Kaspersky Threat Intelligence

kaspersky

Kaspersky Threat Intelligence

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. Enterprises across all sectors are facing a shortage of the up-to-the-minute, relevant data they need to help them manage the risks associated with IT security threats.

Kaspersky Cybersecurity Services

Kaspersky Threat Intelligence

Threat Data Feeds
CyberTrace
APT Intelligence Reporting
Digital Footprint Intelligence
Threat Lookup
Cloud Sandbox
ICS Threat Intelligence Reporting

Kaspersky Threat Hunting

Kaspersky Security Training

Kaspersky Incident Response

Kaspersky Security Assessment

Threat Intelligence Services from Kaspersky gives you access to the intelligence you need to mitigate these threats, provided by our world-leading team of researchers and analysts.

Kaspersky's knowledge, experience and deep intelligence on every aspect of cybersecurity has made it the trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and leading CERTs. You can leverage this intelligence in your organization today.

Kaspersky Threat Intelligence Services include:

- Threat Data Feeds
- CyberTrace
- APT Intelligence Reporting
- Digital Footprint Intelligence
- Threat Lookup
- Cloud Sandbox
- ICS Threat Intelligence Reporting

Threat Data Feeds

Cyber attacks happen every day. Cyber threats are constantly growing in frequency, complexity and obfuscation, as they try to **compromise your defenses**. Adversaries currently use complicated intrusion **kill chains**, campaigns and customized **Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your clients**. It's now clear that protection requires new methods, based on threat intelligence.

By integrating up-to-the-minute threat intelligence feeds containing information on suspicious and dangerous IPs, URLs and file hashes, into existing security controls, like SIEM systems, security teams can automate the initial alert triage process while providing their triage specialists with enough context to immediately identify alerts that need to be investigated or escalated to Incident Response (IR) teams for further investigation and response.

First-tier security vendors and enterprises use time-honored and authoritative Kaspersky Threat Data Feeds to produce premium security solutions or to **protect their business.**

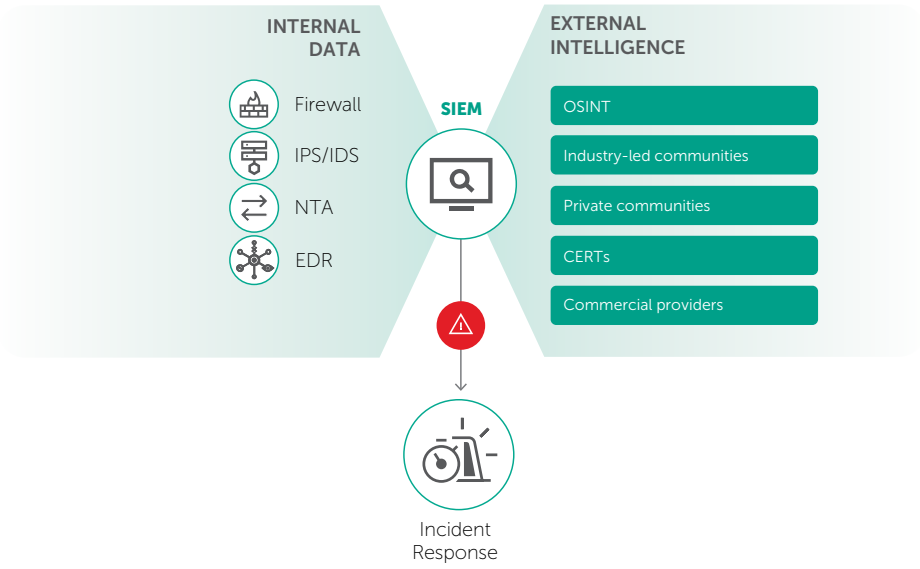


Figure 1. Operationalizing External Threat Intelligence

Contextual Data

Every record in each Data Feed is enriched with **actionable context** (threat names, timestamps, geolocation, resolved IPs addresses of infected web resources, hashes, popularity etc). Contextual data helps reveal the 'bigger picture', further validating and supporting the wide-ranging use of the data. Set in context, the data can more readily be used to answer the **who, what, where, when questions** which lead to identifying your adversaries, helping you make timely decisions and actions **specific to your organization**.

