Kaspersky Threat Intelligence

Mantenete il vantaggio rispetto agli avversari

kaspersky

Fonti della threat intelligence di Kaspersky

Kaspersky Threat Intelligence consente di accedere a un'ampia gamma di informazioni raccolte dai nostri analisti e ricercatori di livello mondiale per aiutare l'organizzazione a contrastare efficacemente le odierne minacce informatiche.

Threat Intelligence basata su competenze e conoscenze globali uniche

Ogni centro contribuisce alle soluzioni e ai servizi Kaspersky

- Ricerca sulle minacce
- Incident investigation

Kaspersky Global Research and Analysis Team

- Ricerca delle minacce più complesse: APT, campagne di cyberspionaggio, cyber epidemie globali, ecc.
- Sicurezza delle tecnologie orientate al futuro
- Indagine sul cybercrimine finanziario sofisticato

Kaspersky Ricerca sulle minacce

- Ricerca anti-malware
- Ricerca sul filtraggio dei contenuti
- SSDLC e metodologie secure-by-design

Kaspersky AI Technology Research

- Cybersecurity AI
- Ricerca AI generativa
- Rilevamento delle minacce basato su AI/soluzioni

Kaspersky Servizi di sicurezza

- MDR
- Incident response
- Security Assessment
- Consulenza SOC
- Digital Footprint Intelligence

Kaspersky ICS CERT

- Analisi delle minacce delle infrastrutture critiche
- Ricerca e valutazione delle vulnerabilità ICS
- Associazioni, analisi e standard tecnologici

Caratteristiche principali di Kaspersky Threat Intelligence

La profonda conoscenza, la vasta esperienza nella ricerca sulle minacce informatiche e la visione unica di tutti gli aspetti della sicurezza informatica hanno fatto di Kaspersky il partner di fiducia per le aziende di tutto il mondo e un valido alleato per le agenzie governative e le forze dell'ordine, tra cui l'Interpol e diverse unità CERT.

Copertura delle minacce globali, con una profonda esperienza nella ricerca delle minacce nelle aree geografiche in cui ha origine la maggior parte degli attacchi

Contributo continuo degli esperti Kaspersky

Threat Intelligence per i segmenti IT e OT

Caratteristiche principali di Kaspersky Threat Intelligence

Teniamo traccia di:

oltre 300

threat actor

oltre 500

campagne di cyberspionaggio

oltre 200

report privati prodotti all'anno

oltre 170000

IoC correlati ai report

oltre 2 500

regole YARA correlate ai report

Livelli di dati sulla Threat Intelligence

Tattica

Informazioni di basso livello e altamente volatile che supportano le operazioni di sicurezza e la risposta agli incidenti. Un esempio di intelligence tattica è rappresentato dagli IOC relativi alla condotta di un attacco appena scoperto.

Ruoli:

- Analista SOC

Systems:

- SIEM
- NGFW
- SOAR
- IPS
- IDS

Processi:

- Threat Hunting
- Monitoraggio

Operativa

Questo livello include in genere dati sulle campagne e sulle TTP di ordine superiore. Può includere informazioni sull'attribuzione di attori specifici e sulle capacità e le intenzioni degli avversari.

Ruoli:

- Analista SOC L3
- Analista DFIR
- Analista IR

Systems:

- SIEM
- NTA
- TIP
- EDR/XDR

Processi:

- Incident response
- Threat Hunting

Strategica

Questo livello supporta i top manager e i consigli di amministrazione che devono prendere decisioni serie sulla valutazione dei rischi, sull'allocazione delle risorse e sulla strategia organizzativa. Queste informazioni includono le tendenze, le motivazioni degli attori e le loro classificazioni.

