

Kaspersky Threat Intelligence

Stay ahead of your adversaries



kaspersky

Kaspersky Threat Intelligence sources

2



Kaspersky Threat Intelligence provides access to a wide range of information gathered by our **world-class analysts and researchers** to help your organization effectively counter today's cyber threats.

Threat Intelligence powered by unique global expertise and knowledge

3



Every center contributes to Kaspersky's solutions and services



Threat Research



Incident Investigation



Kaspersky Global Research and Analysis Team

- Research of the most complex threats: APT, cyber espionage campaigns, global cyber epidemics, etc.
- Security of future-focused technologies
- Investigation of sophisticated financial cybercrime



Kaspersky Threat Research

- Anti-Malware Research
- Content Filtering Research
- SSDLC & Secure-by-Design Methodologies



Kaspersky AI Technology Research

- AI Cybersecurity
- GenAI Research
- AI-Powered Threat Detection / Solutions



Kaspersky Security Services

- MDR
- Incident Response
- Security Assessment
- SOC Consulting
- Digital Footprint Intelligence



Kaspersky ICS CERT

- Critical Infrastructure Threat Analysis
- ICS Vulnerability Research and Assessment
- Technology Associations, Analytics and Standards

Kaspersky Threat Intelligence highlights

4

Our **deep knowledge**, **extensive experience** in cyberthreat research, **and unique insights** into every aspect of cybersecurity have made us a trusted partner for businesses worldwide and a valued ally to law enforcement and government organizations, including Interpol and numerous CERT units.



Coverage of global threats, with longstanding experience researching threats in regions where most attacks originate



Continuous contribution by Kaspersky experts



Threat Intelligence for IT and OT segments



Kaspersky Threat Intelligence highlights

5

We track:

300+



threat actors

500+



campaigns

200+

private reports
a year are produced

170 000+

IoCs related to reports

2 500+

YARA rules related
to reports

Threat Intelligence data levels

6



Tactical

Low-level, highly perishable information that supports security operations and incident response. An example of tactical intelligence is IOCs related to a conduct of a newly discovered attack.

Roles:

SOC Analyst

Systems:

SIEM

NGFW

SOAR

IPS

IDS

Processes:

Threat Hunting

Monitoring



Operational

This level usually includes data on campaigns and higher-order TTPs. It may include information on specific actor attribution as well as capabilities and intent adversaries.

Roles:

SOC L3 Analyst

DFIR Analyst

IR Analyst

Systems:

SIEM

NTA

TIP

EDR / XDR

Processes:

Incident Response

Threat Hunting



Strategic

This level is supporting C-level executives and boards of directors in making serious decisions about risk assessments, resource allocation, and organizational strategy. This information includes trends, actor motivations, and their classifications.

Roles:

CISO

CTO

CIO

CEO

Processes:

Building an IS strategy

Awareness raising

Threat Intelligence delivery formats

7



Machine-readable Threat Intelligence



Kaspersky
Threat Data
Feeds

30+ threat data feeds
focusing on different
needs with IT & OT
coverage and TI Platform



Human-readable Threat Intelligence



Kaspersky
Threat Intelligence
Portal

The core Kaspersky Threat
Intelligence portfolio for IT and
OT environments with a single
access point via Kaspersky
Threat Intelligence Portal



Threat Intelligence expert support



Kaspersky
Takedown
Service



Kaspersky
Ask the Analyst

Expert guidance from seasoned
professionals

Kaspersky Threat Intelligence



Kaspersky Threat Data Feeds

9



30+ out-of-the-box threat data feeds for different tasks.

Threat data feeds tailored to your organization are also available.

- Tactical TI
- Operational TI

General threat data feeds

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

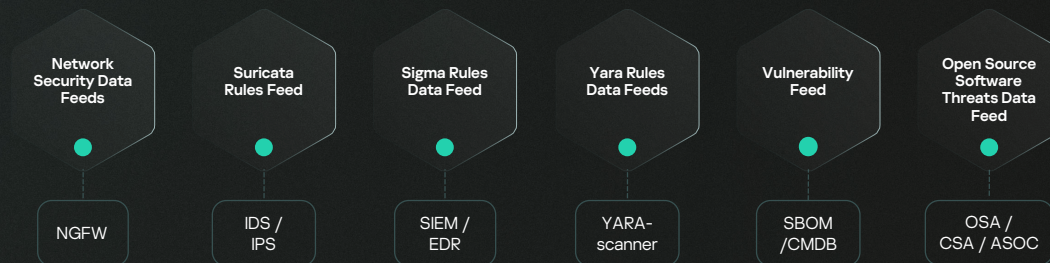


TI Platform

Quickly operationalize your various threat intelligence feeds and reduce SIEMs workload



Specific threat data feeds



Kaspersky Threat Intelligence Portal

10



A single access point to Kaspersky Threat Intelligence within a unified UI / API, where services work together, enriching and reinforcing each other. Bringing together all Kaspersky's cyberthreat expertise and knowledge in one place, it allows monitoring of threats relevant to a specific organization using proprietary data processing and normalization technologies, and enables examination of malware samples and their attribution.