The Data Feeds

Feeds comprise sets of:

- **IP Reputation Feed** – a set of IP addresses with context covering suspicious and malicious hosts;
- **Malicious and Phishing URL Feed** – covering malicious and phishing links and websites;
- **Botnet C&C URL Feed** – covering desktop botnet C&C servers and related malicious objects;
- **Mobile Botnet C&C URL Feed** – covering mobile botnet C&C servers. Identify infected machines that communicates with C&Cs;
- **Ransomware URL Feed** – covering links that host ransomware objects or that are accessed by them.
- **Vulnerability Data Feed** – a set of security vulnerabilities with related threat intelligence (hashes of vulnerable apps/exploits, timestamps, CVEs, patches etc.).
- **APT IoC Feeds** – covering malicious domains, hosts, malicious IP addresses, malicious files used by adversaries to commit APT attacks.
- **Passive DNS (pDNS) Feed** – a set of records that contain the results of DNS resolutions for domains into corresponding IP addresses
- **IoT URL Feed** – covering websites that were used to download malware that infects IoT devices
- **Malicious Hash Feed** – covering the most dangerous, prevalent and emerging malware;
- **ICS Hash Data Feed** – set of file hashes with corresponding context for detecting malicious objects that infect devices used in Industrial Control Systems (ICS);
- **Mobile Malicious Hash Feed** – supporting the detection of malicious objects that infect mobile Android and iPhone platforms;
- **ICS Hash Feed** – set of file hashes with corresponding context for detecting malicious objects that infect devices used in Industrial Control Systems (ICS);
- **P-SMS Trojan Feed** – supporting the detection of SMS Trojans enabling attackers to steal, delete and respond to SMS messages, as well as ringing up premium charges for mobile users;
- **Whitelisting Data Feed** – providing third-party solutions and services with a systematic knowledge of legitimate software.
- **Kaspersky Transforms for Maltego** – providing Maltego users with a set of transforms that give access to Kaspersky Threat Data Feeds. Kaspersky Transforms for Maltego allows you to check URLs, hashes, and IP addresses against the feeds from Kaspersky. The transforms can determine the category of an object as well as provide actionable context about it.