Ruoli:

- CISO
- CTO
- CIO
- CEO

Processi:

- Creazione di una strategia IS
- Maggiore consapevolezza

Formati di distribuzione della Threat Intelligence

Threat Intelligence machine-readable

Kaspersky Threat Data Feeds

Oltre 30 feed di dati sulle minacce basati sulle diverse esigenze con copertura IT e OT e piattaforma TI

Threat Intelligence human-readable

Kaspersky Threat Intelligence Portal

Il portfolio di base di Kaspersky Threat Intelligence per gli ambienti IT e OT con un singolo punto di accesso attraverso Kaspersky Threat Intelligence Portal

Supporto degli esperti per la ThreatIntelligence

Kaspersky Takedown Service

Kaspersky Ask the Analyst

Assistenza avanzata dei professionisti più esperti

Kaspersky Threat Intelligence

Threat Intelligence machine-readable

- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Supporto degli esperti per la Threat Intelligence

- Kaspersky Takedown Service
- Kaspersky Ask the Analyst

Kaspersky Threat intelligence

- Tattica
- Operativa
- Strategia

○ Disponibile tramite

Kaspersky Threat intelligence Portal

Threat Intelligence human-readable

- Kaspersky Threat Lookup
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Analysis
  - Sandbox
  - Attribuzione
  - Similarity
- Kaspersky Threat Intelligence Reporting
  - APT
  - Crimeware
  - ICS
- Kaspersky Threat Infrastructure Tracking

Kaspersky Threat Data Feeds

Oltre 30 feed di dati sulle minacce pronti all'uso per supportare diverse attività

Sono disponibili anche feed di dati creati su misura per l'organizzazione.

- TI tattica
- TI operativa

Feed di dati sulle minacce più comuni

- Malicious URL
- Ransomware URL
- Phishing URL
- Botnet C&C URL
- Mobile Botnet C&C URL
- Hash dannosi
- Mobile Malicious Hashes
- IP Reputation
- URL IoT
- ICS Hashes
- APT Hashes
- APT IP
- APT URL
- Crimeware Hashes
- Crimeware URL

Kaspersky Threat Data Feeds → SIEM, SOAR / IRP, TIP, EDR / XDR

Piattaforma TI

Rendete subito operativi i vari feed di threat intelligence e riducete il workload dei SIEM

Kaspersky CyberTrace

Feed di dati sulle minacce specifiche

Network Security Data Feeds	Feed sulle regole Suricata	Sigma Rules Data Feed	Yara Rules Data Feeds	Feed sulle vulnerabilità	Open Source Software Threats Data Feed
NGFW	IDS / IPS	SIEM / EDR	YARA-scanner	SBOM / CMDB	OSA / CSA / ASOC

Portale Kaspersky Threat Intelligence

Un singolo punto di accesso a Kaspersky Threat Intelligence all'interno di una UI/API unificata, in cui i servizi lavorano insieme, integrandosi e consolidandosi. Combinando tutte le competenze e le conoscenze di Kaspersky sulle minacce informatiche in un'unica posizione. Consente Il monitoraggio delle minacce correlate a una specifica organizzazione attraverso tecnologie proprietarie di elaborazione dei dati e normalizzazione, permettendo di esaminare campioni di malware e la relativa attribuzione.

