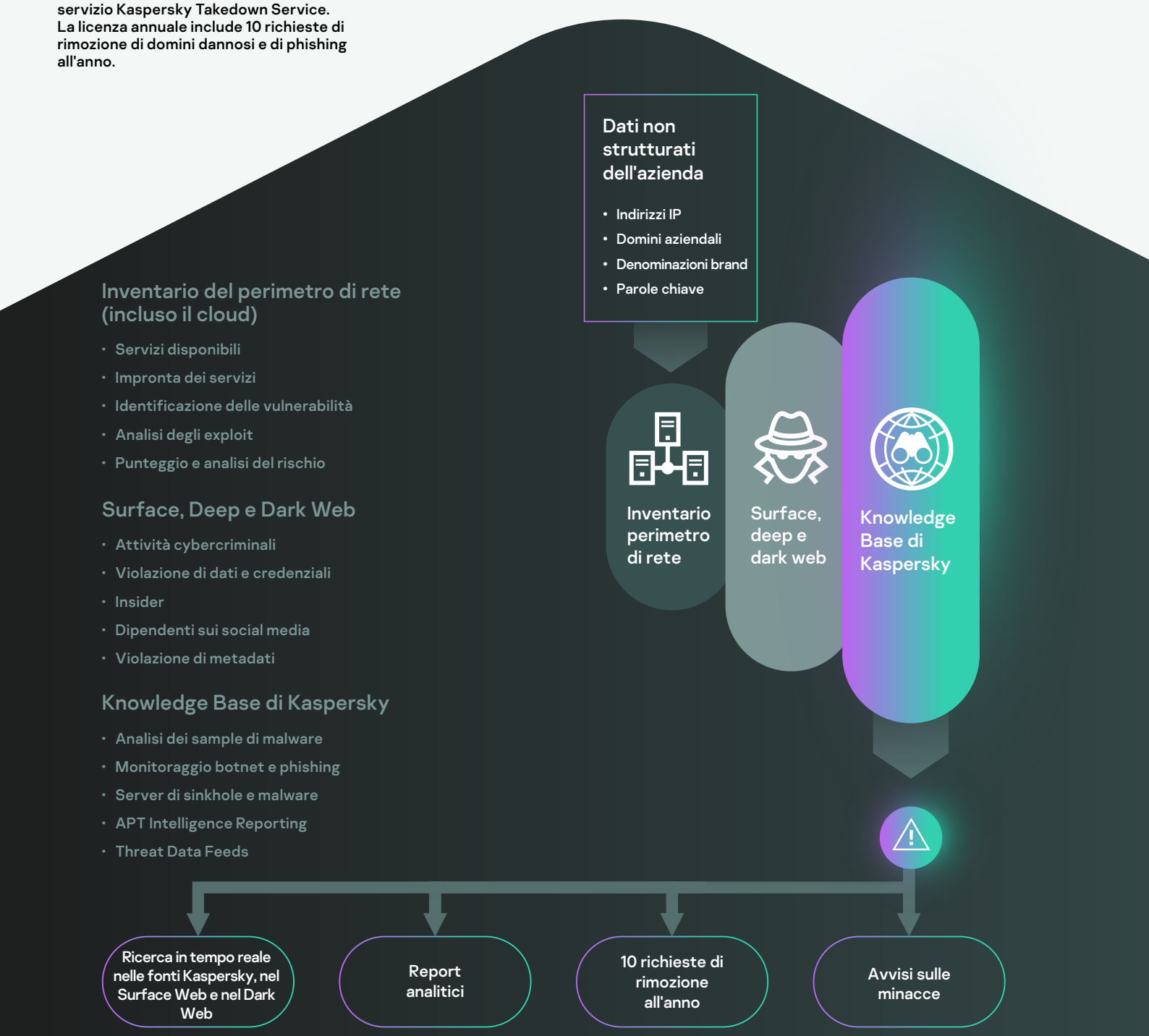
- Servizi disponibili
- Impronta dei servizi
- Identificazione delle vulnerabilità
- Analisi degli exploit
- Punteggio e analisi del rischio