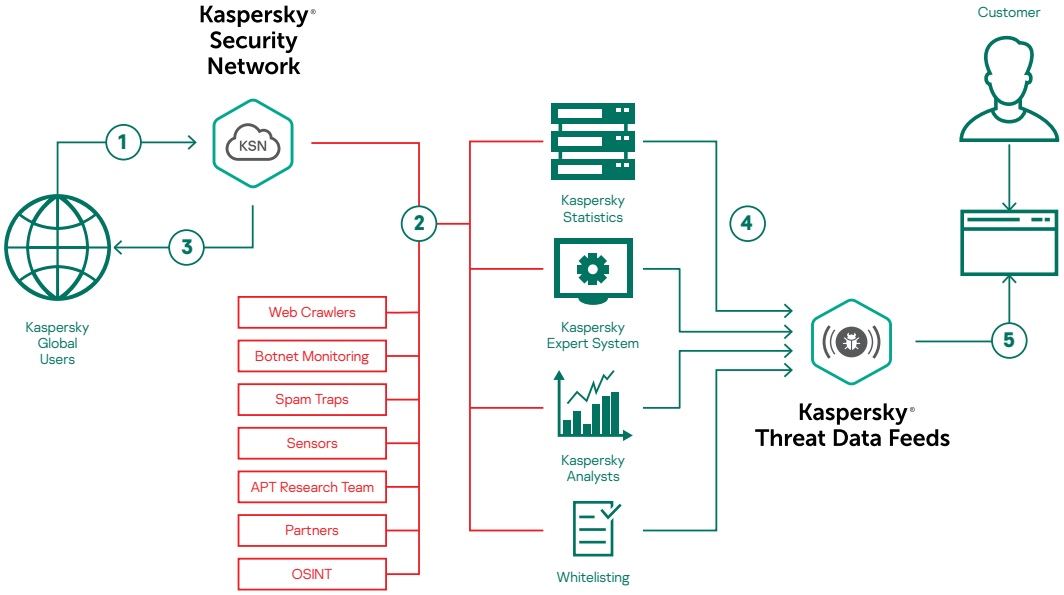


Figure 2. Kaspersky Threat Intelligence Sources

Services Highlights

- Data Feeds littered with **False Positives** are valueless, so very extensive tests and filters are applied before releasing feeds, to ensure that 100% vetted data is delivered;
- Data Feeds are automatically generated in real time, based on findings across the globe (Kaspersky Security Network provides visibility to a significant percentage of all internet traffic, covering tens of millions of end-users in more than 213 countries) providing high **detection rates** and accuracy;
- All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring **continuous availability**;
- The Data Feeds allow **immediate detection of URLs** used to host phishing, malware, exploits, botnet C&C URLs and other malicious content;
- **Malware** in all types of traffic (web, email, P2P, IM,...) and targeted at mobile platforms can also be **instantly detected** and identified;
- Simple lightweight **dissemination** formats (**JSON, CSV, OpenIoC, STIX**) via **HTTPS** or ad-hoc delivery mechanisms support easy integration of feeds into security solutions;
- Hundreds of experts, including **security analysts** from across the globe, world-famous **security experts from GReAT team** and leading-edge R&D teams, contribute to generating these feeds. Security officers receive critical information and alerts generated from the highest quality data, with no risk of being deluged by superfluous indicators and warnings;
- **Ease of implementation**. Supplementary documentation, samples, a dedicated technical account manager and technical support from Kaspersky all combine to enable straightforward integration.

Collection and processing

Data Feeds are aggregated from fused, heterogeneous and highly reliable sources, such as Kaspersky Security Network and our own web crawlers, Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams and partners.

Then, in real-time, all the aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, sandboxes, heuristics engines, multi-scanners, similarity tools, behavior profiling, analysts validation and whitelisting verification:

Benefits

- **Reinforce your network defense solutions**, including SIEMs, Firewalls, IPS/IDS, Security Proxy, DNS solutions, Anti-APT, with continuously updated Indicators of Compromise (IOCs) and actionable context, delivering insight into cyber-attacks and a greater understanding of the intent, capabilities and targets of your adversaries. Leading SIEMs (including HP ArcSight, IBM QRadar, Splunk etc.) are fully supported;
- Develop or enhance **anti-malware protection for perimeter and edge network devices** (such as routers, gateways, UTM appliances).
- **Improve and accelerate your incident response and forensic capabilities** by providing security/SOC teams with meaningful information about threats and global insights into what lies behind targeted attacks. Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats to minimize incident response time and disrupt the kill chain before critical systems and data are compromised;
- **Provide threat intelligence to enterprise subscribers**. Leverage the first-hand information about emerging malware and other malicious threats to **preemptively strengthen your defensive posture and prevent compromises**;
- **Help to mitigate targeted attacks**. Enhance your security posture with tactical and strategic threat intelligence by adapting defensive strategies to counter the specific threats your organization faces;
- Use threat intelligence to **detect malicious content hosted on your networks and data centers**;
- **Prevent the exfiltration of sensitive assets and intellectual property** from infected machines to outside the organization, detecting infected assets fast, preventing competitive advantage and business opportunities loss and protecting the reputation of your brand;
- Conduct deep searches into threat indicators such as command-and-control protocols, IP addresses, malicious URLs or file hashes, with human-validated threat context that allows the prioritization of attacks, improves IT expenditure and resource allocation decisions and **supports you in focusing on mitigating those threats that pose the most risk to your business**;
- Use our expertise and actionable contextual intelligence to **enhance the protection delivered by your products and services** such as web content filtering, spam/phishing blocking and etc;
- **As an MSSP**, grow your business through providing industry-leading threat intelligence as a premium service to your customers. **As a CERT**, enhance and extend your cyber threat detection and identification capabilities.

