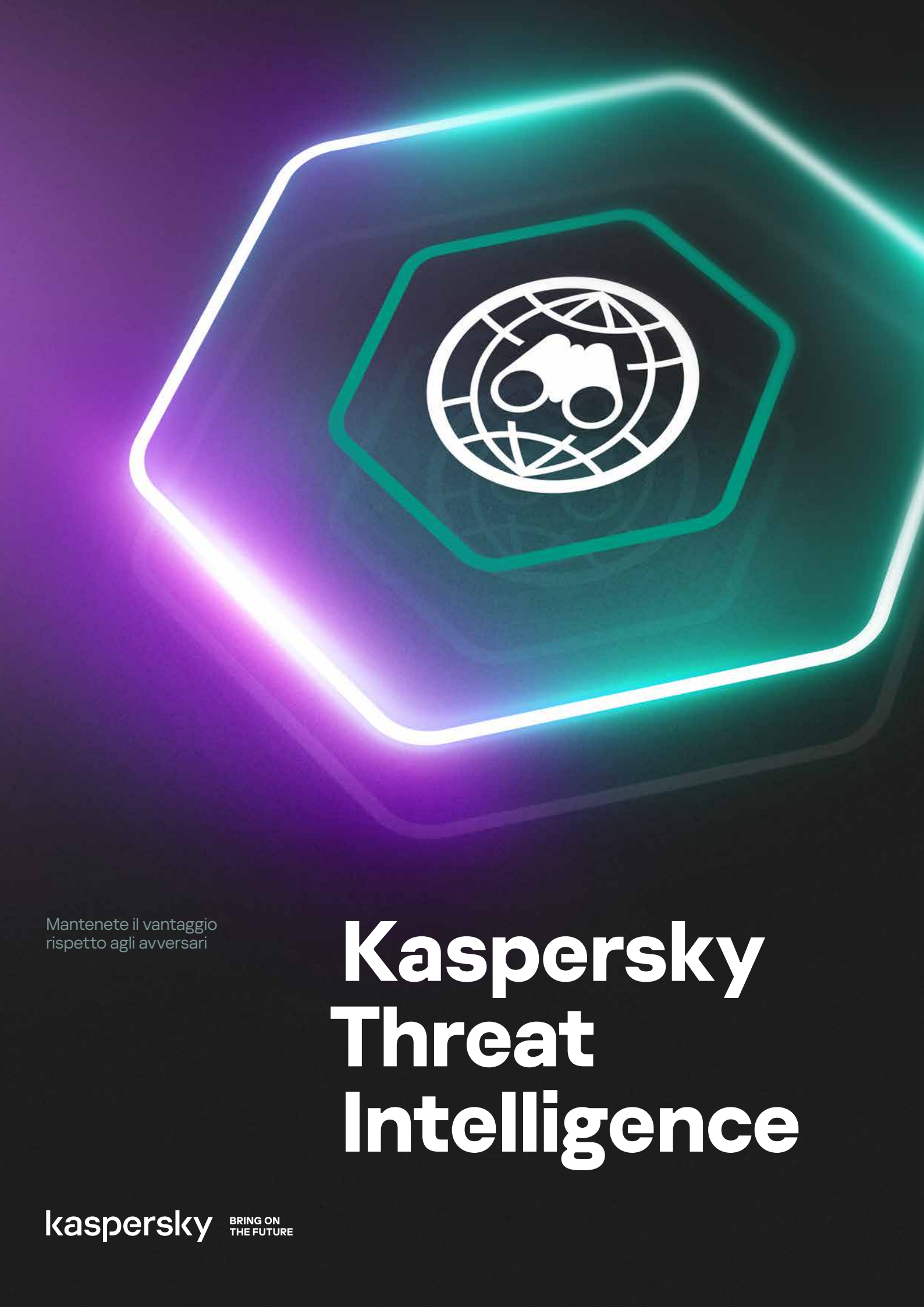


Mantenete il vantaggio
rispetto agli avversari

Kaspersky Threat Intelligence

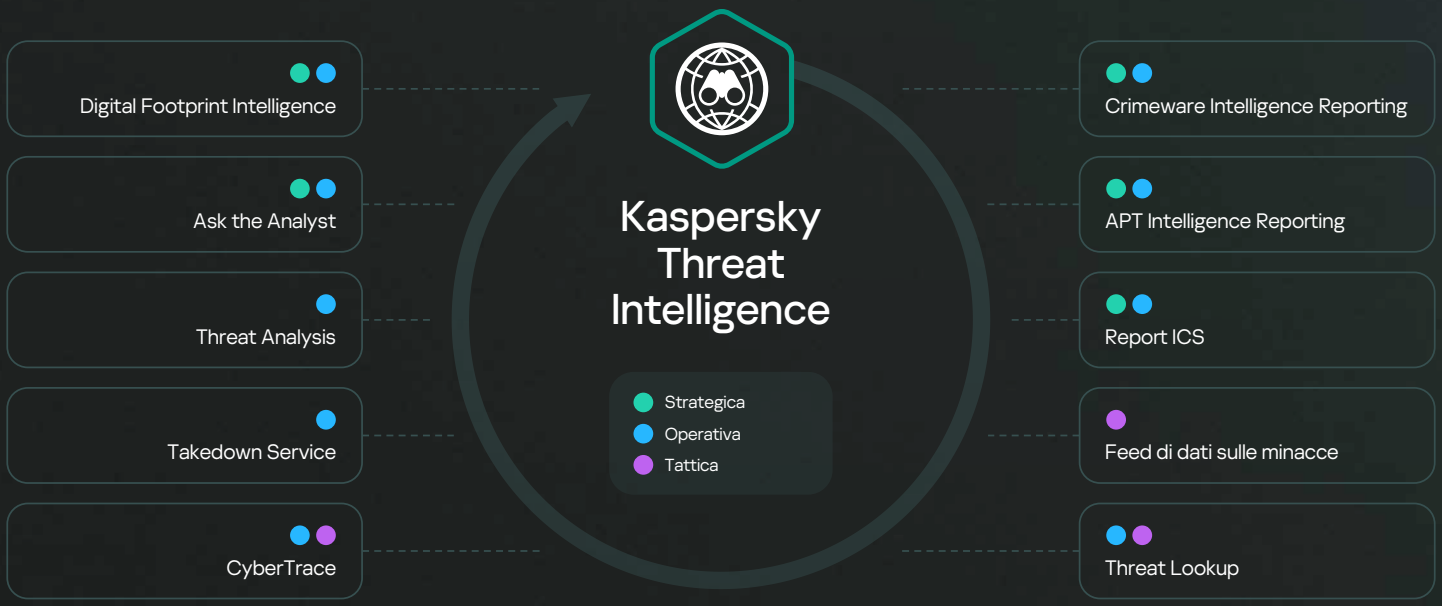
kaspersky BRING ON THE FUTURE

Kaspersky Threat Intelligence

La Threat Intelligence di Kaspersky, offerta dal nostro team che include i migliori ricercatori e analisti del mondo, offre l'accesso alle informazioni necessarie per mitigare le minacce informatiche.

Grazie alle sue conoscenze, all'esperienza e alle informazioni approfondite su ogni aspetto della sicurezza informatica, Kaspersky è il partner di fiducia delle più importanti agenzie governative e forze dell'ordine, tra cui l'Interpol e i principali CERT. La soluzione Kaspersky Threat Intelligence assicura l'accesso istantaneo a una Threat Intelligence tattica, operativa e strategica.

