kaspersky bring on the future

Kaspersky
Threat Intelligence

Kaspersky Threat Data Feeds

Panoramica

Che cosa includono i feed?

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

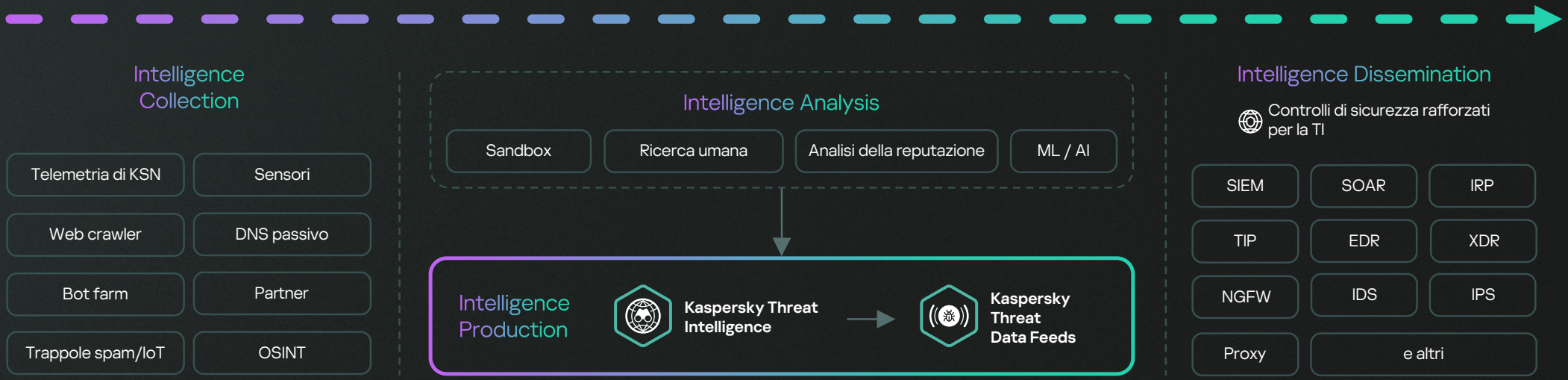
- nome della minaccia
- indirizzi IP e nomi di dominio accertati di risorse Web dannose
- hash di file dannosi
- identificatori di oggetti vulnerabili e compromessi
- tattiche, tecniche e procedure di attacco secondo la classificazione MITRE ATT&CK
- timestamp
- posizione geografica
- popolarità e così via

Il servizio Kaspersky Threat Data Feed fornisce informazioni di threat intelligence in tempo reale per aiutare le organizzazioni a proteggere le reti e i sistemi dalle cyberminacce. I Data Feed includono informazioni su malware noti, siti Web di phishing, vulnerabilità ed exploit più recenti e altri tipi di minacce informatiche. Le organizzazioni possono utilizzare queste informazioni per bloccare il traffico dannoso, aggiornare il proprio software di sicurezza e adottare altre misure per proteggersi dagli attacchi informatici.

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

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.

I Data Feed consentono di raccogliere informazioni generali su un evento e di 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, proteggendo l'azienda dalle minacce di qualsiasi complessità.



Come usare i Data Feed

Nome del feed	Prevenzione	Rilevamento	Investigation
Data Feed Malicious URL	•	•	•
Data Feed Ransomware URL	•	•	•
Data Feed URL di phishing	•	•	•
Data Feed Botnet C&C URL	•	•	•
Data Feed Mobile Botnet C&C URL	•	•	•
Data Feed Malicious Hash	•	•	•
Data Feed Mobile Malicious Hash	•	•	•
Data Feed IP Reputation	•	•	•
Data Feed IoT URL	•	•	•
Data Feed Vulnerability	•	•	•
Data Feed ICS Vulnerability	•	•	•
ICS Vulnerability Data Feed in formato OVAL		•	
Data Feed ICS Hash	•	•	•
Data Feed pDNS			•

