Qual è il tipo di threat intelligence più adatto alla vostra organizzazione?

Threat intelligence su misura

TI su misura per risposte rapide e precise

Kaspersky Cloud Sandbox

Consente di prendere decisioni intelligenti basate sul comportamento di un file, analizzando contemporaneamente la memoria del processo, l'attività di rete, ecc. per comprendere le ultime minacce sofisticate mirate e su misura

Collega i dati TI dettagliati più recenti recuperati da Kaspersky Threat Lookup con un'indagine dettagliata delle origini dei campioni di file, la raccolta di IoC basata sull'analisi comportamentale e il rilevamento di oggetti dannosi non individuati in precedenza

Kaspersky Threat Lookup

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, ecc.

Offre una visibilità globale delle minacce nuove ed emergenti: ciò vi consente di proteggere al meglio l'azienda e di migliorare le attività di incident response

TI su misura per i sistemi e i processi esistenti

Kaspersky CyberTrace

Threat Intelligence Portal che consente l'immediata integrazione dei data feed con le soluzioni SIEM: in tal modo gli analisti possono sfruttare con maggiore efficacia la threat intelligence nei flussi di lavoro delle attività di sicurezza già esistenti

Si integra con tutti i feed TI in formato JSON, STIX, XML e CSV e supporta l'integrazione immediata con numerose soluzioni SIEM e molteplici fonti di log

Riduce considerevolmente il carico di lavoro SIEM analizzando log ed eventi in entrata, eseguendo con rapidità il matching tra dati ottenuti e feed e generando infine i propri avvisi in relazione al rilevamento delle minacce

La combinazione di Kaspersky CyberTrace e Kaspersky Threat Data Feeds consente agli analisti della sicurezza di distillare in modo efficiente enormi quantità di avvisi di sicurezza e di stabilirne la priorità, migliorare e velocizzare il triage e la risposta iniziale, identificare immediatamente gli avvisi critici, decidere consapevolmente quali inoltrare ai team di incident response (IR) e creare difese proattive basate sull'intelligence

TI su misura per il panorama specifico delle minacce

Kaspersky Threat Data Feeds

Integra i feed TI in tempo reale contenenti informazioni su IP, URL e hash di file sospetti e pericolosi con i sistemi di sicurezza esistenti come SIEM, SOAR e le piattaforme di threat intelligence

Automatizza il triage iniziale e fornisce agli specialisti informazioni sufficienti per identificare immediatamente gli avvisi che richiedono ulteriori indagini o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte

Accede a record arricchiti con un contesto finalizzato all'azione (nomi delle minacce, timestamp, geolocalizzazione, indirizzi IP risolti di risorse Web infette, hash, popolarità e così via) che rispondono a domande del tipo "chi, cosa, dove, quando" per identificare gli avversari, prendere decisioni rapide e agire

Kaspersky APT Intelligence Reporting

Fornisce accesso esclusivo alle indagini di Kaspersky e ai relativi risultati, inclusi i dati tecnici completi su ogni APT scoperta, oltre che sulle minacce che non saranno mai rese pubbliche

I report offrono informazioni orientate ai dirigenti di alto livello e facili da capire, insieme a descrizioni tecniche dettagliate delle APT, dei relativi IoC e delle regole YARA per fornire a esperti di cybersecurity, analisti del malware e della sicurezza di rete, security engineer e ricercatori APT dati finalizzati all'azione che consentono di rispondere alle minacce in modo rapido e mirato

Kaspersky ICS Threat Intelligence Reporting

Fornisce informazioni approfondite e una maggiore consapevolezza delle campagne dannose mirate alle organizzazioni industriali, nonché informazioni sulle vulnerabilità presenti nei sistemi di controllo industriale più diffusi e nelle tecnologie sottostanti

I report includono nuove APT e campagne di attacco di elevata intensità rivolte a organizzazioni industriali, cambiamenti significativi nel panorama delle minacce ICS, vulnerabilità appena scoperte e raccomandazioni finalizzate all'azione per mitigarle, comprese informazioni specifiche per area geografica, paese e settore

Kaspersky Crimeware Intelligence Reporting

Consente alle organizzazioni di impostare le proprie strategie difensive fornendo informazioni tempestive sulle campagne di malware, sugli attacchi rivolti alle istituzioni finanziarie ed informazioni sugli strumenti del crimeware utilizzati per attaccare banche, società di elaborazione dei pagamenti e le loro infrastrutture specifiche

Fornisce descrizioni dettagliate di malware popolari, diffusi e altamente pubblicizzati/resi noti, informazioni su campagne di malware pericolose e diffuse e note dei ricercatori/avvisi tempestivi che includono informazioni su minacce di malware nuove e aggiornate

TI su misura per le esigenze del team di sicurezza

Kaspersky Ask the Analyst

Consente di richiedere ai ricercatori Kaspersky indicazioni e insight caso per caso su minacce specifiche da affrontare o a cui si è interessati

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

Kaspersky Digital Footprint Intelligence

Consente agli analisti della sicurezza di esplorare le risorse della vostra organizzazione dal punto di vista di un avversario, di scoprire i potenziali vettori di attacco disponibili e di adottare le difese migliori

Crea un quadro completo sullo stato dell'attacco, identificando i punti deboli da migliorare e rilevando le prove degli attacchi del passato, di quelli in corso e persino di quelli pianificati per il futuro

Può essere combinato in un'unica soluzione con Kaspersky Takedown Service

Kaspersky Takedown Service

Poiché la gestione delle rimozioni dei domini dannosi e di phishing utilizzati per attaccare l'organizzazione e i brand è un processo complesso che richiede competenze e tempo, il servizio attenua rapidamente le minacce poste da questi domini prima che si verifichino danni

Copertura degli scenari di sicurezza

Scenari di sicurezza — Kaspersky Threat Intelligence

Prevenzione	Detection	Indagini	Risposta	Strategica reporting
Kaspersky Threat Data Feeds	Kaspersky Threat Data Feeds Kaspersky CyberTrace Kaspersky Ask the Analyst	Kaspersky Threat Lookup Kaspersky Research Sandbox Kaspersky Threat Attribution Engine Kaspersky CyberTrace TTP da Kaspersky APT Intelligence Reporting TTP da Kaspersky Crimeware Intelligence Reporting TTP dai report di Kaspersky ICS Kaspersky Ask the Analyst	Kaspersky Takedown Service	Kaspersky Digital Footprint Intelligence Sintesi di Kaspersky APT Intelligence Reporting Sintesi di Kaspersky Financial Threat Intelligence Reporting Kaspersky ICS Report su misura

Perché Kaspersky Threat Intelligence

- Un'ampia scelta di fonti di dati che forniscono informazioni sulle minacce attualmente attive in tutto il mondo, compreso il repository dei file dannosi rilevati da Kaspersky in oltre 25 anni
- Accesso immediato alla threat intelligence tecnica, tattica, operativa e strategica fornita dal nostro team composto dai migliori ricercatori e analisti del mondo
- Oltre 20 tipi di feed di dati sulle minacce; sandbox sviluppata internamente che rileva minacce sofisticate ed evasive; Threat Attribution Engine che fornisce informazioni dettagliate sugli autori delle minacce necessarie per la ricerca APT
- Team dedicato composto da esperti di cybersecurity industriale
- Formazione di competenze specifiche per il personale di sicurezza IT
- Collaboratore principale dell'Active Protection Program di Microsoft per la ricerca sulle vulnerabilità

Kaspersky Threat Intelligence

Per saperne di più

www.kaspersky.it