Kaspersky Threat Intelligence offre una visione completa del panorama globale delle minacce, combinando fonti di intelligence, feed di dati sulle minacce e ricerche interne, il tutto analizzato dal nostro team di esperti per fornire alle organizzazioni informazioni utili per proteggersi dalle minacce informatiche.



Kaspersky Threat Intelligence consente di

Identificare e prevenire in modo proattivo le minacce

Con Kaspersky Threat Intelligence è possibile mantenersi sempre informati sulle ultime minacce e vulnerabilità, per adottare le misure proattive necessarie per proteggere i sistemi aziendali prima che si verifichi un attacco.

Ottenere visibilità sul footprint digitale dell'azienda

Kaspersky Threat Intelligence offre una visione completa dell'impronta digitale dell'organizzazione, incluse tutte le risorse che potrebbero essere vulnerabili ad attacchi o compromissioni.

Migliorare le capacità di rilevamento delle minacce

Kaspersky Threat Intelligence consente di potenziare le soluzioni di sicurezza esistenti, migliorando la capacità di rilevare e bloccare le minacce avanzate.

Migliorare le capacità di risposta agli incidenti

Kaspersky Threat Intelligence fornisce informazioni in tempo reale sulle minacce emergenti e indicatori di compromissione, consentendo alle aziende di rispondere in modo rapido ed efficace agli incidenti.

Mantenere la conformità con standard e normative

Tutte le aziende sono soggette ai diversi regolamenti e standard diffusi nel settore in cui operano. Kaspersky Threat Intelligence supporta la conformità aiutandovi a soddisfare questi requisiti.

Sviluppare le competenze del personale interno

Il team Kaspersky è composto da alcuni dei ricercatori più esperti e rispettati del settore, pronti a mettere tutto il loro patrimonio di conoscenze e competenze a disposizione dei vostri team di sicurezza IT.

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 di aziende e organizzazioni. Gli autori degli attacchi usano complicate kill chain, campagne e tattiche, tecniche e procedure (TTP) personalizzate per bloccare i processi aziendali o danneggiare i clienti. Per una protezione efficace è necessario adottare nuovi metodi di protezione, basati sulla Threat Intelligence.

Integrando feed di Threat Intelligence aggiornati ogni minuto che contengono informazioni su IP sospetti e pericolosi, URL e hash dei file nei sistemi di sicurezza esistenti come SIEM, SOAR e piattaforme TI, i team di sicurezza possono automatizzare il processo di triage degli alert iniziali, fornendo al contempo ai loro specialisti un contesto sufficiente per identificare immediatamente gli alert che devono essere indagati o trasferiti ai team di incident response per ulteriori investigation e response.

Kaspersky Threat Data Feed fornisce informazioni di Threat Intelligence in tempo reale per aiutarvi a proteggere le reti e i sistemi dalle minacce informatiche. I feed di dati includono informazioni su malware noti, siti Web di phishing, le vulnerabilità e gli exploit più recenti e altri tipi di minacce informatiche: informazioni per aiutarvi a bloccare il traffico dannoso, aggiornare il software di sicurezza e adottare altre misure per proteggervi dai cyberattacchi.

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 intervenire in modo adeguato.

Come funziona

1

I dati vengono raccolti da un'ampia varietà di fonti attendibili, come Kaspersky Security Network, Web crawler, il servizio di monitoraggio delle minacce botnet (tiene traccia delle botnet e dei loro obiettivi 24 ore su 24, 7 giorni su 7), spam trap, dati di gruppi di ricerca, partner e molto altro.

2

Tutte le informazioni raccolte vengono accuratamente controllate e pulite in tempo reale utilizzando vari metodi di pre-elaborazione: sandbox, analisi statistica ed euristica, strumenti per la somiglianza, profilazione dei comportamenti e analisi da parte di esperti.

3

I feed di dati consentono di raccogliere informazioni sulle minacce relative a un avviso o un incidente e ad approfondire i dettagli. Aiutano anche a rispondere alle domande "Chi? Cosa? Dove? Perché?" e a identificare l'origine di un attacco, consentendo un rapido processo decisionale per proteggere l'azienda dalle minacce di qualsiasi complessità.

Le voci nei feed forniti da Kaspersky contengono dati contestuali che consentono rapidamente di confermare le minacce e definire le priorità:

- Denominazioni delle minacce
- Indirizzi IP e nomi di dominio di risorse Web dannose
- Hash di file dannosi
- Oggetti vulnerabili e compromessi
- Tattiche, tecniche e procedure di attacco secondo la classificazione MITRE ATT&CK
- Timestamp
- Geolocalizzazione
- Popolarità e così via

Vantaggi di Kaspersky Threat Data Feeds

Migliorate e accelerate l'incident response e le capacità di analisi forense

automatizzando il processo di triage iniziale, fornendo agli analisti di sicurezza un contesto sufficiente per identificare immediatamente gli alert che devono essere indagati o inoltrati ai team di incident response per ulteriori indagini.

Rafforzate le soluzioni di sicurezza

inclusi SIEM, firewall, IPS/IDS, proxy per la sicurezza, soluzioni DNS, anti-APT, con Indicatori di Compromissione (IoC) continuamente aggiornati e contestualizzati, per ottenere informazioni approfondite sugli attacchi informatici e una maggiore comprensione delle intenzioni, delle capacità e degli obiettivi degli avversari. Sono pienamente supportati i principali SIEM (inclusi ArcSight, IBM QRadar, MS Sentinel, Splunk e così via) e le piattaforme TI.

Impedite l'esfiltrazione di risorse sensibili e proprietà intellettuale

dai computer infetti all'esterno dell'organizzazione. Rilevate rapidamente le risorse infette per proteggere la reputazione del brand, mantenendo il vantaggio competitivo e tutelando le opportunità aziendali.

Espandete le attività MSSP

fornendo una Threat Intelligence leader del settore come servizio premium per i clienti. Da parte loro, i CERT hanno l'opportunità di potenziare ed estendere considerevolmente le capacità di detection e identificazione delle minacce informatiche.

Kaspersky CyberTrace

Il progressivo aumento del numero di feed di dati e la crescente quantità di fonti di Threat Intelligence disponibili rendono alquanto problematico, per le aziende, poter determinare quali siano le informazioni effettivamente rilevanti. Allo stesso tempo, 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 degli altri controlli di sicurezza implementati a livello di rete.

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 alert che richiedono un'analisi approfondita o che vanno inoltrati ai team di incident response per ulteriori analisi.

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 workflow delle attività di sicurezza già esistenti. Si integra con qualsiasi feed di Threat Intelligence (di Kaspersky, di 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.

