

kaspersky bring on the future



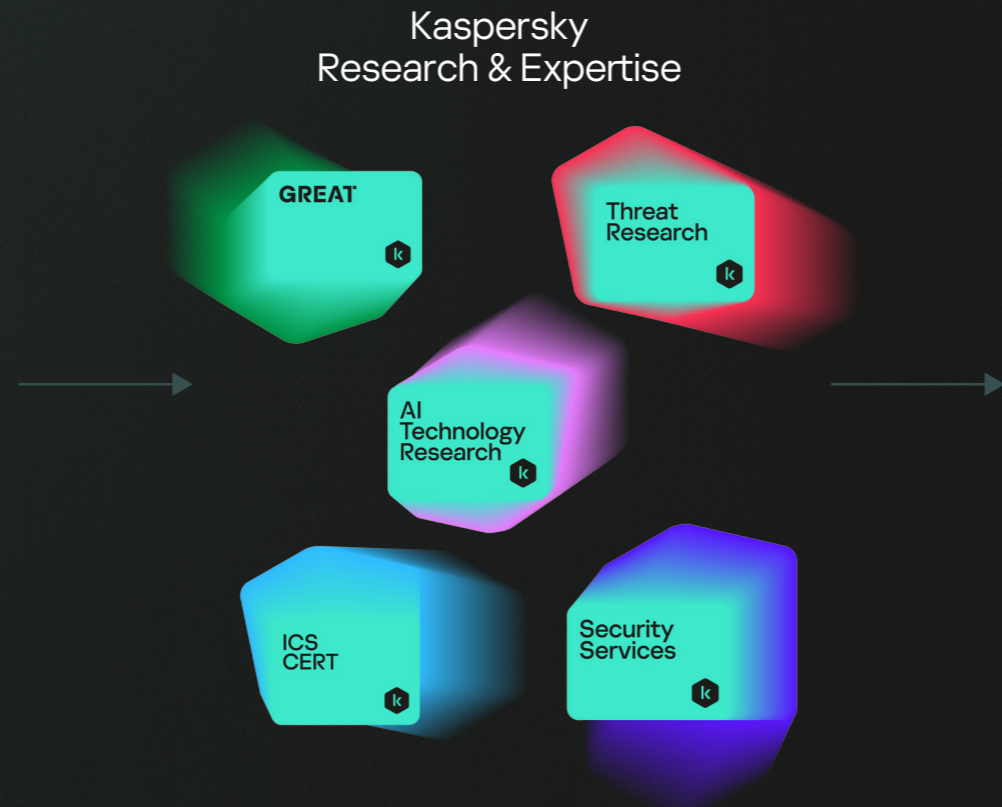
Stay ahead of your adversaries

# Kaspersky Threat Intelligence

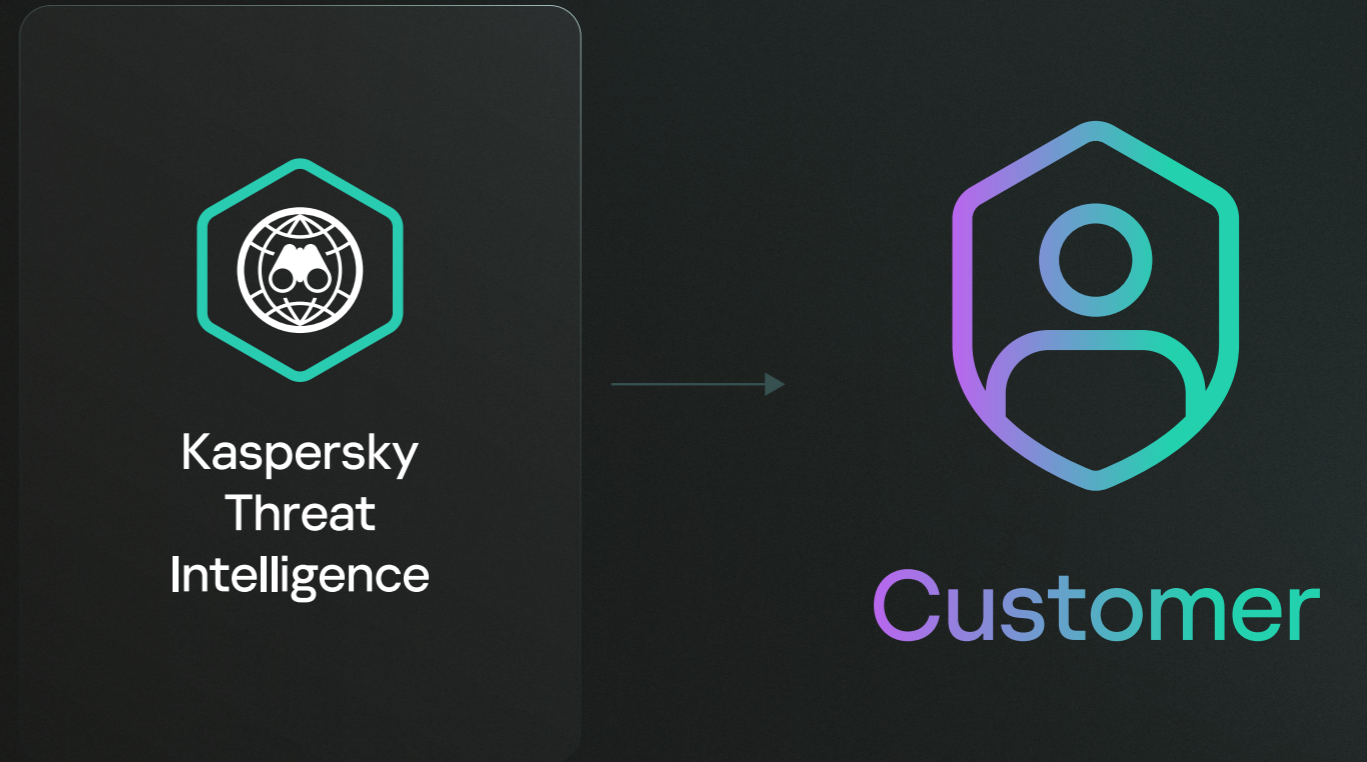


# Kaspersky Threat Intelligence sources

- KSN
- Passive DNS
- Web crawlers
- Files repository
- Bot farms
- Partners
- Spam traps
- OSINT
- Sensors
- And much more ....



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




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

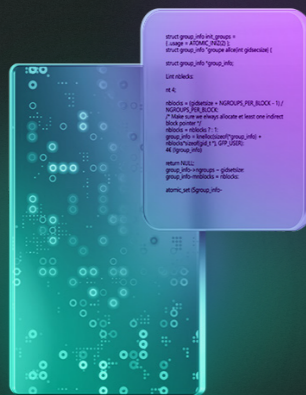
- Critical Infrastructure Threat Analysis
- ICS Vulnerability Research and Assessment
- Technology Associations, Analytics and Standards



# Kaspersky Threat Intelligence highlights



Continuous contribution  
by Kaspersky experts




Threat Intelligence  
for IT and OT segments




Global threats coverage  
and long-term experience  
in researching threats  
in the regions where most  
attacks originate

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



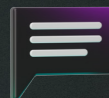
# Kaspersky Threat Intelligence Portfolio



## Machine-readable Threat Intelligence

Kaspersky Threat Data Feeds

Kaspersky CyberTrace



## Threat Intelligence expert support

Kaspersky Takedown Service

Kaspersky Ask the Analyst



- Tactical
- Operational
- Strategic

Available via



## Human-readable Threat Intelligence

Kaspersky Threat Lookup

Kaspersky Digital Footprint Intelligence

Kaspersky Threat Analysis

Sandbox

Attribution

Similarity

Kaspersky Threat Intelligence Reporting

APT

Crimeware

ICS

Kaspersky Threat Infrastructure Tracking



# Kaspersky Threat Intelligence sources

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.