Kaspersky CyberTrace

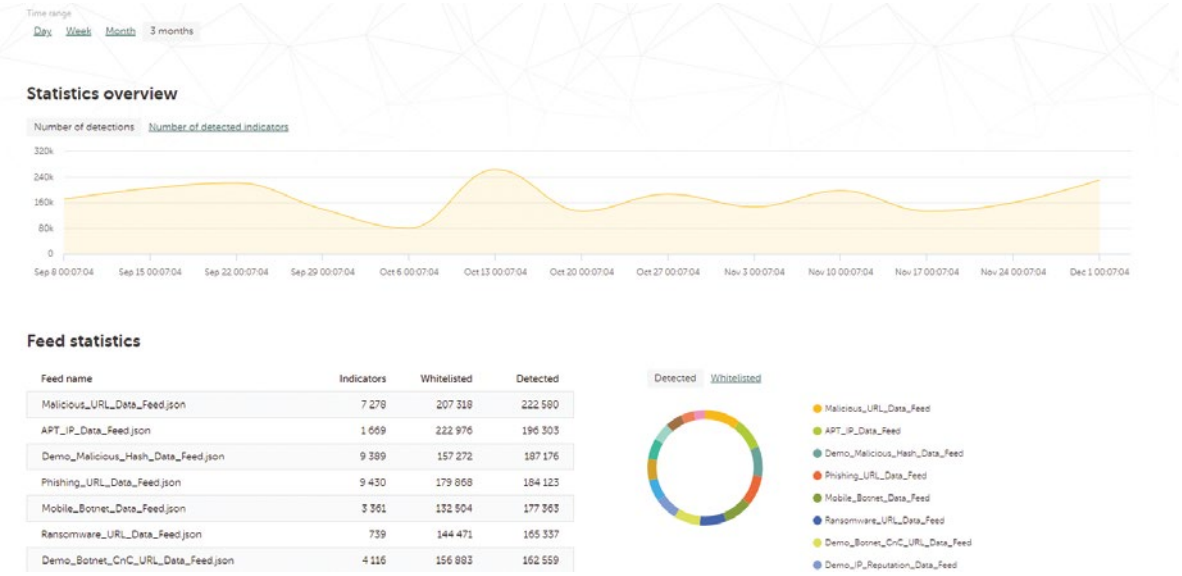
The number of security alerts processed by Security Operations Center's Tier 1 analysts every day is growing exponentially. With this amount of data being analyzed, effective alert prioritization, triage and validation becomes nearly impossible. There are too many blinking lights coming from numerous security products, leading to significant alerts getting buried in the noise, and analyst burnout. SIEMs, log management and security analytics tools aggregating security data and correlating related alarms all help to reduce the number of alerts warranting additional examination, but Tier 1 specialists remain extremely overloaded.

Enabling effective alert triage and analysis

By integrating up-to-the-minute machine-readable threat intelligence into existing security controls, like SIEM systems, Security Operation Centers can automate the initial triage process while providing their Tier 1 specialists with enough context to immediately identify alerts that need to be investigated or escalated to Incident Response (IR) teams for further investigation and response. However, the continuing growth in the number of threat data feeds and available threat intelligence sources makes it difficult for organizations to determine what information is relevant for them. Threat intelligence is provided in different formats and includes a huge number of Indicators of Compromise (IoCs), making it hard for SIEMs or network security controls to digest them.

The Kaspersky CyberTrace is a threat intelligence fusion and analysis tool enabling seamless integration of threat data feeds with SIEM solutions to help analysts leverage threat intelligence in their existing security operations workflow more effectively. It integrates with any threat intelligence feed (in JSON, STIX, XML and CSV formats) you might want to use (threat intelligence feeds from Kaspersky, other vendors, OSINT or your custom feeds), supporting out-of-the-box integration with numerous SIEM solutions and log sources. By automatically matching the logs against threat intelligence feeds, the Kaspersky CyberTrace provides real-time 'situational awareness', allowing Tier 1 analysts to make timely and better informed decisions.