Strumenti

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 quelli contestuali

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'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

Un grafico di ricerca consente di esplorare visivamente i dati e i rilevamenti archiviati in CyberTrace e di individuare 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

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

La multi-tenancy supporta gli MSSP e gli use case delle grandi aziende

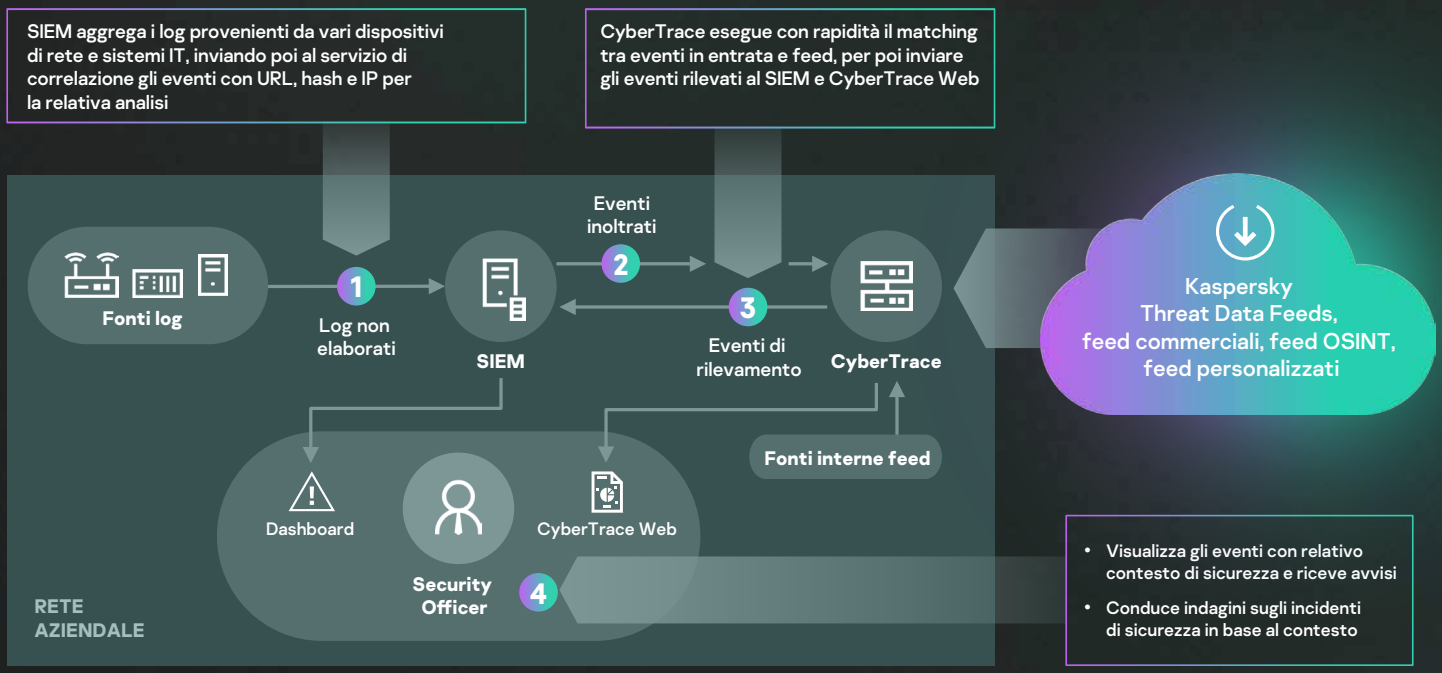
Un filtro invia eventi di detection alle soluzioni SIEM, riducendo il carico di lavoro anche per gli analisti

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

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 confrontarsi sulle minacce e aggiungere informazioni di Threat Intelligence interne sull'indicatore

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, infine genera i propri alert in relazione alla threat detection.

Architettura



Kaspersky CyberTrace e Kaspersky Threat Data Feeds garantiscono agli analisti della sicurezza:

Efficace selezione di grandi quantità di alert di sicurezza e corretta assegnazione delle relative priorità

Perfezionamento e accelerazione dei processi di triage e response iniziale

Creazione di difese proattive basate sull'intelligence

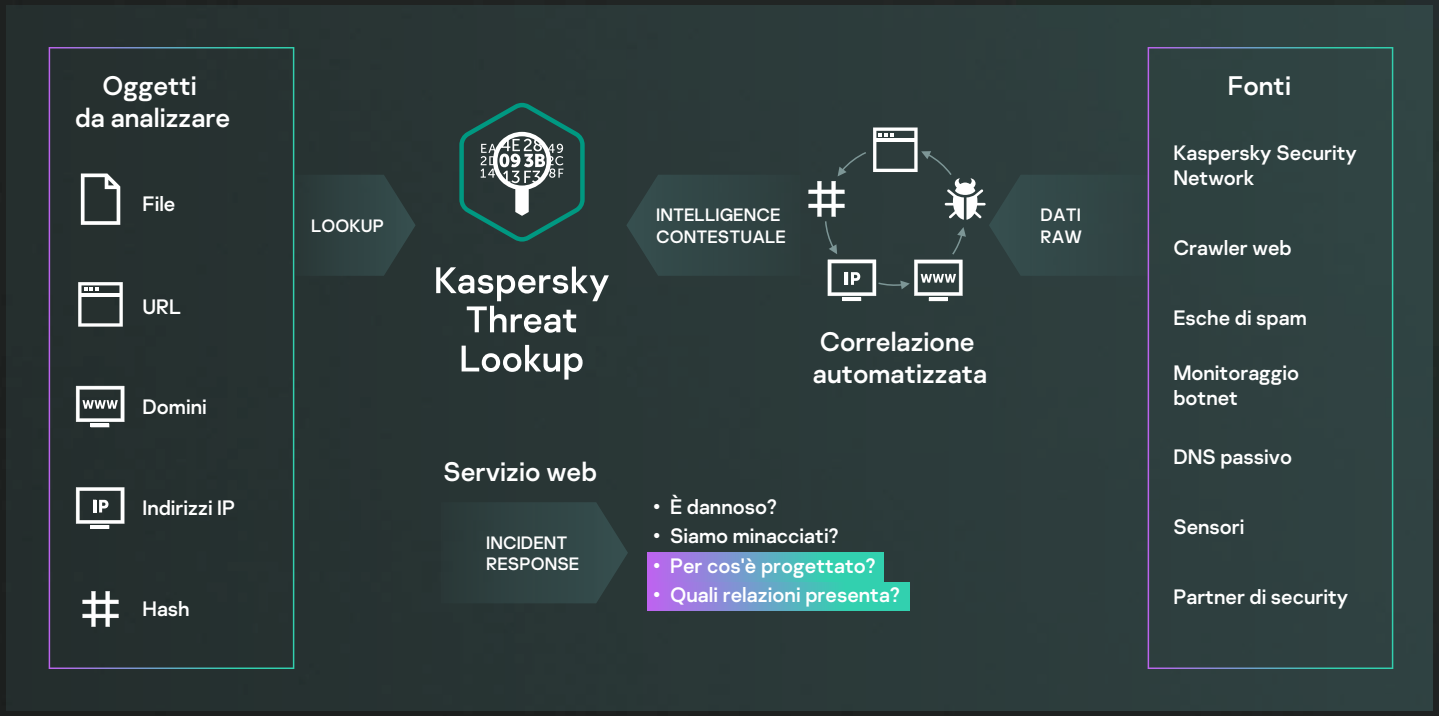
Immediata identificazione degli alert critici per l'azienda e possibilità di prendere decisioni maggiormente informate riguardo agli alert da inoltrare ai team IR

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 difesa. I cybercriminali, nelle loro campagne, utilizzano complesse kill chain, Tattiche, Tecniche e Procedure (TTP) personalizzate nelle loro campagne per interrompere le attività aziendali, rubare gli asset o danneggiare i clienti.

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 la vostra azienda. La piattaforma recupera le informazioni dettagliate più recenti 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.

Come funziona



Caratteristiche principali

Intelligence affidabile

una caratteristica chiave di Kaspersky Threat Lookup è l'affidabilità dei dati della threat intelligence, completati dal contesto di applicabilità. Kaspersky domina i test condotti sulle soluzioni anti-malware, grazie all'impareggiabile qualità della nostra security intelligence e ai tassi di rilevamento estremamente elevati, con falsi positivi vicini allo zero.

Threat Hunting

proattività nella prevenzione, nel rilevamento e nella risposta agli incidenti, al fine di ridurre 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 che può causare. Quanto più rapidamente vengono prese misure correttive, tanto prima potranno tornare al loro normale funzionamento le attività di rete.