Surface, Deep e Dark Web

- Attività cybercriminali
- Violazione di dati e credenziali
- Insider
- Dipendenti sui social media
- Violazione di metadati

Knowledge Base di Kaspersky

- Analisi dei sample di malware
- Monitoraggio botnet e phishing
- Server di sinkhole e malware
- APT Intelligence Reporting
- Threat Data Feeds



Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting fornisce informazioni approfondite e una maggiore consapevolezza delle campagne dannose mirate alle organizzazioni industriali, nonché delle informazioni sulle vulnerabilità presenti nei sistemi di controllo industriale più diffusi e nelle tecnologie sottostanti. I report vengono distribuiti tramite un portale basato sul web, pertanto è possibile iniziare a utilizzare immediatamente il servizio.

Report inclusi nell'abbonamento

1. **Report sulle APT.** Report sulle nuove APT e campagne di attacco di elevata intensità rivolte a organizzazioni industriali, oltre ad aggiornamenti sulle minacce attive.
2. **Il panorama delle minacce.** Report sui cambiamenti significativi nel panorama delle minacce per i sistemi di controllo industriale, nuovi fattori critici scoperti che influenzano i livelli di sicurezza ICS e l'esposizione ICS alle minacce, incluse informazioni per area geografica, paese e settore.
3. **Vulnerabilità rilevate.** Report sulle vulnerabilità identificate da Kaspersky nei prodotti più popolari utilizzati nei sistemi di controllo industriale, nell'Industrial Internet of Things e nelle infrastrutture in vari settori.
4. **Analisi e mitigazione delle vulnerabilità.** Le informazioni disponibili includono suggerimenti applicabili forniti dagli esperti Kaspersky per aiutare a identificare e mitigare le vulnerabilità nell'infrastruttura.

I dati di Threat Intelligence consentono di

Rilevare e prevenire

le minacce segnalate per salvaguardare le risorse importanti, compresi i componenti software e hardware, e garantite la sicurezza e la continuità dei processi tecnologici.

Correlare

eventuali attività dannose e sospette rilevate negli ambienti industriali con i risultati delle ricerche di Kaspersky, per attribuire il vostro rilevamento alla campagna dannosa in questione, identificare le minacce e rispondere tempestivamente agli incidenti

Eseguire

una valutazione delle vulnerabilità degli ambienti e delle risorse industriali in base a valutazioni approfondite sulla portata e sulla gravità delle vulnerabilità, così da prendere decisioni consapevoli sulla gestione delle patch e sull'attuazione delle altre misure preventive consigliate da Kaspersky.

Utilizzare

informazioni su tecnologie, tattiche e procedure di attacco, vulnerabilità scoperte di recente e segnalazioni di altri importanti cambiamenti nel panorama delle minacce per:

- Identificare e valutare i rischi presentati dalle minacce segnalate e altre minacce simili
- Pianificare e progettare modifiche alle infrastrutture industriali per garantire la sicurezza della produzione e la continuità del processo tecnologico
- Eseguire attività di sensibilizzazione sulla sicurezza basate sull'analisi di casi reali per creare scenari di formazione del personale e pianificare esercitazioni di tipo Red Team contro Blue Team
- Prendere decisioni strategiche efficaci per investire nella sicurezza informatica e garantire la resilienza delle operazioni

Kaspersky Ask the Analyst

I criminali informatici sviluppano costantemente strategie sofisticate per attaccare le aziende. Il panorama delle minacce odierno, in rapida evoluzione, presenta tecniche sempre più agili per i crimini informatici. Le organizzazioni affrontano incidenti complessi causati da attacchi non-malware, attacchi fileless, attacchi "living off the land", exploit zero-day e combinazioni di tutte queste tipologie integrate in minacce complesse, attacchi mirati e di tipo APT.

