Panorama delle minacce informatiche su Kaspersky Threat Intelligence Portal

Imparate a difendervi dai vostri nemici: scoprite il vero panorama delle minacce per la vostra organizzazione

kaspersky bring on the future

Kaspersky Threat Intelligence Portal

Panorama delle minacce per l'organizzazione su Kaspersky Threat Intelligence Portal

Il panorama delle minacce globali è in continua evoluzione: ogni giorno emergono nuovi metodi di attacco e quelli già noti diventano sempre più sofisticati. Oggi è sempre più importante che i team per la sicurezza delle informazioni siano in grado di stabilire in modo efficace le priorità delle minacce che devono essere affrontate rapidamente. Ma come concentrarsi sulle minacce più rilevanti per la propria azienda, il proprio settore e la propria area geografica?

Portale Kaspersky Threat Intelligence

Gli utenti hanno un'opportunità unica di valutare il panorama delle minacce nella sezione Panorama delle minacce informatiche, che è stata specificamente progettata per fornire informazioni sugli autori degli attacchi che prendono di mira un settore e un'area geografica specifica. La sezione offre un contesto completo e aggiornato sulle minacce associate ai potenziali avversari, alle loro tattiche, tecniche e procedure (TTP).

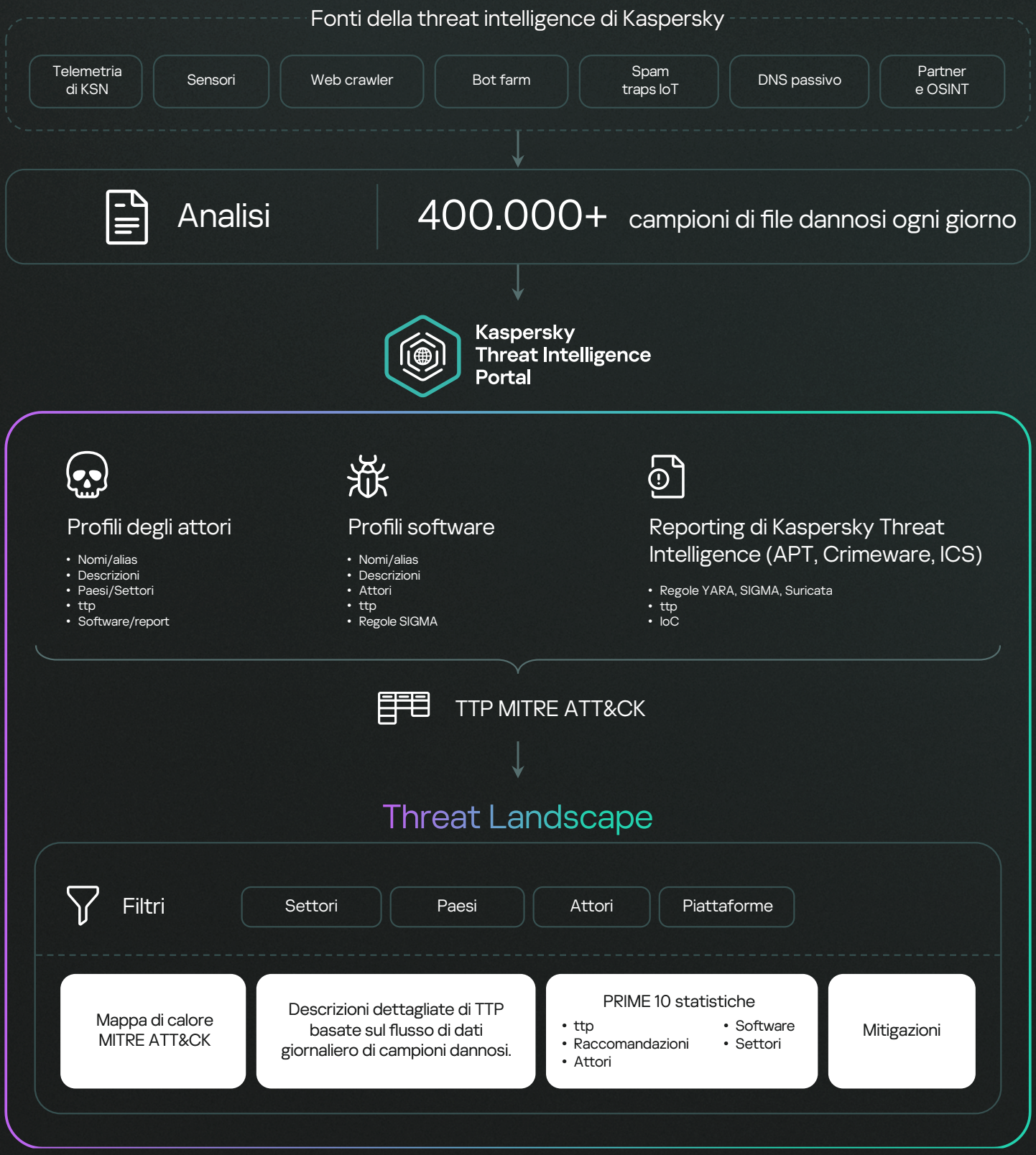
Panorama delle minacce informatiche fornisce informazioni sulle minacce associate a:

- area geografica
- settore
- tipi di minaccia
- threat actor
- tecniche, tattiche e procedure (TTP)
- software dannoso utilizzato
- indicatori di compromissione (IoC)

I dati di intelligence sulle minacce vengono raccolti in tempo reale utilizzando una serie di sistemi avanzati di cui Kaspersky si serve da oltre 25 anni per combattere la criminalità informatica: Kaspersky Security Network, che riceve dati anonimi da milioni di utenti in tutto il mondo, elaborando automaticamente milioni di file al giorno, Web crawler, bot farm, spam traps, honeypot, sensori, DNS passivo, fonti e partner dell'Open e del Dark Web. Noi stessi abbiamo utilizzato questi dati nell'ultimo quarto di secolo, ottenendo i punteggi più alti nei test indipendenti e nelle recensioni esterne. I dati ottenuti vengono attentamente analizzati dai team Kaspersky, dedicati alla ricerca delle minacce. Dati che vengono inoltre elaborati da moderni sistemi automatizzati come sandbox, motori euristici e strumenti di similarità, trasformandoli in informazioni verificate e aggiornate.

Per saperne di più

Come funziona

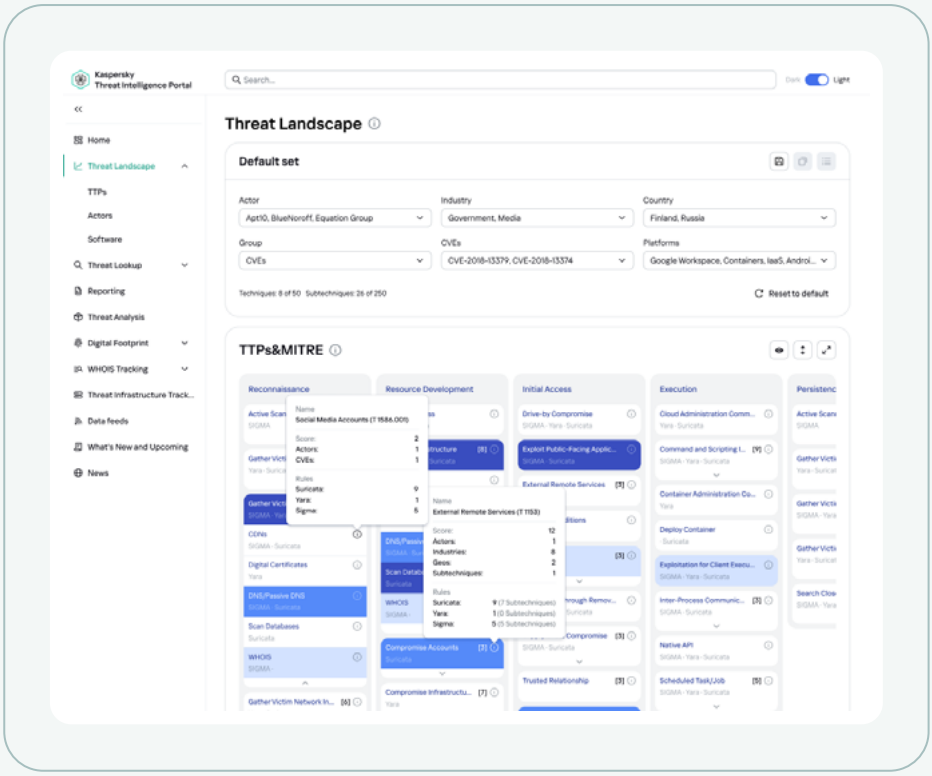


Elaboriamo centinaia di migliaia di campioni di file dannosi ogni giorno, estraendo i dati di geolocalizzazione e di settore. I sistemi interni di Kaspersky estraggono quindi le TTP associate e attribuiscono i file a gruppi di criminali informatici e malware già noti. La sezione Panorama delle minacce informatiche si basa anche su un flusso di dati di incidenti reali provenienti da tutto il mondo, che riceviamo dai nostri team di ricerca formati da esperti.

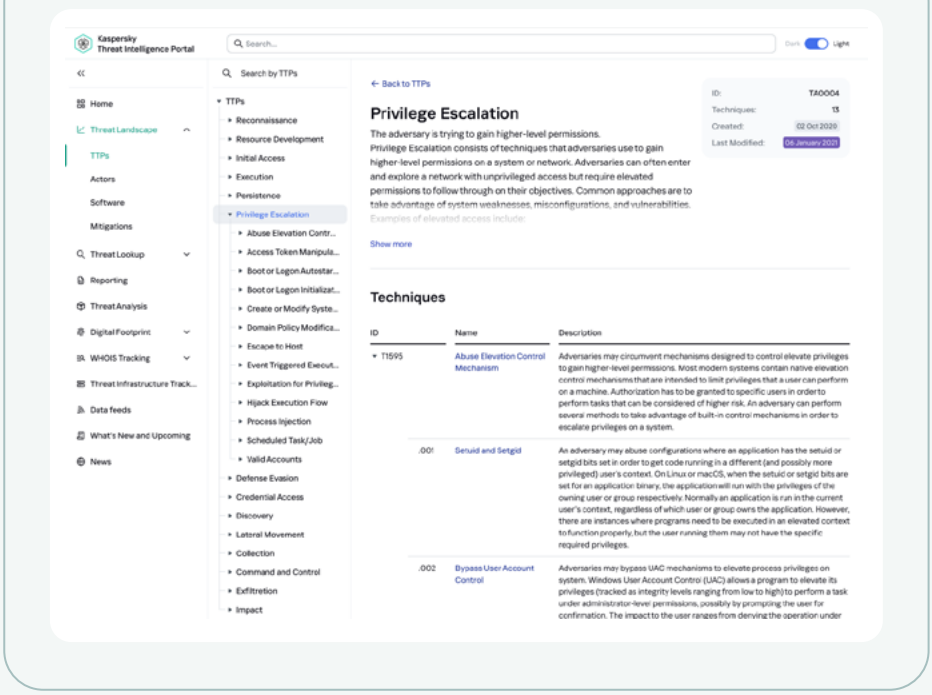
Dopo aver applicato i filtri, gli utenti di Kaspersky Threat Intelligence Portal sono in grado di creare il proprio panorama delle minacce, in linea con il framework MITRE ATT&CK, ottenendo le informazioni più aggiornate sui potenziali avversari: tecniche, tattiche e procedure più probabilmente utilizzate per gli attacchi, descrizioni dettagliate degli attori, del malware e delle TTP utilizzate, report con una descrizione dettagliata degli attacchi e, infine, le mitigazioni, ovvero raccomandazioni specifiche che consentono di evitare che una tecnica venga messa in atto con successo.