Facile da usare

Interfaccia Web o API RESTful. È possibile utilizzare il servizio in modalità manuale tramite un'interfaccia Web (via browser Web) o accedervi tramite una semplice API RESTful, a seconda delle preferenze

Ampia gamma di formati di esportazione

È possibile esportare gli indicatori di compromissione (IOC) o il contesto di applicabilità nei formati di condivisione maggiormente utilizzati e organizzati, nonché leggibili dai computer, come STIX, OpenIOC, JSON, Yara, Snort o addirittura CSV, per usufruire di tutti i vantaggi della Threat Intelligence, per automatizzare il flusso di lavoro operativo o per effettuare l'integrazione con controlli di sicurezza quali SIEM.

Vantaggi di Kaspersky Threat Lookup

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

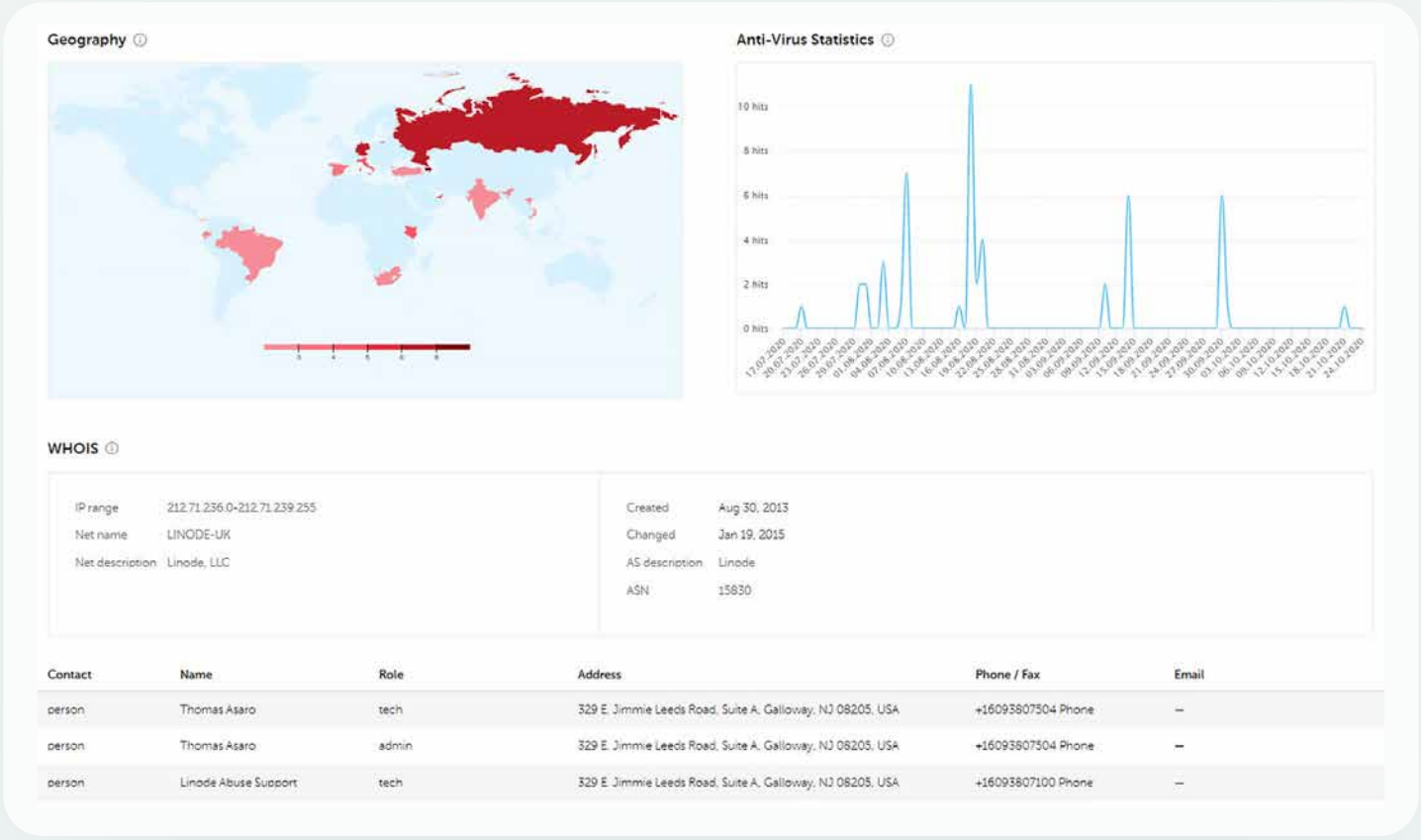
Diagnosi e analisi degli incidenti di sicurezza negli host e nella rete in modo più efficace e assegnazione delle priorità ai segnali dei sistemi interni contro le minacce sconosciute

Ottimizzazione delle capacità di incident response e threat hunting per interrompere la kill chain prima che vengano compromessi dati e sistemi critici

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

È possibile verificare se l'oggetto scoperto è già diffuso o di tipo unico e comprendere perché un oggetto deve essere trattato come dannoso



Kaspersky Research Sandbox

È di fatto impossibile prevenire gli attacchi mirati avvalendosi esclusivamente dei tradizionali anti-virus. I motori anti-virus possono solo bloccare le minacce note e le loro varianti, mentre i sofisticati threat actor utilizzano un'ampia varietà di tecniche per eludere il rilevamento automatico. Le perdite dovute a incidenti di sicurezza delle informazioni continuano ad aumentare, sottolineando l'importanza delle funzionalità di rilevamento immediato delle minacce per garantire una reazione rapida e la capacità di contrastare le minacce prima che possano causare danni.

Prendere una decisione intelligente basata sul comportamento di un file, analizzando contemporaneamente la memoria del processo, l'attività di rete, ecc., è l'approccio ottimale per comprendere le ultime minacce sofisticate mirate e su misura. Mentre i dati statistici possono mancare di 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 la detection di oggetti dannosi non individuati in precedenza.

Kaspersky Research Sandbox consente di indagare sulle origini dei campioni di file, raccogliere IOC in base all'analisi comportamentale e rilevare oggetti dannosi non rilevati in precedenza. Fornisce in tal senso un approccio ibrido, volto a combinare le informazioni di Threat Intelligence ricavate dall'analisi di petabyte di dati statistici (grazie a 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.

Rilevamento e mitigazione proattivi delle minacce

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 con estrema precisione il normale comportamento dell'utente finale.

Kaspersky Research 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 a 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 servizio 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 25 anni di ricerca continua sulle minacce. Questo ci consente di rilevare oltre 400.000 nuovi oggetti pericolosi al giorno per fornire ai nostri clienti soluzioni di sicurezza leader di settore.

Kaspersky Research Sandbox può essere gestito sia da una piattaforma di gestione centrale basata sul cloud che da una console offline in ambienti di tipo "air-gap", avvalendosi della Threat Intelligence e integrando analisi personalizzabili.