La ricerca continua delle minacce

consente a Kaspersky di scoprire, infiltrare e monitorare le community chiuse e i dark forum di tutto il mondo frequentati da nemici e criminali informatici. I nostri analisti sfruttano questo accesso per rilevare e ricercare in modo proattivo le minacce più note e dannose, nonché le minacce create appositamente per colpire organizzazioni specifiche

In un'era di attacchi informatici che paralizzano le aziende, i professionisti della sicurezza informatica sono più importanti che mai, ma trovarli e riuscire a far in modo che restino in azienda non è affatto facile. E anche se disponete di un team di sicurezza informatica ben strutturato, non potete sempre aspettarvi che i vostri esperti contrastino le minacce sofisticate da soli: **hanno bisogno di poter contare sull'assistenza di terze parti.** Un'expertise esterna può far luce sui potenziali percorsi degli attacchi complessi o APT, fornendo consigli da implementare per eliminare il problema nel modo più efficace.

Risultati del servizio Ask the Analyst

(abbonamento unificato basato sulle richieste)

Il servizio **Kaspersky Ask the Analyst** estende il nostro portfolio di intelligence sulle minacce, consentendovi di richiedere indicazioni e approfondimenti su minacce specifiche che state affrontando o alle quali siete interessati. Il servizio adatta le potenti funzionalità di ricerca e intelligence sulle minacce di Kaspersky alle vostre esigenze specifiche, consentendovi di creare solide difese contro le minacce destinate alla vostra organizzazione.

APT e crimeware

Informazioni aggiuntive sui rapporti pubblicati e sulle ricerche in corso (oltre al servizio APT o Crimeware Intelligence Reporting)[1]

Analisi malware

- Analisi dei campioni di malware
- Suggerimenti su ulteriori azioni correttive

Descrizioni di minacce, vulnerabilità e relativi IoC

- Descrizione generale di una famiglia specifica di malware
- Contesto aggiuntivo per le minacce (relativi hash, URL, CnC e così via)
- Informazioni su una vulnerabilità specifica (livello di criticità e meccanismi di protezione corrispondenti nei prodotti Kaspersky)

Intelligence sul Dark Web[2]

- Ricerca nel Dark Web di determinati artefatti, indirizzi IP, nomi di dominio, nomi di file, e-mail, collegamenti o immagini
- Analisi e ricerca di informazioni

Richieste relative a ICS

- Informazioni aggiuntive sui rapporti pubblicati
- Informazioni sulle vulnerabilità ICS
- Statistiche sulle minacce ICS e tendenze per area geografica/settore
- Informazioni sull'analisi del malware ICS in regolamenti o standard

[1] Disponibile solo per i clienti con il servizio APT o Crimeware Intelligence Reporting attivo

[2] Già inclusa nell'abbonamento Kaspersky Digital Footprint Intelligence

Vantaggi offerti dal servizio

Competenze a portata di mano

Ottenete accesso on-demand agli esperti di settore senza dovervi dedicare alla faticosa ricerca e all'assunzione di specialisti a tempo pieno

Indagini più veloci

Definite l'ambito degli incidenti e assegnate le priorità in modo efficace in base a informazioni contestuali dettagliate e personalizzate

Risposta rapida

Rispondete rapidamente a minacce e vulnerabilità usando le nostre linee guida per bloccare gli attacchi tramite vettori noti

Come funziona

Kaspersky Ask the Analyst può essere acquistato separatamente o in abbinamento a uno dei nostri servizi di intelligence sulle minacce.

Potete inviare le vostre richieste tramite Kaspersky Company Account, il nostro portale di assistenza per i clienti aziendali. Risponderemo tramite e-mail ma, in caso di necessità, potremo concordare una conference call e/o una sessione di condivisione dello schermo. Quando la vostra richiesta verrà accettata, verrete informati in merito al tempo stimato per l'elaborazione.

