Servizio completo
di protezione dai rischi digitali

Kaspersky Digital Footprint Intelligence

kaspersky bring on the future

Domande per esperti

Qual è il miglior modo per lanciare un attacco contro la vostra azienda?

Qual è il metodo di attacco più efficiente e vantaggioso in termini di costi?

Quali sono le informazioni di cui dispone un attaccante 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 attacchi attuali e a quelli pianificati per il futuro.

Introduzione

Man mano che cresce il vostro 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 e così via. Per aiutare i security analyst 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 cybercriminali e adeguare di conseguenza le difese, Kaspersky ha creato la soluzione Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence fornisce

Kaspersky Digital Footprint Intelligence è un servizio completo di protezione dai rischi digitali che aiuta i clienti a monitorare le proprie risorse digitali e a rilevare le minacce provenienti da Surface, Deep e Dark Web.

Ricognizione di rete

Identificazione delle risorse di rete e dei servizi esposti che potrebbero essere un potenziale punto di ingresso di un attacco. Analisi su misura delle vulnerabilità esistenti, che permettono di attribuire un punteggio e una valutazione completa del rischio, che si baserà sul punteggio CVSS di base, sulla disponibilità di exploit pubblici, sull'esperienza di penetration test e sulla posizione della risorsa di rete (hosting /infrastruttura).

Monitoraggio del Dark Web

Monitoraggio continuo di decine 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.

Rilevamento delle minacce

Monitoraggio delle attività fraudolente che possono danneggiare la reputazione di un'azienda e/o illudere i clienti.

Supporto multitenancy

Funzionalità ottimizzate per gli MSSP (Managed Security Service Provider) e le grandi organizzazioni con una struttura multi-filiale.

Come funziona

Configurazione	Raccolta	Reazione	Filtro
Rilevamento di informazioni sugli asset digitali dell'azienda	Raccolta automatizzata dei dati da Surface, Deep Web e Dark Web e dalla Knowledge Base di Kaspersky	Fornitura di notifiche operative sulle minacce in Kaspersky Threat Intelligence Portal o tramite API	Rilevamento, analisi e definizione delle priorità delle minacce gestiti dagli analisti

Elementi principali del servizio

1. Dashboard utili con statistiche dettagliate
2. Possibilità di ricerca nel database del Dark Web
3. Avvisi sulle minacce in Threat Intelligence Portal
4. Possibilità di ricerca nel database dei social media
5. Presentazioni e sessioni di domande e risposte con esperti
6. Dati machine-readable
7. Report di analisi compilati dai nostri esperti*
8. Richieste di ricognizione*

*Servizio Add-on

Tipologie di minacce

Kaspersky Digital Footprint Intelligence consente alle organizzazioni di rispondere in modo rapido ed efficiente alle potenziali minacce informatiche, grazie ad avvisi in tempo reale. Riduce la probabilità di danni alla brand reputation, mantenendo quindi la fiducia dei clienti e le operazioni aziendali in generale. Le aziende possono personalizzare le capacità di monitoraggio del servizio per soddisfare le loro esigenze specifiche, mentre report e analisi completi offrono preziose informazioni sulla portata e sull'impatto della violazione del brand e di altri potenziali rischi.

Minacce correlate al perimetro della rete

- Servizi di rete configurati in modo errato
- Identificazione delle vulnerabilità
- Risorse alterate o compromesse

Minacce relative al dark web

- Schemi di frode e piani di attacco
- Vendita violazione dei dati
- Attività interne

Data leak

- Risorse aziendali compromesse
- Carte di credito compromesse
- Credenziali compromesse

Minacce correlate al malware

- Attacchi di phishing
- Attacchi mirati
- Campagne APT

Fonti di intelligence

È essenziale che i nostri clienti abbiano una completa comprensione del loro approccio alla sicurezza esterna. 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
- Brand
- Keyword
- Intervalli di rete
- Numeri di carte BIN/IIN
- Informazioni sui dipendenti

Inventario del perimetro di rete

Ricerca Surface, Deep e Dark Web

Ricerca all'interno della Knowledge Base di Kaspersky

Avvisi sulle minacce

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

Richieste di takedown*

Report analitici*

Capacità di erogazione del servizio

Digital Footprint Intelligence fornisce funzionalità avanzate per gli MSSP e le grandi organizzazioni multi-filiale.