- TI tattica
- TI operativa
- TI strategica

Versione gratuita di Kaspersky Threat Intelligence Portal

Panorama delle minacce su Kaspersky Threat Intelligence Portal

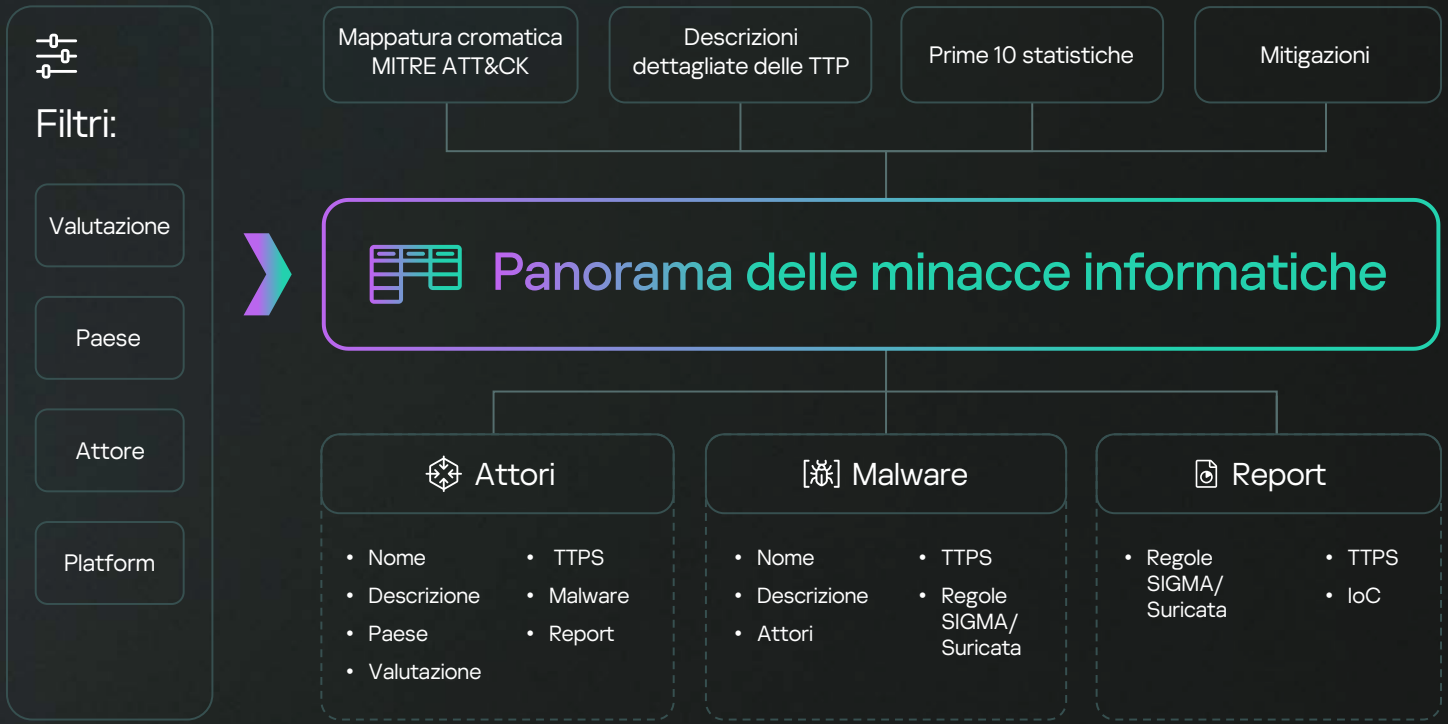
Threat intelligence specifica per il settore e l'area geografica per comprendere le esatte minacce che deve affrontare l'organizzazione

- Allineamento MITRE ATT&CK
- Aggiornamenti in tempo reale basati sulle ricerche continue di Kaspersky
- Profili software e degli avversari Repository di regole di rilevamento

400.000+

file dannosi rilevati quotidianamente

Panorama delle minacce - come funziona



Supporto degli esperti per la Threat Intelligence

Kaspersky Ask the Analyst

- TI operativa
- TI strategica

Il servizio Kaspersky Ask the Analyst estende il nostro portfolio di Threat Intelligence, consentendovi di chiedere informazioni e approfondimenti su minacce specifiche che state affrontando o a cui siete interessati.

Vi offriamo 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.