Casi di utilizzo del servizio:

- Chiarire eventuali dettagli nei rapporti di intelligence sulle minacce pubblicati in precedenza
- Ottenere informazioni aggiuntive per IoC già forniti
- Ottenere dettagli sulle vulnerabilità e suggerimenti su come proteggersi dal relativo sfruttamento
- Ottenere dettagli aggiuntivi sulle specifiche attività del Dark Web alle quali siete interessati
- Ottenere un rapporto generico sulla famiglia di malware che includa il comportamento dello stesso, il potenziale impatto e i dettagli sulle attività correlate osservate da Kaspersky
- Assegnare le priorità ad avvisi/incidenti in modo efficace con informazioni contestuali dettagliate e categorizzazione per i relativi IoC forniti tramite brevi rapporti
- Richiedere assistenza per l'identificazione, se vengono rilevate attività insolite relative a un APT o a un autore di crimeware
- Inviare file malware per l'analisi completa al fine di capire il comportamento e le funzionalità dei campioni forniti

Aumentate le vostre conoscenze e risorse

Kaspersky Ask the Analyst vi offre l'accesso a un gruppo di ricercatori Kaspersky specifico per ciascun caso. Il servizio garantisce una comunicazione completa tra gli esperti per potenziare le competenze esistenti con le nostre risorse e conoscenze esclusive.

Kaspersky Takedown Service

Sfida

I criminali informatici creano domini dannosi e di phishing che vengono utilizzati per attaccare la vostra azienda e i vostri brand. L'incapacità di mitigare rapidamente queste minacce, una volta identificate, può comportare perdita di guadagni, danni all'immagine del brand, perdita di fiducia dei clienti, fughe di dati e a molto altro. Ma la gestione della rimozione di questi domini è un processo complesso che richiede esperienza e tempo.

Soluzione

Kaspersky blocca oltre 15.000 URL di phishing/truffa e previene ogni giorno oltre un milione di clic su tali URL. Grazie ai numerosi anni di esperienza nell'analisi di domini dannosi e di phishing siamo in grado di raccogliere tutte le prove necessarie per dimostrarne la natura dannosa. Ci occupiamo della gestione della rimozione e offriamo la possibilità di intervenire rapidamente per ridurre al minimo il rischio digitale, consentendo al vostro team di concentrarsi su altre attività prioritarie.

Kaspersky offre ai suoi clienti un'efficace protezione dei servizi online e della reputazione collaborando con organizzazioni internazionali, forze dell'ordine nazionali e regionali (ad esempio INTERPOL, Europol, Microsoft Digital Crimes Unit, The National High-Tech Crime Unit (NHTCU) della polizia dei Paesi Bassi e della City of London Police), nonché con Computer Emergency Response Teams (CERTs) in tutto il mondo.

Come funziona

Potete inviare le vostre richieste tramite Kaspersky Company Account, il nostro portale di assistenza per i clienti aziendali. Prepareremo tutta la documentazione necessaria e invieremo la richiesta di rimozione all'autorità locale/regionale di pertinenza (CERT, registrar e così via) in possesso dei diritti legali necessari per eliminare il dominio. Riceverete le notifiche in ogni fase del processo, fino al completamento della richiesta.

Protezione immediata

Il servizio Kaspersky Takedown Service mitiga rapidamente le minacce costituite dai domini dannosi e di phishing prima che possano causare danni al vostro brand e alla vostra azienda. La gestione end-to-end dell'intero processo consente di risparmiare tempo e risorse preziosi.

Vantaggi offerti dal servizio

Protezione globale

Indipendentemente da dove sia stato registrato il dominio dannoso o di phishing, Kaspersky ne richiederà la rimozione dall'organizzazione regionale presso l'autorità legale opportuna.

Gestione end-to-end

Gestiamo l'intero processo di rimozione, riducendo al minimo il coinvolgimento dell'azienda.

Visibilità completa

Riceverete una notifica in ogni fase del processo, dalla registrazione della richiesta alla rimozione.

Integrazione con Digital Footprint Intelligence

Il servizio si integra con Kaspersky Digital Footprint Intelligence, che offre notifiche in tempo reale sui domini di phishing e malware, progettati per danneggiare, violare o rappresentare il vostro brand o la vostra organizzazione. Una soluzione unica è un elemento importante di una strategia di sicurezza informatica completa.