## 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



# Various Threat Intelligence delivery formats



Human-readable  
Threat Intelligence



Kaspersky  
Threat Intelligence  
Portal



Machine-readable Threat Intelligence



Kaspersky  
Threat Data  
Feeds



Threat Intelligence support



Kaspersky  
Takedown Service



Kaspersky  
Ask the Analyst



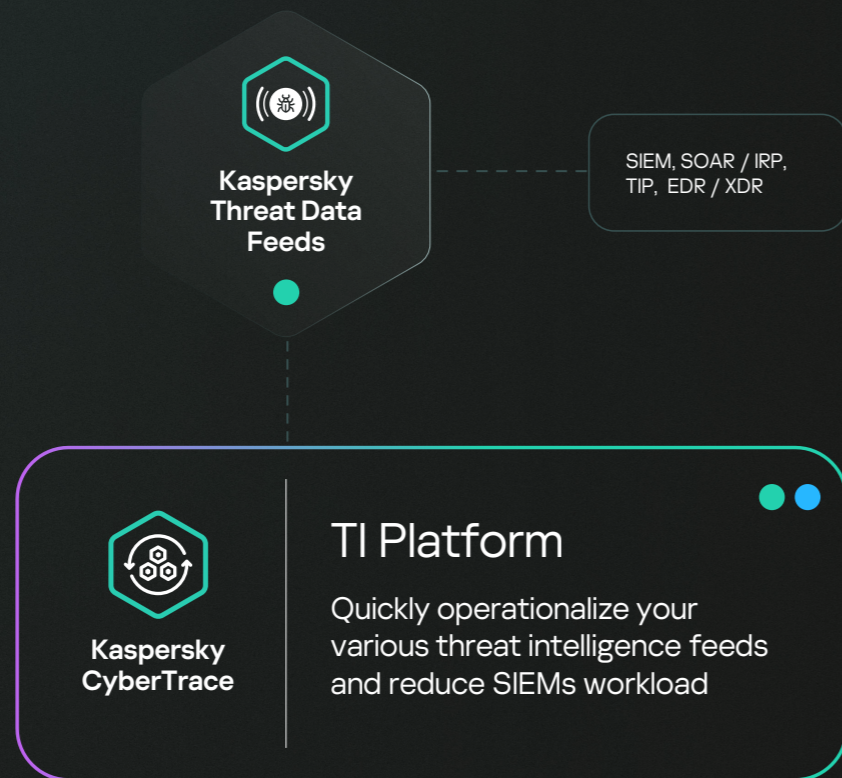
# Kaspersky Threat Data Feeds



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

Threat data feeds tailored to your organization are also available.

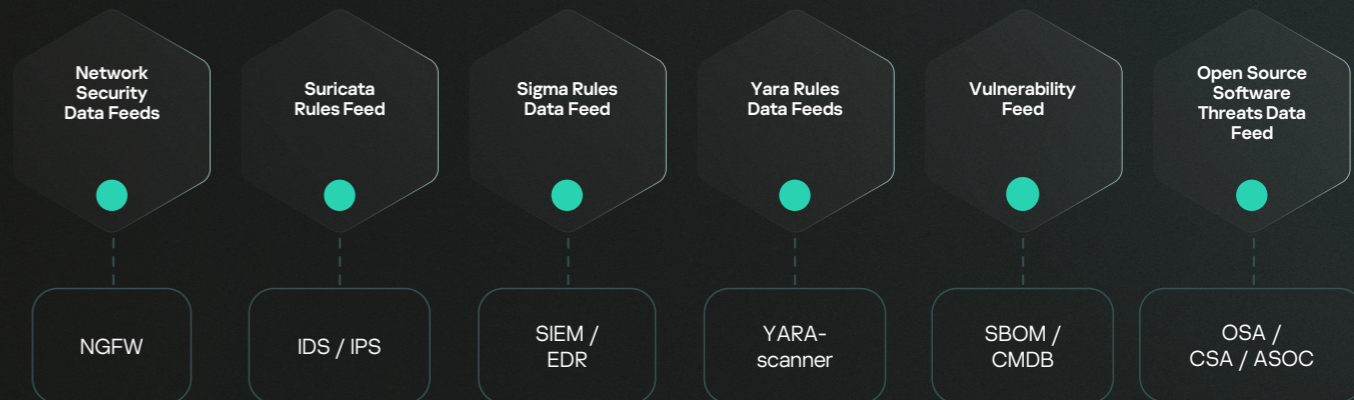
- Tactical TI
- Operational TI



## 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

## Specific threat data feeds







# Kaspersky Threat Intelligence Portal

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 subsequent attribution.



Kaspersky Threat Intelligence Portal free version





# Threat Landscape on Kaspersky Threat Intelligence Portal

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



Filters:

Industry

Country

Actor

Platform

MITRE ATT&CK heat map

Detailed TTPs descriptions

Top-10 Statistics

Mitigations



Threat Landscape



Actors

- Name
- Description
- Country
- Industry
- TTPs
- Malware
- Reports



Malware

- Name
- Description
- Actors
- TTPs
- SIGMA / Suricata rules



Reports

- SIGMA / Suricata rules
- TTPs
- IOCs



# Kaspersky Threat Intelligence support



## Kaspersky Ask the Analyst

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

- Operational TI
- Strategic TI



## Kaspersky Takedown Service

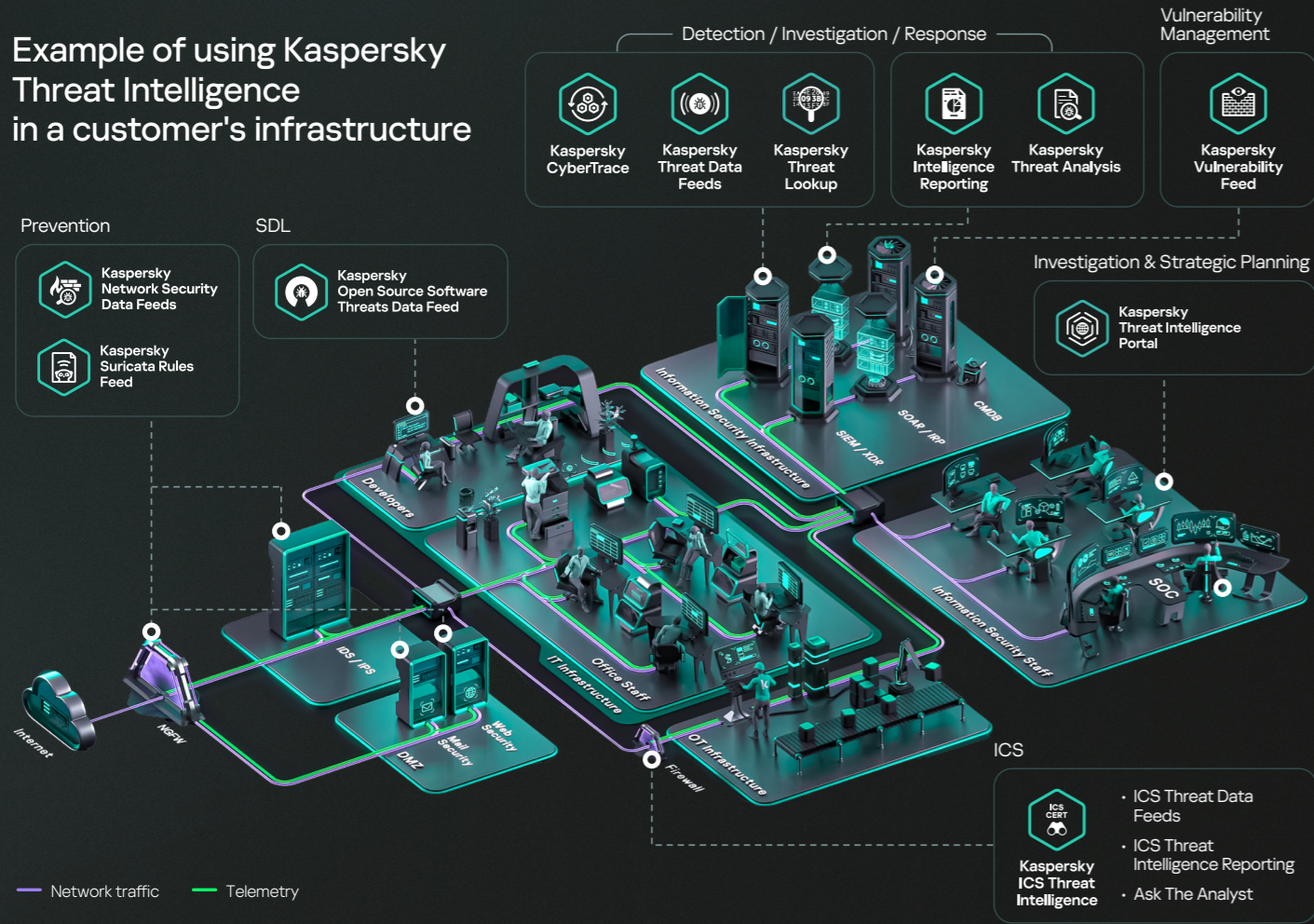
Kaspersky Takedown Service quickly mitigates the threats posed by malicious and phishing domains before any damage can be caused to a customer's brand and business.

With years of 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, enabling rapid action to minimize your digital risk so your team can focus on other priorities. The service is delivered globally in cooperation with international organizations and national and regional law enforcement agencies.

- Operational TI

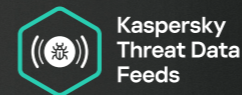


## Example of using Kaspersky Threat Intelligence in a customer's infrastructure



## Kaspersky Industrial Threat Intelligence offer

### 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

Tactical

### Human-readable Threat Intelligence

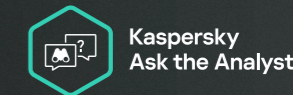


**Kaspersky ICS Intelligence Reporting**

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

Operational TI

### 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.

Strategic TI



# Why to choose Kaspersky Threat Intelligence



## A leading TI offering recognized by industry analysts

Proven to be the most effective threat intelligence provider in the cybersecurity industry and verified by analysts from multiple global research companies.



## 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. Kaspersky also has contributed threat intelligence to MITRE ATT&CK.



## 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), has contributed threat intelligence to MITRE ATT&CK.



## 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.



## 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.

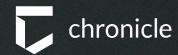


# Public success stories

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

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 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



## 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.



## 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.



## 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.



## 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.



## 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.



## 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.





# Kaspersky Threat Intelligence

Learn more



Request a demo



[www.kaspersky.com](https://www.kaspersky.com)

© 2024 AO Kaspersky Lab.  
Registered trademarks and service marks  
are the property of their respective owners.

#kaspersky  
#bringonthefuture