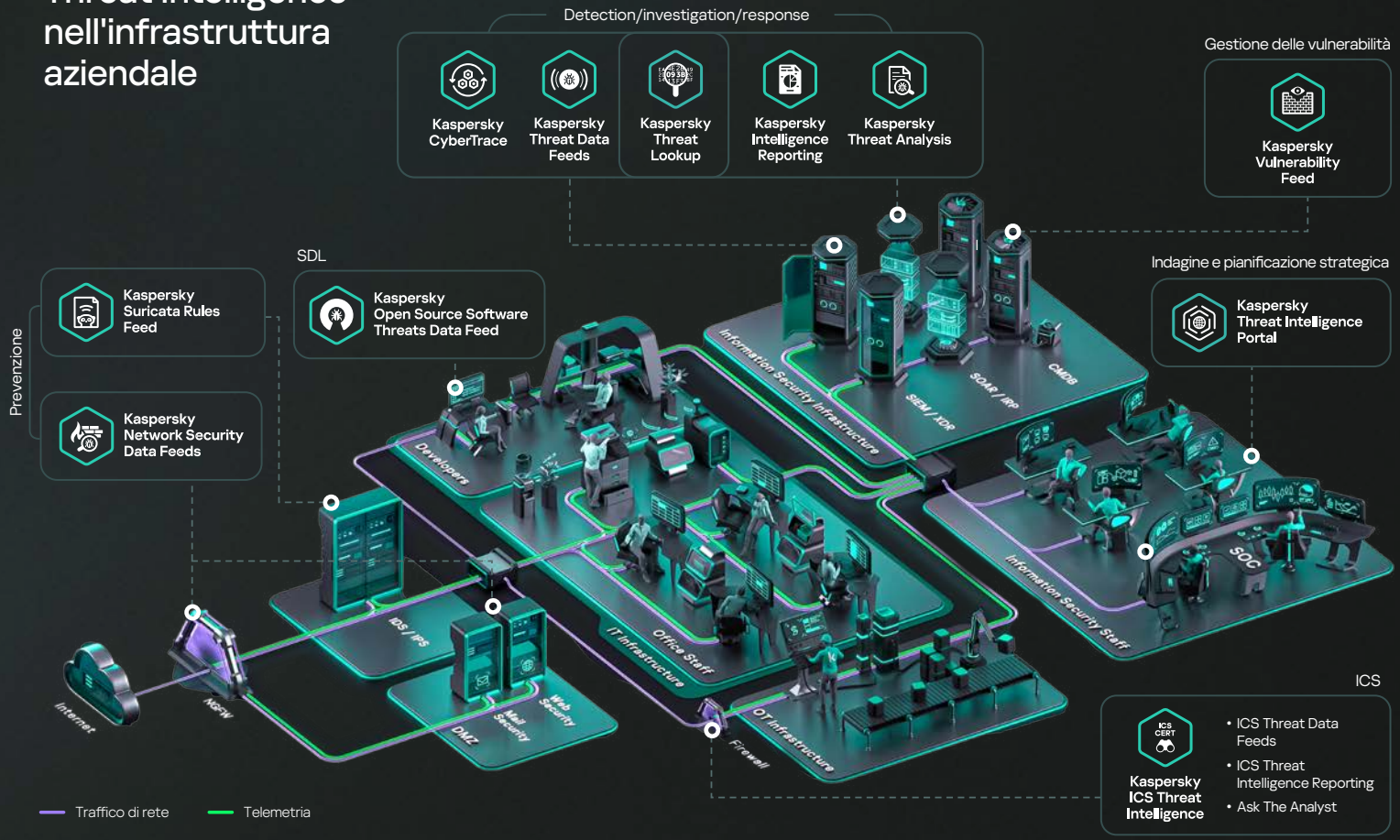
Kaspersky Takedown Service

- TI operativa

Il servizio Kaspersky Takedown Service mitiga rapidamente le minacce costituite dai domini di phishing dannosi prima che possano causare danni al vostro brand e alla vostra azienda. Grazie all'avanzata esperienza nell'analisi dei domini, siamo in grado di raccogliere tutte le prove necessarie per dimostrarne la natura dannosa. Ci occupiamo della gestione e della rimozione.

Il servizio è disponibile a livello globale in collaborazione con organizzazioni internazionali e forze dell'ordine nazionali e regionali.

Esempio di Kaspersky Threat Intelligence nell'infrastruttura aziendale



Offerta di Kaspersky Threat Intelligence Industrial

Threat Intelligence machine-readable

Kaspersky Threat Data Feeds

Dati machine-readable sulle minacce e le vulnerabilità della cybersecurity industriale.

Kaspersky ICS Hashes Data Feed
Kaspersky ICS Vulnerability Data Feed
Kaspersky ICS Vulnerability Data Feed in formato OVAL

Threat Intelligence human-readable

Kaspersky ICS Intelligence Reporting

Accedete a pubblicazioni regolari relative alle minacce e alle vulnerabilità della sicurezza informatica industriale sul Kaspersky Threat Intelligence Portal

Supporto degli esperti per la Threat Intelligence

Kaspersky Ask the Analyst

Consultate direttamente gli esperti Kaspersky ICS CERT per suggerimenti personalizzati sulle minacce e le vulnerabilità della sicurezza informatica industriale, statistiche e panoramiche sulle minacce, standard di settore e molto altro.