Vantaggi chiave

Consente la visibilità globale delle minacce, il rilevamento tempestivo delle minacce informatiche, l'assegnazione delle priorità agli avvisi di sicurezza e una risposta efficace agli incidenti relativi alla sicurezza delle informazioni

Facilita il lavoro degli analisti e aiuta a concentrare la forza lavoro su autentiche minacce

Le informazioni approfondite su tattiche, tecniche e procedure utilizzate dagli autori delle minacce in diversi settori e aree geografiche consentono una protezione proattiva dalle minacce complesse e mirate

Una panoramica completa del vostro orientamento in merito alla sicurezza con suggerimenti applicabili sulle strategie di mitigazione vi consente di concentrarvi sulla strategia difensiva in aree identificate come obiettivi primari degli attacchi informatici

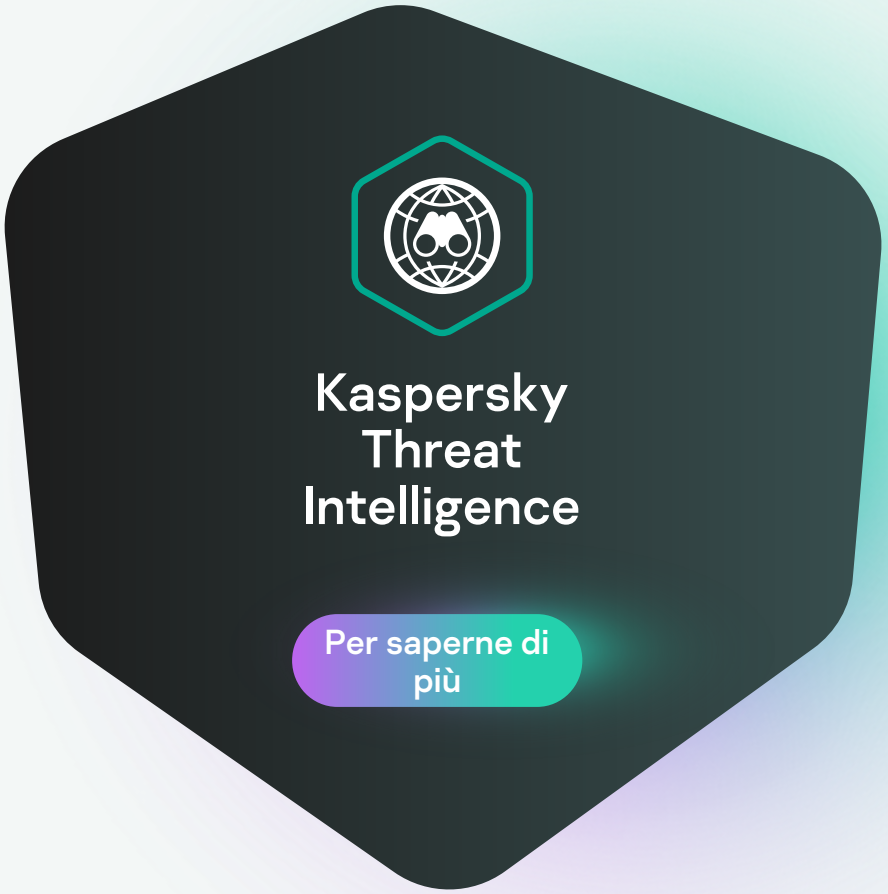
La risposta agli incidenti accelerata e migliorata e le funzionalità di ricerca delle minacce aiutano a ridurre significativamente il tempo di permanenza degli attacchi e i possibili danni

Conclusione

Il contrasto alle attuali minacce informatiche richiede una visione a 360 gradi di tattiche e strumenti utilizzati dagli attori delle stesse. La generazione di questa intelligence e l'identificazione delle contromisure più efficaci richiede una costante dedizione e alti livelli di competenza. Con la possibilità di estrapolare petabyte di dati sulle minacce, tecnologie di machine learning avanzate e un pool di esperti unico al mondo, noi di Kaspersky lavoriamo per supportare i nostri clienti con la più recente tecnologia di Threat Intelligence proveniente da tutto il mondo, al fine di garantire la sicurezza anche contro gli attacchi informatici precedentemente passati inosservati.

FORRESTER®

Kaspersky è riconosciuta come Leader nel report Forrester Wave: External Threat Intelligence Services, 2021



www.kaspersky.it

© 2022 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.