Nome del feed	Prevenzione	Rilevamento	Investigation
Data Feed Suricata Rules		•	
Data Feed Cloud Access Security Broker (CASB)		•	
APT Hash Data Feed		•	•
Data Feed APT IP		•	•
Data Feed APT URL		•	•
Data Feed APT Yara		•	•
Data Feed Open Source Software Threats	•	•	•
Crimeware Hash Data Feed		•	•
Data Feed Crimeware URL			•
Data Feed Crimeware Yara			•
Data Feed Sigma Rules	•		
Data Feed Network Security IP	•	•	
Data Feed Network Security URL	•	•	
Data Feed Network Security Web Filtering	•	•	

L'elenco di Kaspersky Threat Data Feeds è in costante espansione.

Descrizione di Kaspersky Threat Data Feeds

Feed commerciali

I feed commerciali consentono di accedere alla raccolta più completa di informazioni disponibile su abbonamento. Le informazioni vengono aggiornate regolarmente. A seconda del tipo di feed, la frequenza degli aggiornamenti può variare da alcuni minuti a diverse ore. Oltre ai data feed elencati, è possibile richiedere di creare un feed personalizzato in base alle proprie esigenze.

Nome del feed	Descrizione del feed	Tipo di indicatore	Scenari di utilizzo
Data Feed Malicious URL	Risorse Web da cui viene distribuito il malware	Mask	• I sistemi di gestione della sicurezza delle informazioni possono essere arricchiti con fonti esterne di informazioni. La connessione di questi flussi a SIEM/SOAR/IRP consente agli utenti di rispondere tempestivamente alle minacce attuali e di creare un ulteriore contesto quando si indaga su un incidente. • L'integrazione con i sistemi di sicurezza di rete ed e-mail (ad esempio, NGFW/IDS/IPS/Protezione della posta/Sicurezza Web) aiuta a prevenire gli incidenti informatici arricchendo le funzionalità native di controllo della sicurezza con gli IOC provenienti dal feed di dati.
Data Feed Ransomware URL	Risorse Web da cui viene distribuito il ransomware		
Data Feed URL di phishing	Risorse Web di phishing		
Data Feed Botnet C&C URL	Server Botnet C&C e oggetti dannosi correlati (bot)		
Data Feed Mobile Botnet C&C URL	Server C&C di botnet mobili con oggetti dannosi associati (bot)		

#Prevenzione

#Rilevamento

#Indagine

Nome del feed	Descrizione del feed	Tipo di indicatore	Scenari di utilizzo	
Data Feed Malicious Hash	Hash di file dannosi comuni	Hash	• Integrazione con i sistemi di sicurezza dell'infrastruttura (Endpoint Security, Sicurezza del server, Protezione della posta/Sicurezza Web) per impedire il download e l'esecuzione di malware e per rilevare quelli già in esecuzione. • L'integrazione con i sistemi SIEM/SOAR/IRP consente agli utenti di rispondere rapidamente alle minacce attuali e di creare un contesto aggiuntivo durante le indagini su un incidente.	#Prevenzione #Rilevamento #Indagine
Data Feed Mobile Malicious Hash	Hash di file dannosi comuni per sistemi operativi mobili (Android e iOS)			
Data Feed IP Reputation	Diverse categorie di indirizzi IP sospetti e dannosi	IP	• L'integrazione con i sistemi di sicurezza della rete e della posta (NGFW/Protezione della posta) aiuta a prevenire gli incidenti informatici integrando il database nativo degli indicatori di compromissione con i dati sulle minacce attuali. • L'integrazione con i sistemi di classe SIEM/SOAR/IRP consente agli utenti di rispondere rapidamente alle minacce attuali e di creare un contesto aggiuntivo durante le indagini su un incidente.	#Prevenzione #Rilevamento #Indagine
Data Feed IoT URL	Risorse Web che distribuiscono software dannoso per dispositivi IoT (telecamere IP, aspirapolvere, teiere, caffettiere intelligenti e così via).	Mask		
Data Feed Vulnerability	Vulnerabilità del software aziendale	CVE	• Identificazione degli elementi infrastrutturali vulnerabili attraverso l'integrazione con gli scanner di vulnerabilità e i sistemi di gestione delle risorse. • Integrazione con i sistemi di protezione degli endpoint per impedire il lancio di software contenenti vulnerabilità critiche. • Rilevamento del lancio di software vulnerabile. • Assistenza con le indagini. • Consigli per le mitigazioni delle vulnerabilità.	#Prevenzione #Rilevamento #Indagine
Data Feed ICS Vulnerability	Vulnerabilità nel software e nell'hardware ICS, nonché nel software aziendale usato nell'infrastruttura di controllo dei processi.			