- Tactical TI
- Operational TI
- Strategic TI



Kaspersky
Threat Intelligence
Portal
free version



Threat Landscape on Kaspersky Threat Intelligence Portal

11

Region- and industry-specific threat intelligence to understand the exact threats facing your organization

- MITRE ATT&CK alignment
- Real-time updates based on ongoing Kaspersky researches
- Auto-fill adversary and software profiles
- Repository of detection rules

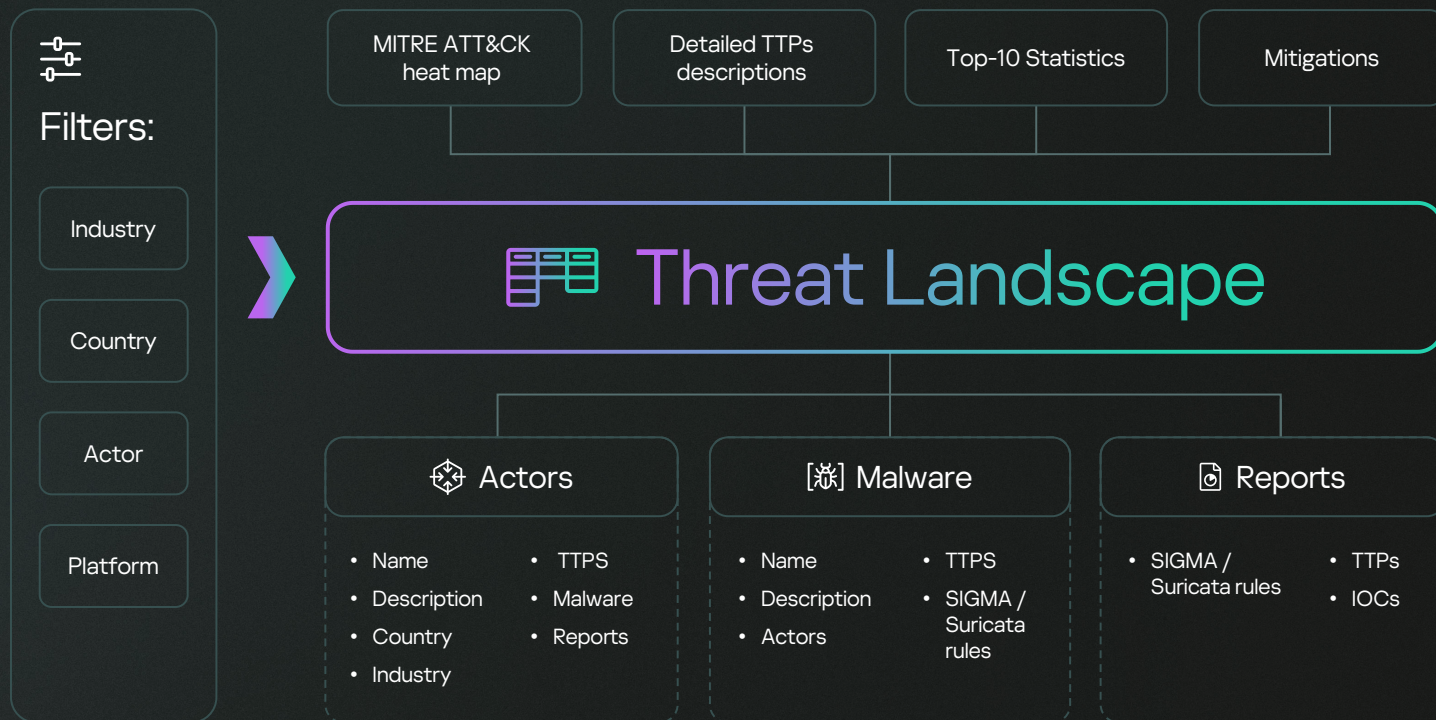


400 000+

Malicious files we detect daily

Threat Landscape — how it works

12



Kaspersky Threat Intelligence expert support

13



Kaspersky Ask the Analyst

- Operational TI
- Strategic TI

The Kaspersky Ask the Analyst service extends our Threat Intelligence portfolio, enabling you to request guidance and insights into specific threats you're facing or are interested in.