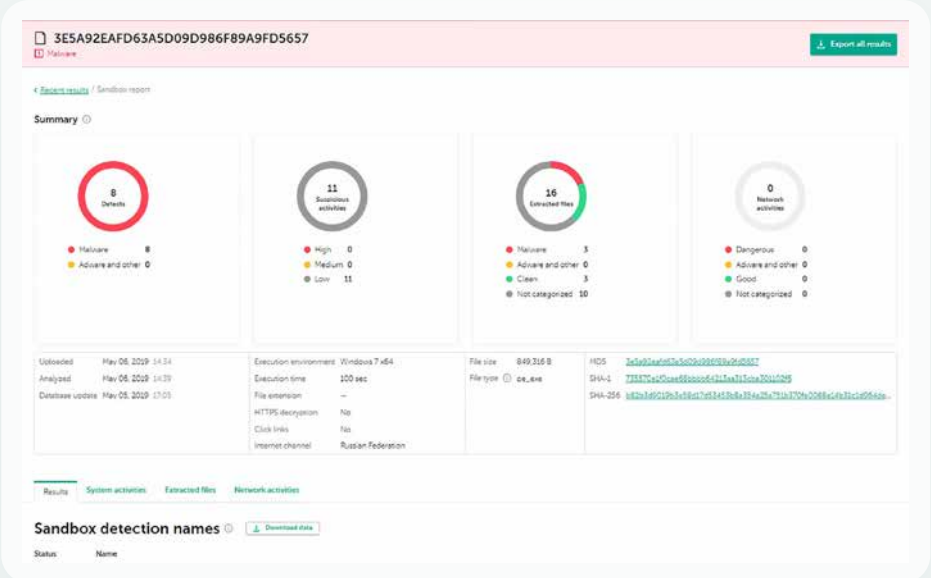
Nell'ambito del Threat Intelligence Portal, Kaspersky Research Sandbox rappresenta il componente finale nel vostro flusso di lavoro di Threat Intelligence. Mentre Threat Lookup recupera le più recenti e dettagliate informazioni di Threat Intelligence relative a URL, domini, indirizzi IP, hash di file, denominazioni delle minacce, dati statistici/comportamentali, dati WHOIS/DNS e così via, Research Sandbox collega tali conoscenze agli IoC generati attraverso l'analisi dei file.

Reporting completo

- Percentuale delle minacce unificata
- Attività di sistema sospette con descrizioni dettagliate
- Caricamento ed esecuzione di DLL
- Creazione, modifica ed eliminazione di file
- Dump della memoria di processo e dump del traffico di rete (PCAP)
- Creazione di esclusioni reciproche (mutex)
- Modifica e creazione di chiavi di registro
- Processi creati dall'esecuzione di un file
- Attività di rete (sessioni SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, SOCKS; HTTP(s), richieste e risposte)
- Dettagliate informazioni di threat intelligence, contestualizzate, per ogni Indicatore di Compromissione (IoC) rivelato
- Mappa di esecuzione dettagliata con tecniche MITRE ATT&CK evidenziate
- Rilevamenti YARA e attivazione di regole IDS (comprese quelle personalizzate)
- Download e analisi di un file ospitato su un determinato URL
- Clic sui collegamenti nei documenti di Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) e Adobe Reader
- Possibilità di esportare i dettagli delle analisi nei formati STIX, JSON, CSV
- Varietà di ambienti tra cui sistema operativo mobile (Android) e funzionalità di personalizzazione dell'ambiente
- Parametri personalizzati per l'esecuzione dei file
- Diversi canali Internet, possibilità di instradare il traffico tramite un canale VPN personalizzato
- API RESTful
- Screenshot e molto altro

Con Kaspersky Research Sandbox è possibile condurre con elevata efficacia complesse indagini sugli incidenti, per un'immediata comprensione della natura delle minacce. Ciò consente di acquisire informazioni particolarmente dettagliate, in grado di rivelare le correlazioni tra gli 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 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 Threat Attribution Engine

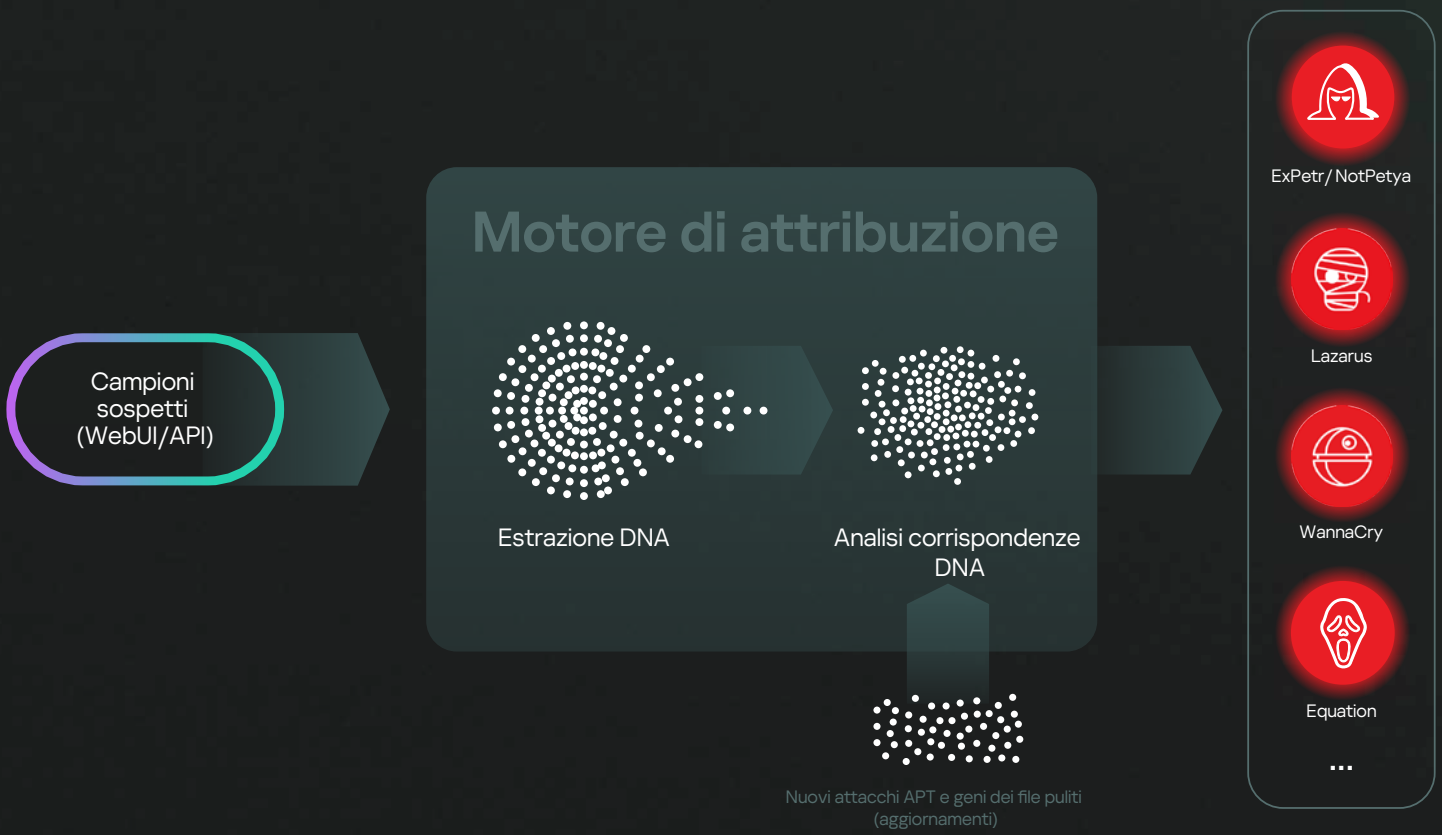
C'è una buona ragione per cui l'attribuzione delle minacce riveste un ruolo così significativo nella sicurezza informatica. L'intervallo di tempo medio tra il rilevamento e la reazione a minacce altamente sofisticate può essere molto lungo, a causa dei complessi processi di indagine e reverse engineering coinvolti. In molti casi, questo ritardo può concedere agli aggressori tempo sufficiente per raggiungere i loro obiettivi. L'attribuzione corretta e tempestiva non solo consente di ridurre i tempi di incident response da ore a minuti, ma anche di diminuire il numero di falsi positivi.