Tattica · TI operativa · TI strategica

Perché scegliere Kaspersky Threat Intelligence

Un'offerta TI di livello superiore riconosciuta dagli analisti del settore	Verificato dagli analisti di varie aziende di ricerca globali come Frost & Sullivan, Quadrant Knowledge Solutions, Forrester, IDC ecc.
Molteplici fonti uniche e affidabili per produrre una TI attendibile	L'infrastruttura di Kaspersky Security Network include oltre 100 milioni di sensori in 200 paesi, i maggiori repository di file dannosi e legittimi, Dark Web, attività TH e IR continue, Web crawler, spam trap, ecc.
Competenza di esperti in IT e OT	Oltre 200 esperti certificati di cinque centri di competenza inclusi il team GReAT e ICS-CERT distribuiti a livello internazionale, che parlano più di 20 lingue. Gli esperti Kaspersky sono sempre tra i primi a scoprire le minacce più note, da Stuxnet e WannaCry a Operation Triangulation.
Presenza globale	Una forte presenza nelle aree geografiche in cui ha origine la maggior parte degli attacchi (Russia, CSI, Cina, ecc.) ci assicura la possibilità unica di raccogliere, analizzare e distribuire una threat intelligence verificata al 100% per le organizzazioni di qualsiasi paese.
Esperienza unica nelle tecnologie di rilevamento del malware	In quanto maggior fornitore di soluzioni antivirus (con prodotti pluripremiati), analizziamo milioni di nuovi campioni di malware ogni giorno, utilizzando le nostre tecnologie proprietarie di rilevamento delle minacce.
Esperienza unica di ricerca APT	Teniamo traccia di centinaia di campagne e attori APT, rilasciamo oltre 200 report strategici TI approfonditi ogni anno e disponiamo della più grande raccolta di file APT del settore, con oltre 70.000 campioni.
TI basata sull'intelligenza artificiale per migliorare la detection and response e i report sulle minacce	AI/ML consentono di estrarre informazioni finalizzati all'azione, generare report personalizzati e automatizzare l'analisi, assicurando un notevole risparmio di tempo e risorse.
Fornitore affidabile e sicuro	Infrastruttura trasparente a tolleranza di errore con elevate capacità di monitoraggio e SLA rigorosi, realizzata utilizzando metodologie SDLC, con regolari valutazioni indipendenti di terze parti (SOC 2 Tipo 2 o ISO 27001).

Case study pubblici di successo

Questo ci consente di avere una grande visibilità sulle minacce che i nostri clienti devono affrontare. Quando si verifica un alert, disporre di informazioni autorevoli a cui fare riferimento, con tutti i dati collaterali disponibili, è fondamentale per formarsi un quadro completo di ciò che sta accadendo e di ciò che possiamo imparare.

Paul Colwell
CyberGuard Technologies

CyberGuard Technologies

Leggete la storia

Kaspersky è spesso il primo a identificare una nuova minaccia quando fa la sua comparsa, anche prima che i produttori di software se ne siano accorti.

Kaspersky ha le competenze per informarci sulle nuove minacce, su cosa si nasconde nell'ombra e che non conosciamo, anziché limitarsi a fornirci una raffica di notizie riciclate che non aggiungono niente di nuovo alla nostra comprensione.

Juan Andres Guerrero Saade
Ricercatore, Chronicle Security

chronicle

Leggete la storia

Kaspersky ha superato le mie aspettative con le sue funzionalità perché ha prestato ascolto alle nostre esigenze. Ha aumentato la nostra fiducia nel prodotto e nelle persone che ci lavorano e ci ha consentito di avere una rete più sicura.

Rashid AlNahlawi
Consulente per la sicurezza IT, Comitato olimpico del Qatar

قطر
QATAR

Leggete la storia

Kaspersky Threat Intelligence vi 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.

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.

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.

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.

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.

Grazie!

Kaspersky Threat Intelligence Portal dove risiedono le conoscenze sulla cybersecurity

Kaspersky Threat Intelligence Portal

Per saperne di più

Richiedete una demo