Caratteristiche principali

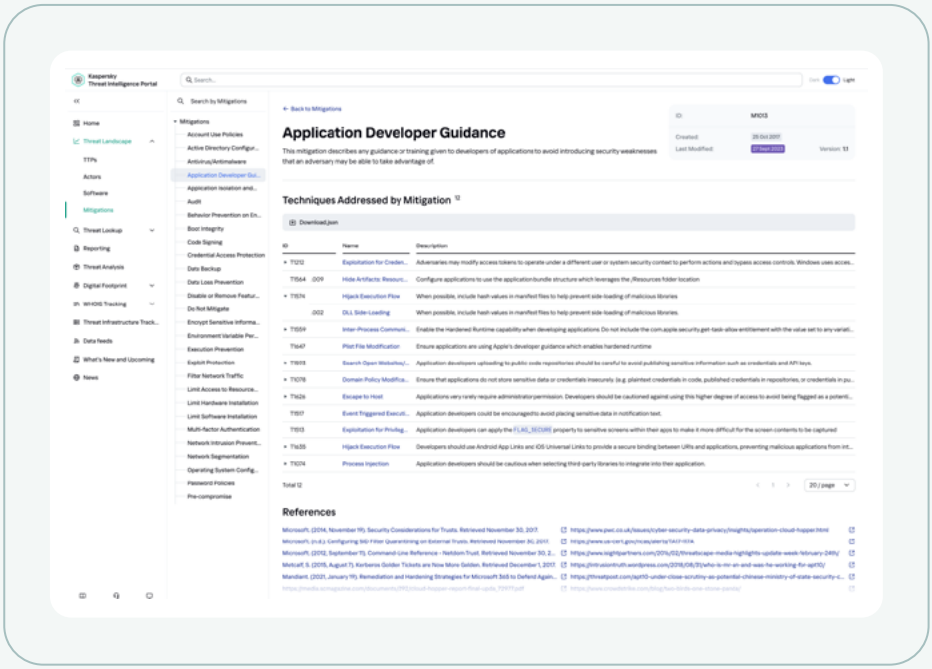
Mappa di calore MITTRE ATT&CK per elaborare un panorama delle minacce unico per l'organizzazione in tempo reale. Applicando i filtri, l'utente ha accesso ai dati più recenti, inclusi gli aggiornamenti delle ultime 24 ore, ottenuti dai nostri sistemi e dai nostri esperti attraverso una ricerca continua. L'utente, avrà la possibilità di salvare i filtri per una successiva analisi.



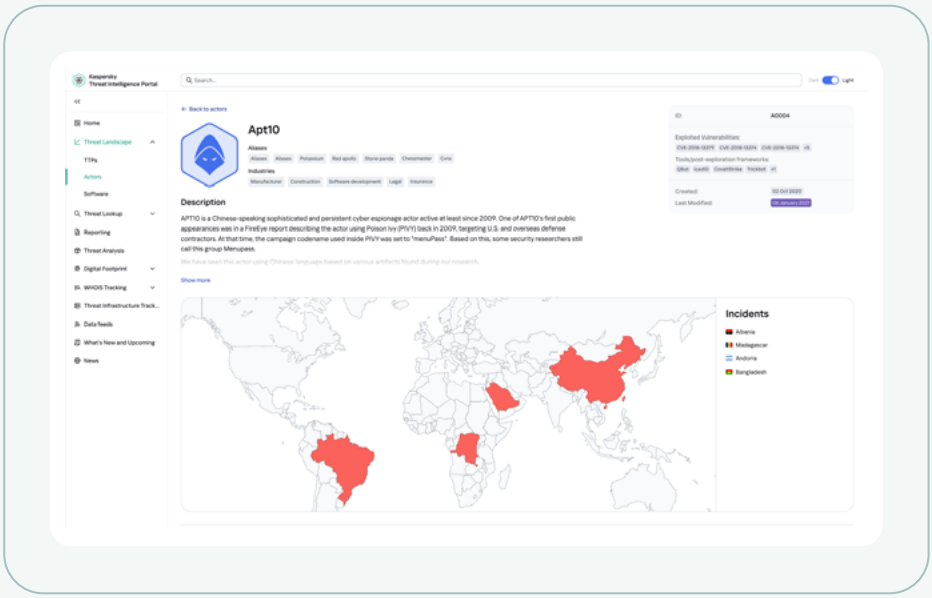
Informazioni in tempo reale sulle tecniche, le tattiche e le procedure degli autori degli attacchi, basate sui sistemi avanzati di Kaspersky.