We empower you with access to a core group of Kaspersky researchers on a case-by-case basis. The service delivers comprehensive communication between experts to augment your existing capabilities with our unique knowledge and resources.



Kaspersky Takedown Service

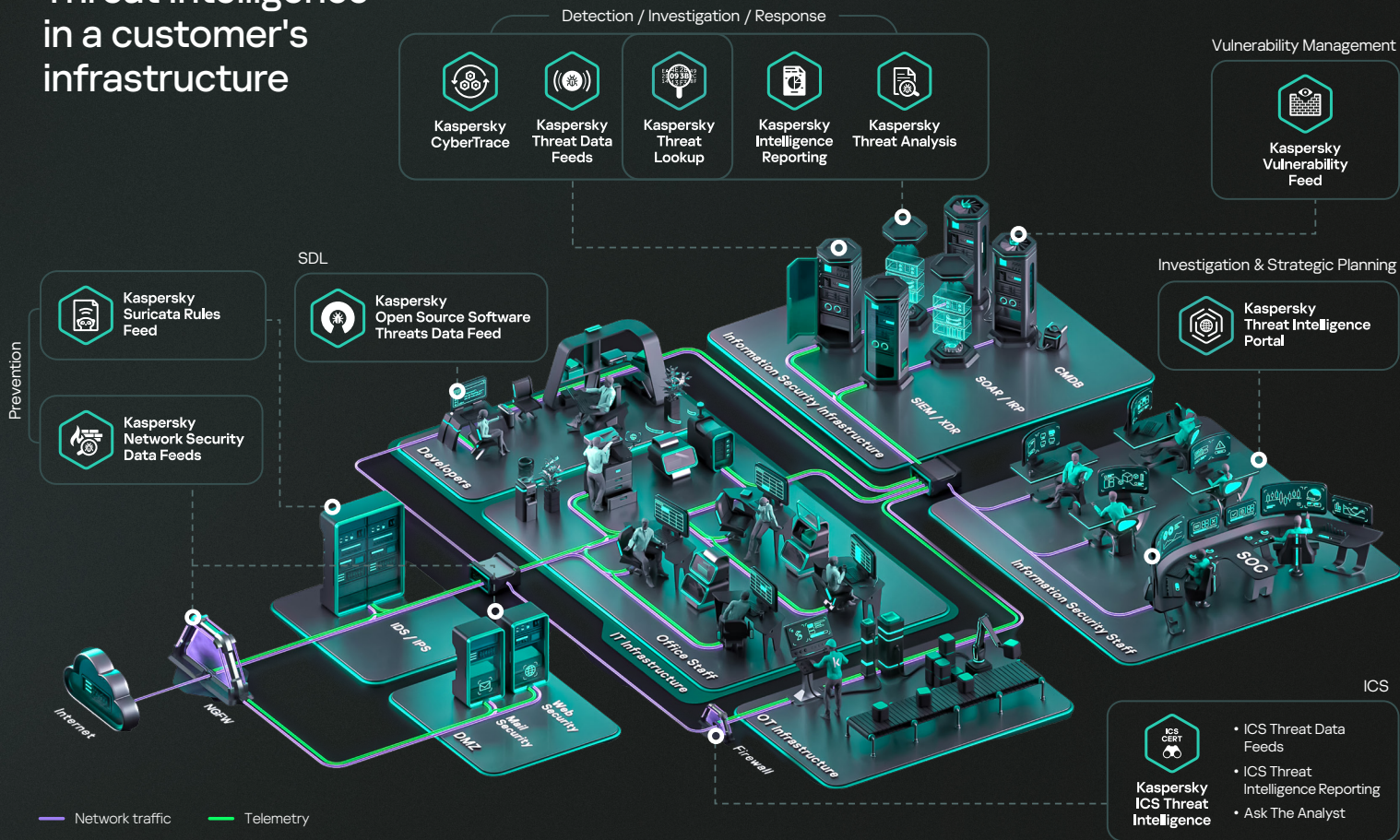
- Operational TI

The Kaspersky Takedown Service quickly mitigates threats posed by malicious phishing domains before they can cause damage to your business and brand. With extensive experience in analyzing domains, we know how to gather all the necessary evidence to prove that they are malicious. We'll take care of your takedown management.

The service is delivered globally in cooperation with international organizations and national and regional law enforcement agencies.