Nome del feed	Descrizione del feed	Tipo di indicatore	Scenari di utilizzo	
ICS Vulnerability Data Feed in formato OVAL	Regole per le ricerche automatizzate di vulnerabilità del software ICS	Controllo OVAL	• Arricchimento dei più diffusi scanner di vulnerabilità del software per rilevare il software ICS vulnerabile.	#Rilevamento
Data Feed ICS Hash	File dannosi comuni che costituiscono una minaccia per ICS	Hash	• Nel perimetro delle reti OT, analogamente agli scenari di utilizzo del data feed Malicious Hash. • All'interno delle reti OT per rilevare file potenzialmente pericolosi.	#Prevenzione #Rilevamento #Indagine
Data Feed pDNS	Record delle ricerche DNS di domini per gli indirizzi IP corrispondenti in un periodo di tempo.	IP, FQDN	• Fornire il contesto quando si indaga su incidenti informatici	#Indagine
Data Feed Suricata Rules	Regole per il rilevamento di varie categorie di minacce nel traffico di rete, come APT, C&C di botnet, ransomware e così via.	Regola Suricata	• Integrazione con i sistemi NGFW/IDS/IPS/NTA/NDR per arricchire le regole di rilevamento delle attività dannose.	#Rilevamento
Data Feed Cloud Access Security Broker (CASB)	Domini e host correlati ai servizi cloud più diffusi	Mask	• Creazione di una soluzione CASB, in particolare per configurare i criteri di accesso ai servizi cloud.	#Rilevamento

Nome del feed	Descrizione del feed	Tipo di indicatore	Scenari di utilizzo	
APT Hash Data Feed	Hash di file usati dai gruppi APT per sferrare attacchi mirati	Hash	• Integrazione con i sistemi di sicurezza dell'infrastruttura (sicurezza di endpoint e server) per impedire il download e l'esecuzione di malware e per rilevare quelli già in esecuzione. • L'integrazione con i sistemi di sicurezza di rete ed e-mail (ad esempio, NGFW/IDS/IPS/Protezione della posta/Sicurezza Web) aiuta a prevenire gli incidenti informatici arricchendo le funzionalità native di controllo della sicurezza con gli IOC provenienti dal data feed. • L'integrazione con i sistemi di classe SIEM/SOAR/IRP consente agli utenti di creare un contesto aggiuntivo durante l'indagine su un incidente, nonché di rispondere tempestivamente alle minacce attuali relative ad attacchi mirati o a membri di gruppi APT.	#Rilevamento #Indagine
Data Feed APT IP	Informazioni su elementi dell'infrastruttura rilevanti per sferrare attacchi mirati.	IP		
Data Feed APT URL		Mask		
Data Feed APT Yara	Regole YARA per identificare i file usati negli attacchi mirati	Regola YARA	• Ricerca proattiva di segnali di attacchi mirati nell'infrastruttura di un'organizzazione. • Utile quando si indaga su incidenti informatici	#Rilevamento #Indagine
Data Feed Open Source Software Threats	Pacchetti di software open source contenenti vulnerabilità, funzionalità dannose o compromissioni di funzionalità a sfondo politico (blocco in alcune aree geografiche, slogan politici e così via)	Nome e versione del pacchetto	• Progettato per l'analisi dei componenti del software sviluppato nell'ambito del processo di sviluppo sicuro (DevSecOps), al fine di proteggere il software dagli attacchi della catena di fornitura, individuare ed eliminare tempestivamente le vulnerabilità e prevenire l'uso di pacchetti contenenti funzionalità non dichiarate di natura politica (NDV).	#Prevenzione #Rilevamento #Indagine

