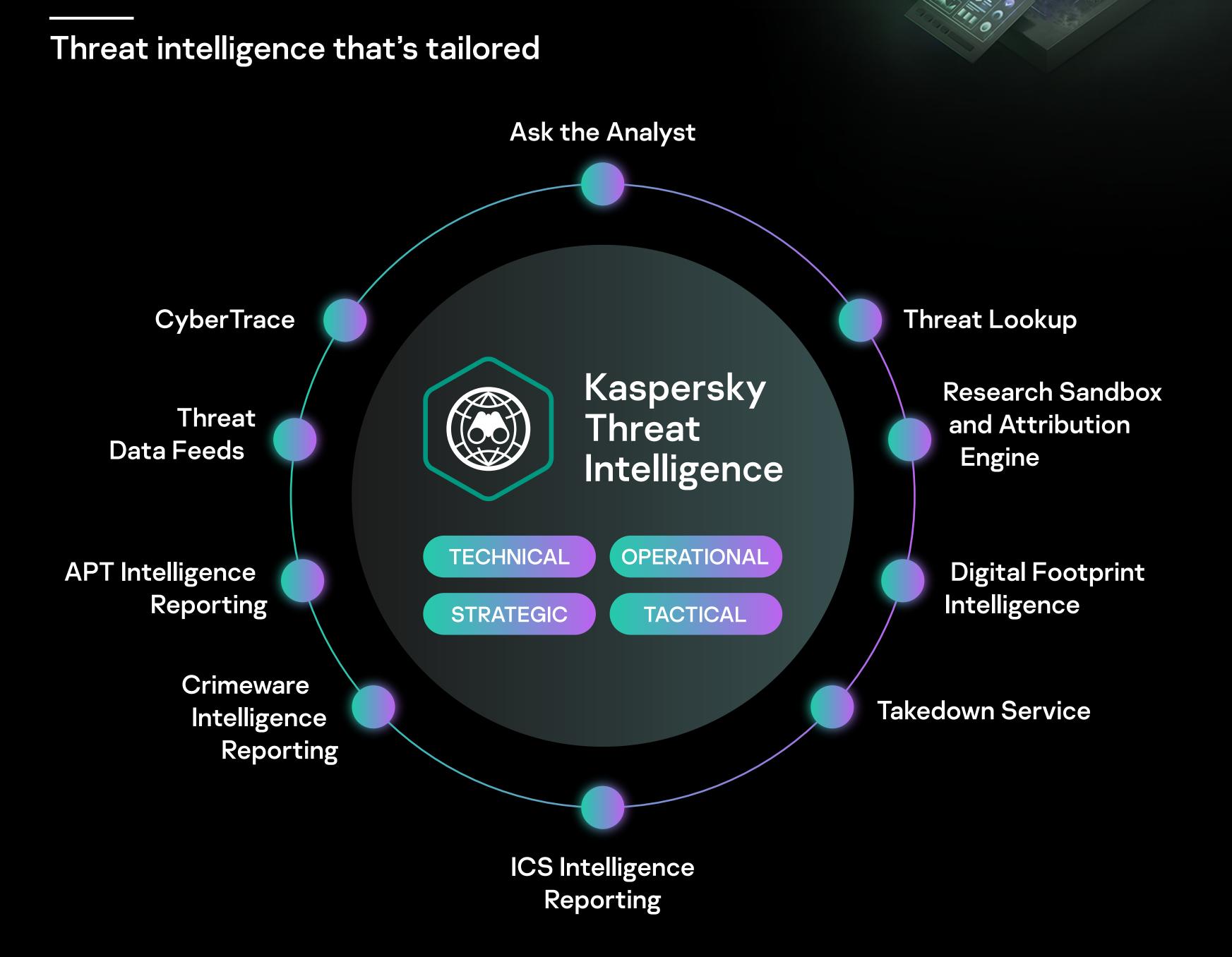
What kind of threat intelligence does your organization need?



TI tailored for fast and accurate response

Kaspersky Threat Lookup Kaspersky Cloud Sandbox **Retrieves the latest detailed TI about** Enables intelligent decision-making based on a file's behavior, while URLs, domains, IP addresses, file simultaneously analyzing process hashes, threat names, statistical/ behavior data, WHOIS/DNS data, memory, network activity, etc. to understand the latest sophisticated file attributes, geolocation data, download chains, timestamps etc. targeted and tailored threats Links the latest detailed TI retrieved by Delivers global visibility of new Kaspersky Threat Lookup with detailed and emerging threats, helping secure investigation of file sample origins, the your organization and boost

collection of IoCs based on behavioral analysis, and detection of malicious objects not previously seen

TI tailored to your existing systems and processes

Kaspersky CyberTrace



Threat Intelligence Portal enabling seamless integration of threat data feeds with SIEM solutions to help your analysts more effectively leverage TI in their existing security operations workflow



Significantly reduces SIEM workload by parsing incoming logs and events, rapidly matching the resulting data to feeds, and generating its own alerts on threat detection



Integrates with any TI feed in JSON, STIX, XML and CSV formats, and supports out-of-the-box integration with numerous SIEM solutions and log sources