Example of Kaspersky Threat Intelligence in a customer's infrastructure

14



Kaspersky Threat Intelligence Industrial offer

15

Machine-readable Threat Intelligence



Kaspersky Threat Data Feeds

Machine-readable data about industrial cybersecurity threats and vulnerabilities:

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

Human-readable Threat Intelligence



Kaspersky ICS Intelligence Reporting

Access regular publications covering industrial cybersecurity threats and vulnerabilities on the Kaspersky Threat Intelligence Portal

Threat Intelligence expert support



Kaspersky Ask the Analyst

Consult directly with Kaspersky ICS CERT experts for personalized advice on industrial cybersecurity threats and vulnerabilities, threat statistics, the threat landscape, industry standards and more.

● Tactical

● Operational TI

● Strategic TI

Why to choose Kaspersky Threat Intelligence

16

 A leading TI offering recognized by industry analysts

Verified by analysts from various global research companies such as Frost & Sullivan, Quadrant Knowledge Solutions, Forrester, IDC etc.

 Multiple credible and unique sources to produce reliable TI

Our Kaspersky Security Network infrastructure covering 100M+ sensors in 200 countries, the largest repositories of malicious and legitimate files, Dark Web, continuous TH and IR activities, web crawlers, spam traps, etc.

 Renowned people expertise in IT and OT

200+ certified experts from 5 centers of expertise including GReAT team and ICS-CERT distributed worldwide, speaking more than 20 languages. Kaspersky's experts are always among the first to uncover the most notorious threats — from Stuxnet and WannaCry to Operation Triangulation.

 Global presence

A strong presence in the regions where most attacks originate (Russia, CIS, China, etc.) gives us the unique ability to collect, analyze and distribute 100% vetted threat intelligence for organizations in any country.

 Unique experience in malware detection technologies

As the largest AV vendor (with the most award-winning products), we process millions of new malware samples every day, using our proprietary threat detection technologies.

 Unique experience in APT research

We track hundreds of APT actors and campaigns, release 200+ in-depth TI strategic reports annually and own the largest APT file collection in the industry that includes 70K+ samples.

 AI powered TI to enhance detection, response and threat reporting

AI / ML enables us to extract actionable insights, generate custom reports, and automate analysis, saving us / significant time and resources.

 Robust and secure vendor

Fault tolerant, transparent infrastructure with high SLA and monitoring capabilities, built using SDLC methodologies, with regular independent 3-rd party assessments (SOC 2 Type 2 or ISO 27001).

Public success stories

17



This gives us great visibility of the threats that our customers are facing. When an alert does occur, having that authoritative, referenceable information, with all the collateral data that you get with it, is vital in building a complete picture of what's going on and what we can learn from it.

Paul Colwell
CyberGuard Technologies



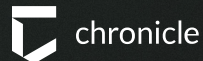
[Read the story](#)



Kaspersky is often the first to identify when a new threat is emerging, even before the software manufacturers know anything about it.

Kaspersky has the expertise to tell me about new threats, what's lurking in the shadows that we're unfamiliar with, rather than simply giving me a barrage of recycled news that doesn't add anything new to our understanding.

Juan Andres Guerrero Saade
Researcher, Chronicle Security



[Read the story](#)



Kaspersky exceeded my expectations with their features and by listening to what we needed. They gave us confidence in the product and the people behind it and enabled us to have a more secure network.

Rashid AlNahlawi
IT Security Consultant,
Qatar Olympic Committee



[Read the story](#)

Kaspersky Threat Intelligence empowers you to...

18



Proactively identify and prevent threats

Kaspersky Threat Intelligence keeps you informed about the latest threats and vulnerabilities, empowering you to take proactive measures to protect your systems before an attack occurs.



Enhance your threat detection capabilities

Kaspersky Threat Intelligence helps you augment your existing security solutions with the latest threat intelligence, improving your ability to detect and block advanced threats.



Improve your incident response

Kaspersky Threat Intelligence delivers real-time information about emerging threats and indicators of compromise, so you can respond quickly and effectively to incidents.



Gain visibility into your digital footprint

Kaspersky Threat Intelligence provides a comprehensive view of your digital footprint, including any assets that may be vulnerable to attack or compromise.



Enrich your in-house expertise

Kaspersky's team of experts are among the most experienced and respected researchers in the industry, bringing a wealth of knowledge and expertise to your Information Security teams.



Comply with regulations and standards

All companies are subject to various regulations and standards within their industry. Kaspersky Threat Intelligence supports compliance by helping you meet these requirements.

Thank you!

The Kaspersky Threat Intelligence Portal –
where cybersecurity knowledge lives



Kaspersky
Threat Intelligence
Portal



[Learn more](#)



[Request a demo](#)