Nome del feed	Descrizione del feed	Tipo di indicatore	Scenari di utilizzo	
Crimeware Hash Data Feed	Hash dei file usati nelle campagne fraudolente descritte nei report di Kaspersky Crimeware	Hash	• Rilevamento di attività dannose associate alle azioni fraudolente degli intrusi. • Assistenza con la risoluzione degli incidenti fornendo informazioni aggiuntive contenute nei feed di dati sulle minacce.	#Rilevamento #Indagine
Data Feed Crimeware URL	Informazioni sugli elementi dell'infrastruttura relativi alle campagne fraudolente descritte nei report di Kaspersky Crimeware	Mask		
Data Feed Crimeware Yara	Regole YARA per identificare i file usati nelle campagne fraudolente descritte nei report di Kaspersky Crimeware	Regola YARA	• Ricerca proattiva dei segni di campagne fraudolente nell'infrastruttura dell'organizzazione. • Utile quando si indaga su incidenti informatici	#Indagine
Data Feed Sigma Rules	Regole in formato YAML per rilevare attività dannose	Regole SIGMA	• Integrazione con SIEM/EDR per rilevare attività dannose	#Rilevamento
Data Feed Network Security IP	Elenco di indirizzi IP NGFW con avvisi/negati	IP	• Integrazione con i controlli di sicurezza di rete (NGFW) per aumentare il livello di protezione.	#Rilevamento #Prevenzione

Nome del feed	Descrizione del feed	Tipo di indicatore	Scenari di utilizzo	
Data Feed Network Security URL	Elenco di URL per gli indirizzi NGFW con avvisi/negati	URL	• Integrazione con i controlli di sicurezza di rete (NGFW) per aumentare il livello di protezione.	#Rilevamento #Prevenzione
Data Feed Network Security Web Filtering	Elenco di domini classificati per gli indirizzi NGFW con avvisi/negati	URL	• Integrazione con i controlli di sicurezza di rete (NGFW) per aumentare il livello di protezione.	#Rilevamento #Prevenzione

Feed demo

I feed demo sono solo a scopo di valutazione. I dati contengono campioni limitati con informazioni significativamente ridotte e aggiornamenti meno frequenti. La struttura dei feed è simile al formato dei feed commerciali, ma in alcuni casi può differire.

- Data Feed demo IP Reputation
- Data Feed demo Botnet C&C URL
- Data Feed demo Malicious Hash
- Data Feed demo APT IP
- Data Feed demo APT URL
- Data Feed demo Sigma Rules
- Data Feed demo APT Hash
- Data Feed demo Suricata Rules
- Data Feed demo Suricata Rules
- Data Feed demo ICS Vulnerability
- Data Feed demo ICS Vulnerability in formato OVAL
- Data Feed demo Crimeware Hash
- Data Feed demo Crimeware URL

Richiedete una demo

Kaspersky Threat Intelligence

Il vostro contesto di supporto eterogeneo

I Kaspersky Data Feed sulle minacce ottimizzano le funzionalità di rilevamento dei controlli di sicurezza esistenti, inclusi i sistemi SIEM, i sistemi di rilevamento delle intrusioni, i proxy di sicurezza e così via.

Ulteriori informazioni

www.kaspersky.it