Combining Kaspersky CyberTrace and Kaspersky Threat Data Feeds enables your security analysts to effectively distill and prioritize huge amounts of security alerts, improve and accelerate triage and initial response, immediately identify critical alerts, make informed decisions about which to escalate to incident response (IR) teams, and build proactive intelligence-driven defense

TI tailored to your individual threat landscape

Kaspersky Threat Data Feeds

platforms (TIP)

/	\sim

Integrate up-to-the-minute TI feeds containing information on suspicious and dangerous IPs, URLs and file hashes into existing security systems like SIEM, SOAR and threat intelligence



Automate initial alert triage and provide your triage specialists with the context to immediately identify alerts that need to be investigated or escalated to IR teams for further investigation and response



Access records enriched with actionable context (threat names, timestamps, geolocation, resolved IP addresses of infected web resources, hashes, popularity etc.) answering 'who, what, where, when' questions to identify adversaries, make quick decisions and take action

Kaspersky APT Intelligence Reporting



Provides unique access to Kaspersky investigations and discoveries, including full technical data on every APT as it's discovered, as well as on threats that will never be made public

|--|

Reports offer C-level-oriented and easy to understand information, together with detailed technical descriptions of APTs and related IoCs and YARA rules to give security researchers, malware analysts, security engineers, network security analysts and APT researchers actionable data enabling fast and accurate threat response

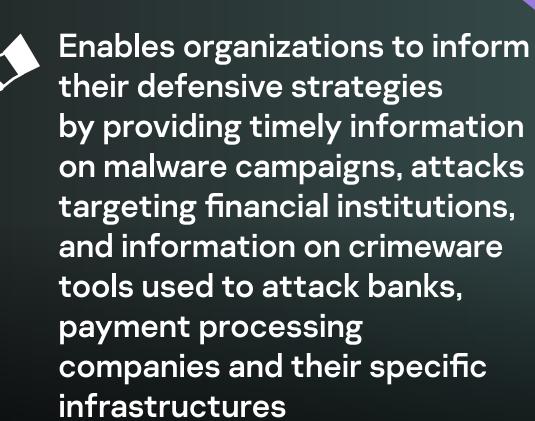
Kaspersky ICS Threat Intelligence Reporting

Kaspersky Crimeware Intelligence Reporting

Provides in-depth intelligence and greater awareness of malicious campaigns targeting industrial organizations, as well as information on vulnerabilities found in the most popular industrial control systems and underlying technologies



Reports include new APT and high-volume attack campaigns targeting industrial organizations, significant changes to the ICS threat landscape, newly discovered vulnerabilities, and actionable recommendations to mitigate these including regional, country and industry-specific information





Delivers detailed descriptions of popular, widespread and highly-publicized/hyped malware; information on dangerous, widespread malware campaigns; and researcher notes/early warnings including information on new and updated malware threats

TI tailored to the needs of your security team

Kaspersky Ask the Analyst



Lets you request guidance and insights on a case-by-case basis from Kaspersky researchers on specific threats you're facing or interested in

Kaspersky Digital Footprint Intelligence



Helps your security analysts explore an adversary's view of your organization's resources, discover potential attack vectors available to them, and adjust your defenses accordingly

Č	\square
с С	ম্প

Builds a comprehensive picture of your attack status, identifying weak spots ripe for exploitation, and revealing evidence of past, present and even planned attacks



Tailors Kaspersky's powerful TI and research

capabilities to your specific needs, enabling

you to build resilient defenses against

threats targeting your organization

Can be combined to form a single solution with the Kaspersky Takedown Service

Kaspersky Takedown Service



Because managing takedowns of malicious and phishing domains used to attack your organization and brands is a complex process requiring expertise and time, the service quickly mitigates threats posed by these domains before any damage can be done

Security scenarios coverage

Security scenarios



Kaspersky Threat Intelligence

Prevention	Detection	Investigation	Response	Strategic reporting
Kaspersky Threat Data Feeds	Kaspersky Threat Data Feeds Kaspersky CyberTrace Kaspersky Ask the Analyst	 Kaspersky Threat Lookup Kaspersky Research Sandbox Kaspersky Threat Attribution Engine Kaspersky CyberTrace Kaspersky CyberTrace TTPs from Kaspersky APT Intelligence Reporting TTPs from Kaspersky Crimeware Intelligence Reporting TTPs from Kaspersky ICS Reporting Kaspersky Ask the Analyst 	Kaspersky Takedown Service	Kaspersky Digital Footprint Intelligence Executive summaries from Kaspersky APT Intelligence Reporting Executive summaries from Kaspersky Financial Threat Intelligence Reporting Kaspersky ICS Tailored Reporting

Why Kaspersky Threat Intelligence

- Extensive range of data sources providing information on currently active threats worldwide, including repository of malicious files detected by Kaspersky over 25+ years
- Instant access to technical, tactical, operational and strategic TI provided by our world-leading team of researchers and analysts
- More than 20 types of threat data feeds; in-house developed Sandbox detecting sophisticated and evasive threats; and Threat Attribution Engine providing detailed information on threat actors required for APT research
- Dedicated team of industrial cybersecurity experts
- Specific skills training for IT security staff
- Top contributor to Microsoft's Active Protection Program for vulnerability research

www.kaspersky.com

© 2023 AO Kaspersky Lab. Registered trademarks and service marks are the property of their respective owners.