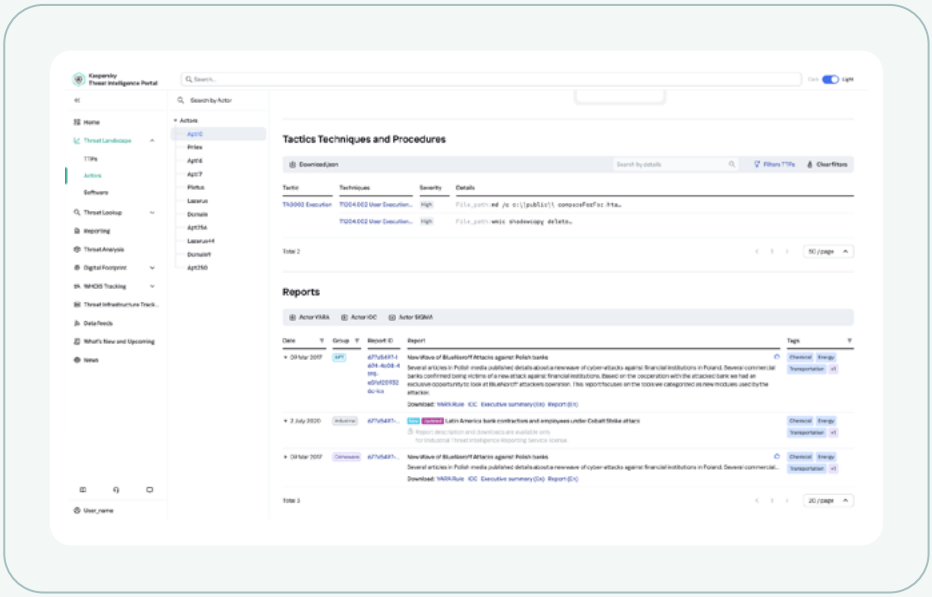
La sezione delle mitigazioni fornisce descrizioni dettagliate delle misure di protezione e di prevenzione che le organizzazioni devono adottare per evitare falle nella sicurezza.