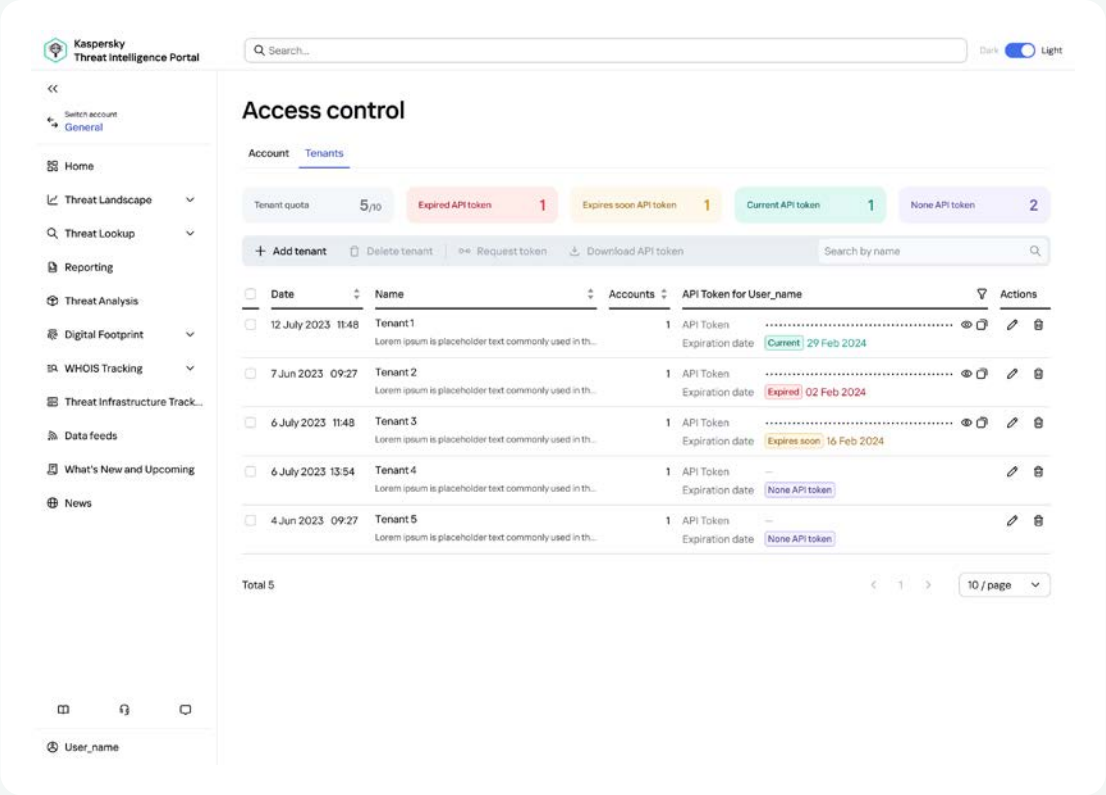
L'interfaccia di Kaspersky Threat Intelligence Portal, attraverso il quale viene fornito il servizio DFI, consente agli MSSP di differenziare l'accesso alle informazioni relative alle filiali delle grandi organizzazioni o alle singole organizzazioni a cui gli MSSP offrono servizi di gestione della sicurezza.

Creazione di tenant separati e configurazione del controllo degli accessi

La gestione viene eseguita attraverso la creazione di tenant: entità logiche create per ogni nuova struttura, che deve essere gestita separatamente dagli altri.