Identificare un attacco mirato, tracciare un profilo degli autori e creare fattori di attribuzione per i diversi threat actor è un lavoro lungo e complesso, che può richiedere anni. La creazione di un'attribuzione corretta richiede anche una grande quantità di dati accumulati nel tempo, nonché un team di ricercatori altamente qualificati con un'adeguata esperienza nel campo delle indagini. Questi ricercatori in genere seguono l'attività di diversi gruppi e popolano un database con tutte le informazioni accumulate. Questo database diventa quindi una risorsa preziosa da condividere sotto forma di soluzione di sicurezza.

Kaspersky Threat Attribution Engine incorpora un database contenente campioni di malware APT e file raccolti dagli esperti di Kaspersky negli ultimi 25 anni di lavoro e oltre. Monitoriamo oltre 1.100 threat actor e campagne e pubblichiamo oltre 120 rapporti di Threat Intelligence all'anno. Le nostre attività di ricerca continuative supportano una raccolta APT che contiene circa 83.000 file. Ciò migliora il rilevamento dei falsi positivi e, insieme all'uso di strumenti automatizzati, si traduce in livelli di attribuzione straordinariamente accurati.

Il prodotto offre un approccio unico per il confronto di campioni simili, garantendo al tempo stesso tassi di falsi positivi prossimi allo zero. Qualsiasi nuovo attacco può essere rapidamente collegato a malware APT noto, attacchi mirati precedenti e gruppi di hacker, aiutandovi a distinguere le minacce ad alto rischio dagli incidenti meno gravi, in modo da poter adottare misure di protezione tempestive per impedire all'autore dell'attacco di penetrare nel sistema.

Come funziona



Per collegare il malware alle entità di attribuzione, Kaspersky Threat Attribution Engine utilizza un metodo esclusivo e proprietario per la ricerca delle somiglianze tra i file. Questo metodo comprende:

1

Analisi della genetica di un campione, estraendo dal suo codice i seguenti elementi:

- Genotipi: pezzi distintivi di codice binario.
- Stringhe: stringhe distintive di caratteri.

2

Ricerca automatica nei file analizzati di genotipi, stringhe simili a genotipi e stringhe di campioni APT precedentemente analizzati o già collegati a entità di attribuzione.

3

Sulla base dei genotipi e delle stringhe simili rilevati nei campioni APT, viene generato un rapporto sull'origine del campione analizzato, le entità di attribuzione correlate e le eventuali somiglianze con campioni APT noti.

Il prodotto si può implementare in ambienti air-gap sicuri, atti a limitare l'accesso di terze parti alle informazioni elaborate e agli oggetti analizzati. Un'apposita interfaccia API connette il motore ad altri framework e strumenti, al fine di implementare il processo di attribuzione nell'ambito delle infrastrutture e dei processi automatizzati già esistenti.

Principali caratteristiche del prodotto

- Fornisce un accesso istantaneo a un archivio di dati selezionati su migliaia di gruppi APT, campioni e minacce più ampie (tramite il motore anti-virus)
- Consente di assegnare in modo efficiente la priorità delle minacce, in modalità automatica o manuale, e di attivare il processo di triage
- Supporta l'aggiunta di campioni e attori privati, configurando il prodotto per identificare campioni simili ai file presenti nella raccolta privata
- Consente il caricamento manuale dei campioni e offre funzionalità avanzate dell'API REST per l'integrazione con flussi di lavoro automatizzati
- Supporta la distribuzione su Amazon Web Services (AWS), consentendo una rapida configurazione del prodotto e assicurando un risparmio sui costi, in quanto non richiede investimenti hardware in anticipo
- Facilità di esportazione in regole YARA per ulteriori attività di ricerca/scansione automatizzata di file simili o integrazione con soluzioni di terze parti
- Facilità di esportazione in formato STIX 2.1 (sono supportati anche i formati TXT e JSON) per ulteriori attività di analisi automatizzata dei log di sicurezza o l'integrazione con soluzioni/controlli di sicurezza di terze parti
- Consente la decompressione degli archivi protetti da password con password personalizzate
- Consente di accedere rapidamente alla documentazione e al Contratto di licenza con l'utente finale (EULA) nell'interfaccia Web
- Invia gli attributi in file paralleli per l'analisi in un'unica richiesta

Vantaggi di Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine calcola il punteggio di reputazione

del campione e ne rivela la genetica e l'attribuzione del codice. Ciò fornisce informazioni sull'origine del campione e può consentire la sua attribuzione ai possibili responsabili.

Il team di sicurezza può aggiungere entità di attribuzione private

e campioni correlati al database di Kaspersky Threat Attribution Engine. Il team può quindi fare in modo che l'applicazione attribuisca i campioni inviati a tali campioni ed entità di attribuzione private.

Il processo di attribuzione richiede solo pochi secondi

Con Kaspersky Threat Attribution Engine, il processo di attribuzione richiede solo pochi secondi, anziché mesi o anni come in passato.

Kaspersky Threat Attribution Engine amplia e consolida

il portfolio Kaspersky dedicato ai Security Operations Center (SOC) di natura commerciale e alle agenzie di cybersecurity nazionali, fornendo un prezioso supporto nella definizione di un efficace processo di gestione degli incidenti.

Kaspersky APT Intelligence Reporting

I clienti Kaspersky APT Intelligence Reporting beneficiano dell'accesso costante ed esclusivo alle nostre 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 operativa con informazioni per il board rilevanti e facili da capire che descrivono l'APT correlata, insieme a una descrizione tecnica dettagliata dell'APT con i relativi IOC e le regole YARA, per fornire ai ricercatori, agli analisti di malware, agli ingegneri, agli analisti della sicurezza di rete e ai ricercatori di APT dei dati che consentono una risposta rapida e precisa alla minaccia.

I nostri esperti segnalano immediatamente eventuali modifiche rilevate nelle tattiche dei gruppi cybercriminali. Sarà inoltre garantito l'accesso al database completo dei report APT, un altro potente strumento di analisi e ricerca nell'ambito delle vostre difese di sicurezza.

Oltre 300
threat actor

Oltre 160
report privati all'anno

Oltre 12.000
IoC

Oltre 400
cyberspionaggio

Oltre 700
Regole Yara

Kaspersky APT Intelligence Reporting fornisce

Profili dei threat actor

Mapping in MITRE ATT&CK

Introduzione

Informazioni per i responsabili aziendali

Analisi tecnica approfondita
- Metodi di attacco
- Exploit utilizzati
- Descrizione del malware
- Descrizione dell'infrastruttura e dei protocolli C&C
- Analisi delle vittime
- Analisi dell'esfiltrazione dei dati
- Attribuzioni

Conclusioni e raccomandazioni

Indicatori di Compromissione (IOC) e regole Yara

Vantaggi di Kaspersky APT Intelligence Reporting

Informazioni sulle APT non pubbliche

Per diversi motivi, non tutte le minacce di alto profilo vengono rese note pubblicamente, ma le condivideremo con voi

Accesso privilegiato

Ricezione di descrizioni tecniche sulle minacce più recenti mentre sono in corso le indagini, prima della divulgazione pubblica

Analisi retrospettiva

Per tutta la durata 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, oltre all'accesso alle regole YARA

Intelligence sui profili dei threat actor

Includono il presunto Paese di origine e l'attività principale, le famiglie di malware utilizzate, i settori operativi e le aree geografiche colpite, oltre alle descrizioni di tutte le TTP utilizzate, con mappatura in MITRE ATT&CK

Integrazione e automazione immediate

Integrazione e automazione immediate dei workflow di sicurezza esistenti con l'API RESTful

Monitoraggio continuo delle campagne APT

Accesso a intelligence applicabile durante le indagini con informazioni sulla distribuzione APT, IOC, infrastrutture di command and control e così via

MITRE ATT&CK

Tutti i TTP descritti nei report sono mappati a MITRE ATT&CK, consentendo di migliorare la detection e response attraverso lo sviluppo e la prioritizzazione dei corrispondenti use case del monitoraggio della sicurezza, eseguendo analisi delle differenze e testando le difese attuali contro i TTP rilevanti.