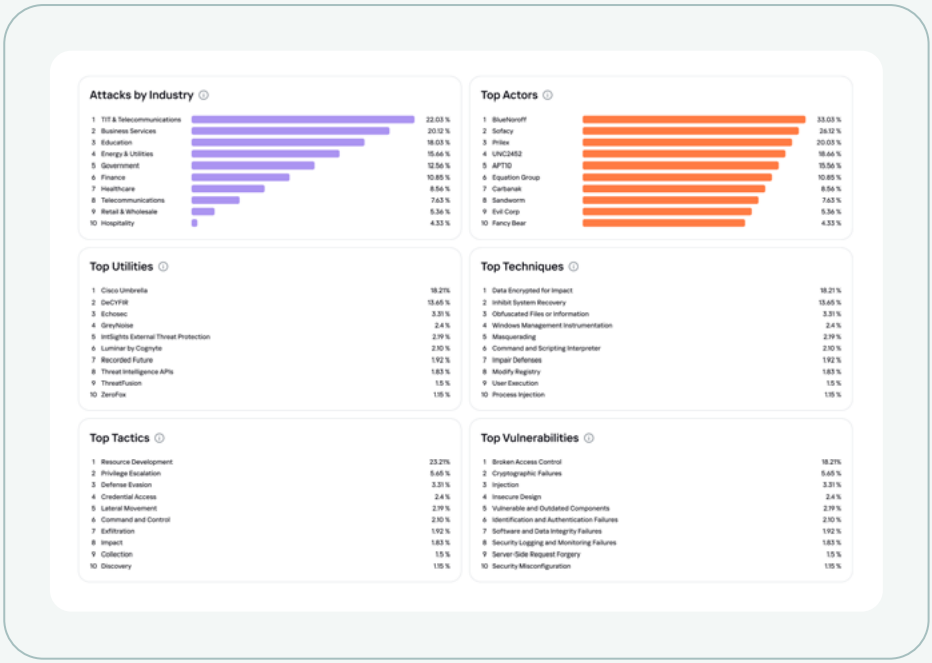
Accesso al repository più vasto del settore di profili di attori e di malware con descrizioni dettagliate compilate dagli esperti Kaspersky.



Accesso alle regole Sigma/ Yara/Suricata relative alle tecniche, alle tattiche e alle procedure MITRE ATT&CK per rilevare le minacce rilevanti per l'organizzazione.



PRIME 10 statistiche su settori, attori, TTP, vulnerabilità e software.



Il mondo in continua evoluzione delle cyberminacce contiene oggi una grande quantità di dati di threat intelligence disponibili attraverso una varietà di prodotti e servizi. Comprendendo il panorama di minacce, le organizzazioni sono in grado di adottare misure strategicamente ragionevoli per difendersi in modo proattivo da attacchi specifici.

Vantaggi dell'utilizzo

Approccio proattivo alla difesa

Imparate a conoscere i vettori di attacco più probabili per l'organizzazione al fine di creare una strategia di difesa efficace

Monitoraggio della superficie di attacco

Identificate le falle nella sicurezza prima che gli autori degli attacchi le sfruttino

Puntare sulle minacce rilevanti

Possibilità di concentrarsi sulle minacce che più probabilmente interesseranno la propria azienda, il proprio settore e la propria area geografica

Pianificazione strategica

Utilizzate le informazioni sul panorama delle minacce per la pianificazione degli investimenti e lo sviluppo di strumenti e metodi di protezione

Maggiore efficienza dei reparti di sicurezza delle informazioni

Aumentate l'efficienza del personale e riducetene i costi grazie all'accesso alle informazioni sulle minacce rilevanti e sulle tendenze globali.

Consapevolezza delle minacce

Consapevolezza delle minacce più recenti e delle tendenze globali per una difesa efficace

Se conosci il nemico e conosci te stesso, non dovrai temere l'esito di cento battaglie. Se conosci te stesso, ma non il tuo avversario, per ogni vittoria subirai una sconfitta. Se non conosci te stesso né il tuo rivale, perderai in ogni battaglia

Sun Tzu

da L'arte della guerra

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence consente di accedere a una serie di informazioni raccolte dai nostri analisti e ricercatori di livello mondiale. Questi dati aiuteranno qualsiasi organizzazione a contrastare efficacemente le odierne minacce informatiche.

La nostra azienda dispone di una profonda conoscenza, di una vasta esperienza nella ricerca sulle minacce informatiche e di una visione unica di tutti gli aspetti della sicurezza informatica. Questo ha reso Kaspersky un partner affidabile delle forze dell'ordine e delle organizzazioni governative di tutto il mondo, tra cui l'Interpol e diverse unità CERT. Kaspersky Threat Intelligence fornisce informazioni aggiornate sulle minacce tattiche, operative e strategiche.

Kaspersky Threat Intelligence

Per saperne di più

www.kaspersky.it

#kaspersky
#bringonthefuture