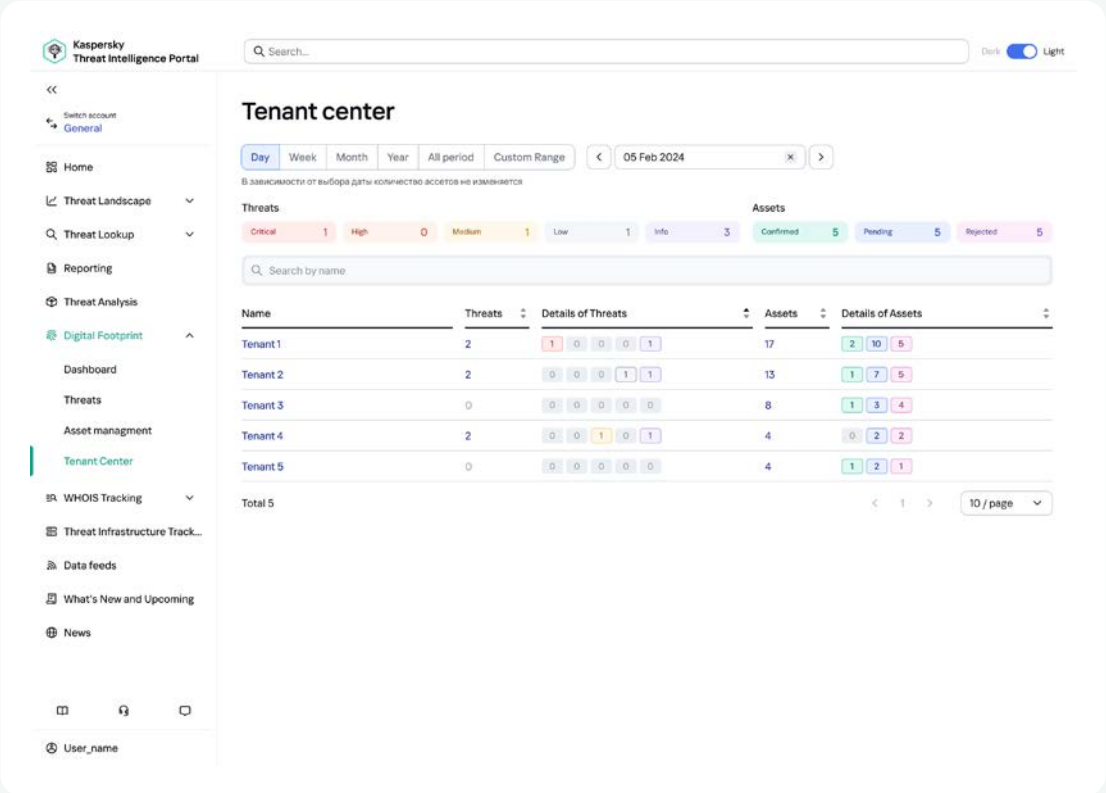
1. Accesso a tutte le risorse e le notifiche delle minacce specifiche per i tenant
2. Cambio di gruppo di tenant semplificato e visualizzazione delle informazioni specifiche per quel tenant
3. Controllo degli accessi tramite token API e TOTP
4. Capacità di cambiare le licenze dei tenant

*Servizio Add-on



Statistiche centralizzate sulle risorse e le minacce di ciascun tenant

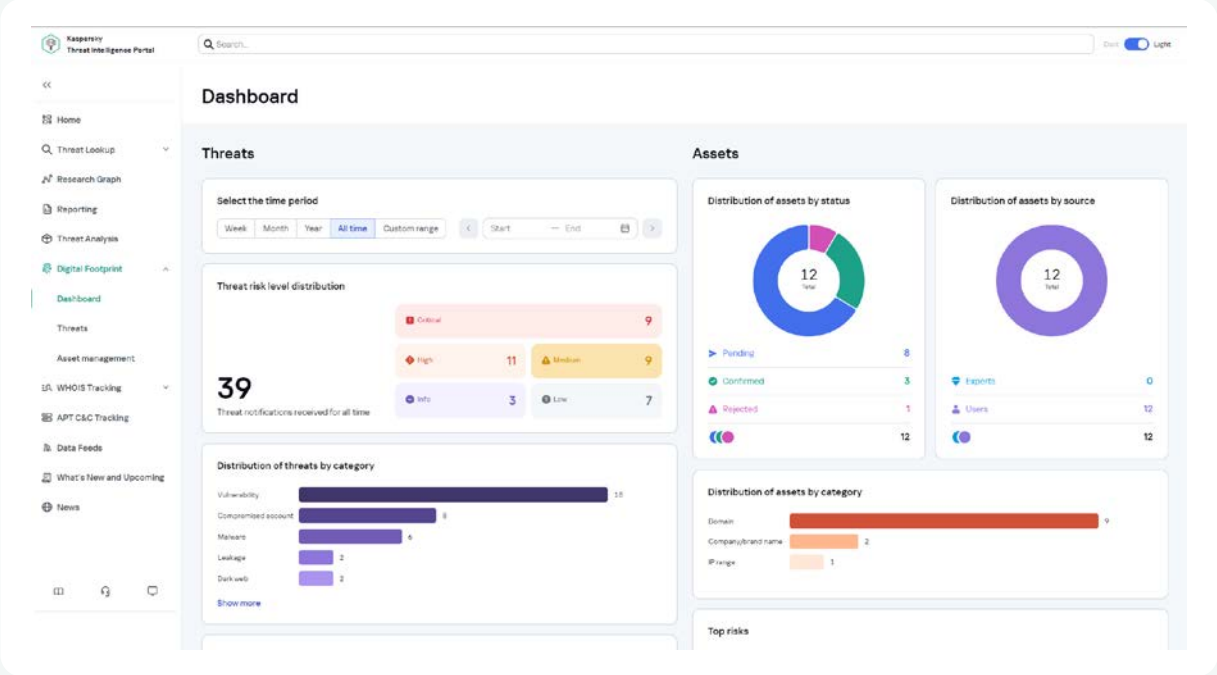
Fornendo il servizio a un gran numero di organizzazioni, è necessario disporre di strumenti per monitorare lo stato attuale dei tenant. Il Tenant Center consente di visualizzare il riepilogo di ciascun tenant, incluso il numero delle minacce rilevate con il relativo livello di criticità, nonché informazioni sulle risorse che i tenant vorrebbero monitorare e sui relativi stati.