Kaspersky Crimeware Intelligence Reporting

Il cybercrime motivato finanziariamente non si limita a colpire specifici settori verticali. E mentre continuano gli attacchi alle infrastrutture finanziarie come bancomat e dispositivi PoS (Point of Sale), qualsiasi azienda di ogni settore è a rischio di ransomware. Negli ultimi due anni c'è stato un assottigliamento dei confini tra diversi tipi di minacce e diversi tipi di threat actor. Un esempio è la comparsa sulla scena di campagne APT (Advanced Persistent Threat) focalizzate non sul cyberspionaggio, ma sul furto: rubare denaro per finanziare altre attività in cui il gruppo ATP è coinvolto. La crescente sofisticazione delle minacce del crimeware non deve essere sottovalutata.

Kaspersky Crimeware Intelligence Reporting potenzia le strategie difensive con informazioni tempestive sulle campagne di malware, sugli attacchi rivolti alle istituzioni finanziarie e sugli strumenti di crimeware utilizzati per attaccare banche, società di elaborazione dei pagamenti e le loro infrastrutture specifiche.

Kaspersky Crimeware Intelligence Reporting assicura

- Descrizioni dettagliate di malware popolari, diffusi e molto pubblicizzati
- Note dei ricercatori e alert tempestivi, incluse informazioni sulle minacce nuove e aggiornate
- Informazioni su campagne malware pericolose e diffuse
- Descrizioni dettagliate delle minacce alle infrastrutture finanziarie e degli strumenti di attacco sviluppati o venduti dai criminali informatici sul Dark Web in varie aree geografiche

Vantaggi di Kaspersky Crimeware Intelligence Reporting

Accesso privilegiato

Ricezione di descrizioni tecniche sulle minacce più recenti mentre sono in corso le indagini, prima della divulgazione pubblica

Analisi retrospettiva

Per tutta la durata dell'abbonamento è disponibile l'accesso all'archivio dei report privati

Integrazione e automazione immediate

Integrazione e automazione immediate dei workflow di sicurezza esistenti con l'API RESTful

Accesso ai dati tecnici

È incluso un ampio elenco di IoC, disponibile in formati standard quali OpenIOC o STIX, oltre all'accesso alle regole YARA

Informazioni sui profili degli autori del crimeware

Includono il presunto Paese di origine e l'attività principale, le famiglie di malware utilizzate, i settori operativi e le aree geografiche colpite, oltre alle descrizioni di tutte le TTP utilizzate, con mappatura in MITRE ATT&CK

Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting fornisce informazioni approfondite e una maggiore consapevolezza delle campagne dannose che prendono di mira le organizzazioni industriali, nonché informazioni sulle vulnerabilità riscontrate nei sistemi di controllo industriale più diffusi e nelle tecnologie sottostanti. I report vengono distribuiti tramite Kaspersky Threat Intelligence Portal, pertanto è possibile iniziare immediatamente a utilizzare il servizio.

Tutte le ricerche di Threat Intelligence relative a ICS sono condotte da un team dedicato, Kaspersky ICS CERT:

- Fondato nel 2016
- Il primo team CERT creato da un'organizzazione commerciale
- Circa 20 esperti altamente qualificati in ricerca su minacce e vulnerabilità ICS, incident response e analisi della security

Report inclusi nell'abbonamento

Report sugli APT

Report sui nuovi APT e campagne di attacco di elevata intensità rivolte a organizzazioni industriali, oltre ad aggiornamenti sulle minacce attive

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

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

Evoluzione del 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

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

Valutazione delle vulnerabilità

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

Correlare

Eventuali attività dannose e sospette rilevate negli ambienti industriali con i risultati delle ricerche di Kaspersky, per attribuire la vostra detection alla campagna dannosa in questione, identificare le minacce e rispondere tempestivamente agli incidenti

Sfruttare le 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 Digital Footprint Intelligence

Con l'espansione delle attività di business, crescono anche la complessità e la distribuzione dei vostri ambienti IT, presentando una sfida: proteggere la vostra realtà digitale distribuita senza controllo diretto o 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: è quindi vitale disporre di un quadro ampio e dettagliato riguardo alla presenza online dell'azienda. Allo stesso tempo, è essenziale poterne monitorare i progressivi cambiamenti e saper reagire prontamente alle minacce che mettono a rischio gli asset digitali esposti.

Anche se le imprese fanno uso di una vasta gamma di strumenti nelle proprie attività di sicurezza informatica, continuano a incombere numerose minacce digitali, che richiedono capacità molto specifiche: rilevare e mitigare le fughe di dati, monitorare i piani e gli insidiosi schemi di attacco dei criminali informatici che popolano i forum del Dark Web, ecc. Kaspersky ha creato Kaspersky Digital Footprint Intelligence per aiutare gli analisti di sicurezza a scoprire in che modo gli autori degli attacchi intendono compromettere le risorse dell'azienda, scoprire prontamente i potenziali vettori di attacco a loro disposizione e adattare di conseguenza le difese informatiche.

Kaspersky Digital Footprint Intelligence fornisce

Ricognizione della rete

Identificazione delle risorse di rete del cliente e dei servizi esposti, potenziale punto di ingresso per un attacco. Analisi su misura delle vulnerabilità esistenti, con un ulteriore punteggio e una valutazione completa del rischio basata sul punteggio CVSS di base, sulla disponibilità di exploit pubblici, sull'esperienza di penetration test e sulla posizione della risorsa di rete (hosting/infrastruttura).

Protezione del brand

Monitoraggio e blocco dell'uso non autorizzato del brand di un'azienda online. Identificazione di account e applicazioni di social media falsi, siti Web di phishing e altre attività fraudolente che possono danneggiare la reputazione di un'azienda e/o ingannare i clienti. Rimozione di applicazioni e account di social network falsi nei marketplace per dispositivi mobili.

Monitoraggio del Dark Web

Monitoraggio continuo di risorse sul Dark Web (forum, blog sul ransomware, messenger, siti Tor e così via), per il rilevamento di eventuali riferimenti e minacce all'azienda, ai clienti e ai partner. Analisi di attacchi mirati attivi o in fase di pianificazione e delle campagne APT volte a colpire l'azienda, il settore o le aree geografiche in cui l'impresa svolge le proprie attività di business.

Rilevamento delle fughe di dati

Rilevamento di credenziali compromesse di dipendenti, partner e clienti, carte bancarie, numeri di telefono e altre informazioni sensibili che possono essere utilizzate per eseguire un attacco o mettere a rischio la reputazione della vostra azienda.