Monitoraggio dettagliato

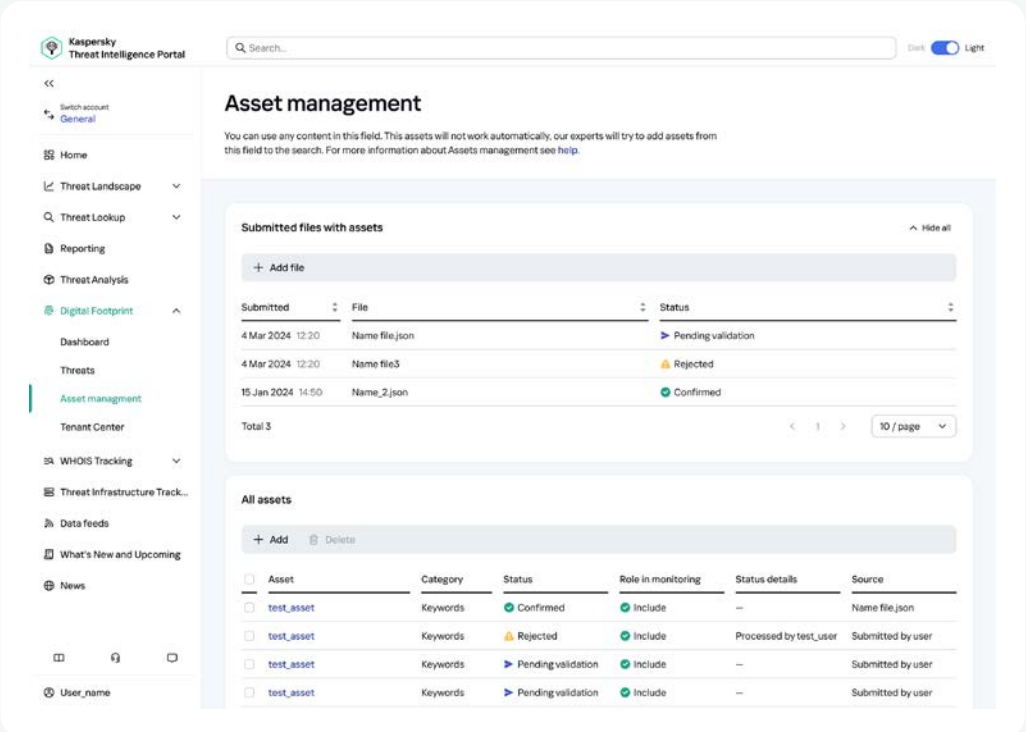
L'MSSP o la sede centrale possono visualizzare un riepilogo dettagliato per ciascun tenant:

- Il numero totale di minacce identificate in un dato periodo e il relativo livello di criticità per l'organizzazione
- Categorizzazione delle minacce rilevate
- Le risorse più vulnerabili del tenant
- Panorama delle minacce che cambia nel corso del tempo



Gestione delle risorse

L'amministratore del tenant è in grado di aggiungere nuove risorse per il monitoraggio sia separatamente tramite l'interfaccia di Kaspersky Threat Intelligence Portal sia caricando file con una grande quantità di risorse. Questo approccio semplifica essenzialmente il processo di aggiornamento delle risorse.



Valore aziendale

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

Protegge il vostro 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.

Efficienza di fornitura del servizio

L'avvio rapido e la facile scalabilità in modalità multi-tenancy consentono di risparmiare tempo sia per i fornitori di servizi di sicurezza gestiti (MSSP) che per i loro clienti, nonché per le grandi organizzazioni con numerosi filiali.

Per saperne di più sui vari piani di abbonamento, contattate il nostro team.

Contattateci

Kaspersky Digital Footprint Intelligence

Ulteriori informazioni

www.kaspersky.it

#kaspersky
#bringonthefuture