Fonti di intelligence

È essenziale avere una completa comprensione dell'approccio alla sicurezza esterna della vostra azienda. Per fornire queste informazioni, gli analisti della sicurezza di Kaspersky raccolgono e aggregano informazioni dalle seguenti fonti di intelligence:

Dati non strutturati dell'azienda

- Indirizzi IP
- Domini aziendali
- Marchi
- Keyword

Inventario del perimetro di rete

Surface, deep e dark web

Knowledge Base di Kaspersky

Report analitici

Alert sulle minacce

10 richieste di rimozione all'anno

Ricerca in tempo reale nelle fonti Kaspersky, in OSINT, nel Surface Web e nel Dark Web

Come funziona

Configurazione	Raccolta	Filtro	Reazione
Rilevamento di informazioni sugli asset digitali dell'azienda	Raccolta automatizzata dei dati da Surface, Deep e Dark Web e dal database di Threat Intelligence di Kaspersky	Rilevamento, analisi e definizione delle priorità delle minacce gestiti dagli analisti	Invio di informazioni di intelligence complete

Valore aziendale

Kaspersky Digital Footprint Intelligence assicura importanti vantaggi e un valore significativo alla vostra organizzazione:

Protezione del brand

Rileva le potenziali minacce in tempo reale per proteggere la reputazione del brand, preservare la fiducia dei clienti, ridurre il rischio di perdite finanziarie e danni per le operazioni aziendali.

Riduzione dei rischi informatici

Fornite alle parti interessate (CxO e consiglio di amministrazione) le informazioni su dove concentrare la spesa per la cybersecurity, rivelando le lacune nella configurazione attuale e i rischi che comportano.

Reazione più rapida

Il contesto aggiuntivo per gli avvisi di sicurezza migliora la risposta agli incidenti e riduce il tempo medio di risposta (MTTR)

Riduzione della superficie di attacco

Gestite la presenza digitale della vostra azienda e controllate le risorse di rete esterne per ridurre al minimo i vettori di attacco e le vulnerabilità che possono essere sfruttate per un attacco.

Conoscenza degli avversari

L'informazione è fondamentale: scoprite cosa stanno pianificando i cybercriminali nel Dark Web in merito alla vostra azienda in modo da essere preparati.

Conoscere l'ignoto

Migliorate la vostra capacità di resistere agli attacchi informatici e di identificare le minacce che non rientrano nella giurisdizione dei vostri team di sicurezza interni.

Kaspersky Takedown Service

Visibilità completa

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

Gestione end-to-end

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

Protezione globale

Ovunque sia registrato un dominio dannoso o di phishing, Kaspersky ne richiederà il takedown all'organizzazione locale presso l'autorità legale competente

Integrazione con Kaspersky Digital Footprint Intelligence

Kaspersky Takedown Service può essere acquistato separatamente, ma l'integrazione con Kaspersky Digital Footprint Intelligence sfrutta al massimo la naturale sinergia tra questi servizi. Kaspersky Digital Footprint Intelligence offre notifiche in tempo reale sui domini malware e di phishing che possono essere inviati immediatamente a Kaspersky Takedown Service per il blocco.

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 portare a una perdita di denaro, danni al brand, perdita di fiducia dei clienti, perdite di dati e altro ancora. Ma la gestione della rimozione di questi domini è un processo complesso che richiede esperienza e tempo.

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 ai clienti di risparmiare tempo e risorse preziosi. Il servizio viene fornito a livello globale.

Kaspersky blocca oltre 15.000 URL di phishing/truffa e previene ogni giorno oltre un milione di clic su tali URL. Grazie ai molti 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 Team (CERT) 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, ecc.) in possesso dei diritti legali necessari per eliminare il dominio Riceverete le notifiche in ogni fase del processo, fino alla rimozione della risorsa desiderata

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.

Kaspersky Ask the Analyst

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

In un'era di attacchi informatici che paralizzano le aziende, i professionisti della cybersecurity 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 cybersecurity ben strutturato, non potete sempre aspettarvi che i vostri esperti contrastino da soli le minacce sofisticate: 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.

Una costante ricerca sulle minacce consente a Kaspersky di scoprire, infiltrare e monitorare le community chiuse e i dark forum di tutto il mondo frequentati da 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.

Kaspersky Ask the Analyst estende il nostro portfolio di Threat Intelligence, consentendovi di chiedere indicazioni e approfondimenti su minacce specifiche che state affrontando o a cui siete interessati. Il servizio adatta le potenti funzionalità di ricerca e Threat Intelligence di Kaspersky alle vostre esigenze specifiche, consentendovi di creare solide difese contro le minacce che prendono di mira la vostra azienda.

Risultati di Kaspersky Ask the Analyst (abbonamento unificato basato sulle richieste)

APT e crimeware

Informazioni aggiuntive sui report pubblicati e sulle ricerche in corso (oltre ad APT o al servizio Crimeware Intelligence Reporting)

Descrizioni di minacce, vulnerabilità e relativi IoC

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

Richieste relative a ICS

- Informazioni aggiuntive sui report 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

Intelligence sul Dark Web

- 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

Analisi malware

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

Come funziona

Kaspersky Ask the Analyst può essere acquistato separatamente o in aggiunta a uno dei nostri servizi di Threat Intelligence. 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, sarete informati sul tempo stimato per l'elaborazione.

Casi di successo

1

Ricevete chiarimenti su dati presenti nei report sull'intelligence delle minacce pubblicati in precedenza

2

Ottenete intelligence aggiuntiva per indicatori IoC già forniti

3

Ottenete dettagli sulle vulnerabilità e suggerimenti su come proteggervi dal relativo sfruttamento

4

Ottenete dettagli aggiuntivi sulle specifiche attività del Dark Web alle quali siete interessati

5

Ottenete un report generico su una famiglia di malware che include il comportamento del malware, il potenziale impatto e i dettagli sulle attività correlate osservate da Kaspersky

6

Assegnare le priorità ad alert/ incidenti in modo efficace con informazioni contestuali dettagliate e categorizzazione per i relativi IoC forniti tramite report sintetici

7

Richiedete assistenza per l'identificazione, in caso di attività inusuali relative a una minaccia APT o a un autore di crimeware

8

Inviate file malware per l'analisi completa al fine di capire il comportamento e le funzionalità dei campioni forniti

Vantaggi di Kaspersky Ask the Analyst

Competenze a portata di mano

Ottenete l'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

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 esaustiva tra gli esperti per ampliare le competenze esistenti con le nostre risorse e conoscenze esclusive.

Conclusione

Il contrasto alle attuali minacce informatiche richiede una visione a 360 gradi di tattiche e strumenti utilizzati dagli attori delle stesse. Generare queste informazioni e identificare le contromisure più efficaci richiede una dedizione costante 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, 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 i cyberattacchi mai rilevati prima.

Vantaggi chiave

Consente la visibilità globale delle minacce, la detection tempestiva delle minacce informatiche, l'assegnazione delle priorità agli alert di sicurezza e una response efficace agli incidenti di information security

Le informazioni approfondite su tattiche, tecniche e procedure utilizzate dai threat actor in diversi settori e aree geografiche consentono una protezione proattiva dalle minacce complesse e mirate

Una panoramica completa della vostra security posture con suggerimenti concreti sulle strategie di mitigazione vi consente di concentrarvi sulla strategia difensiva sulle aree identificate come obiettivi principali di cyberattacco

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

L'incident response accelerata e migliorata e le funzionalità di threat hunting aiutano a ridurre significativamente il tempo di permanenza degli attacchi e i possibili danni

Kaspersky Threat Intelligence

Per saperne di più

www.kaspersky.it

#kaspersky
#bringonthefuture