Figure 3. Kaspersky CyberTrace statistics



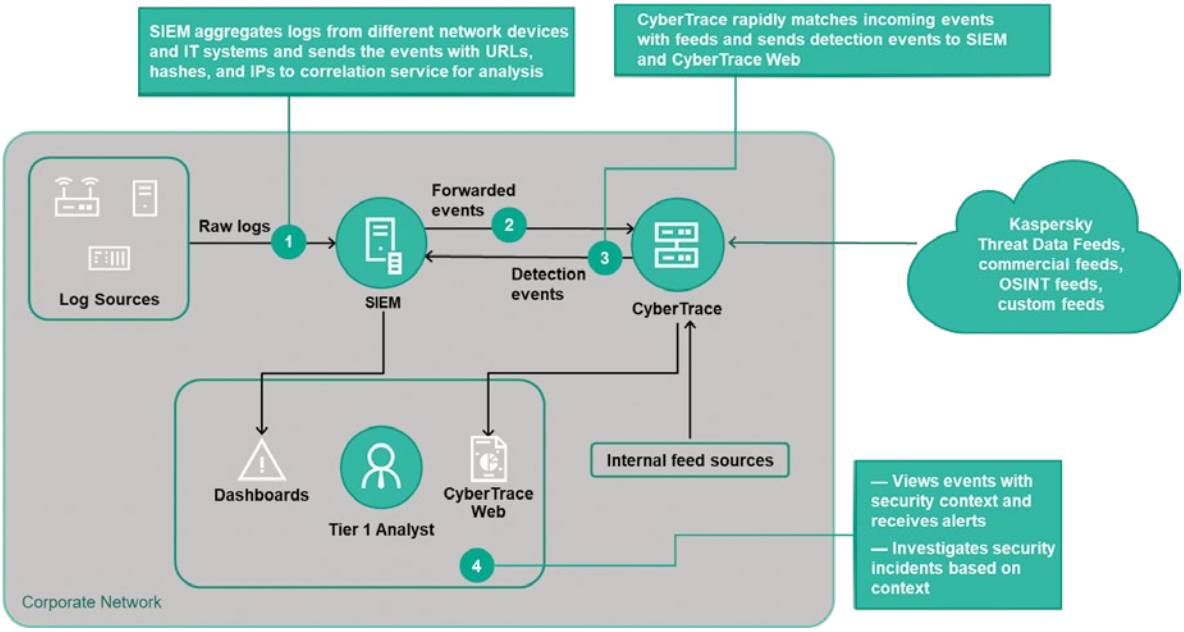
Kaspersky CyberTrace provides a set of instruments to operationalize threat intelligence for conducting effective alert triage and initial response:

- Demo threat data feeds from Kaspersky and OSINT feeds are available out-of-the-box
- SIEM connectors for a wide range of SIEM solutions to visualize and manage data about threat detections
- Feed usage statistics for measuring the effectiveness of the integrated feeds
- On-demand lookup of indicators (hashes, IP addresses, domains, URLs) for in-depth threat investigation
- A web user interface providing data visualization, access to configuration, feed management, log parsing rules, blacklists and whitelists
- Advanced filtering for feeds (based on the context provided with each of the indicators, including threat type, geolocation, popularity, time stamps and more) and log events (based on custom conditions)
- Export of lookup results matching data feeds to CSV format for integration with other systems (firewalls, network and host IDS, custom tools)
- Bulk scanning of logs and files
- Command-line interface for Windows and Linux platforms

- Stand-alone mode, where Kaspersky CyberTrace is not integrated with a SIEM but receives and parses the logs from various sources such as networking devices
- Installation in DMZ-supporting scenarios where it needs to be isolated from the Internet.

The tool uses an internalized process of parsing and matching incoming data, which significantly reduces SIEM workload. Kaspersky CyberTrace parses incoming logs and events, rapidly matches the resulting data to feeds, and generates its own alerts on threat detection. A high-level architecture of the solution integration is shown in the Figure below:

Figure 4. Kaspersky CyberTrace integration scheme



Although Kaspersky CyberTrace and Kaspersky Threat Data Feeds can be used separately, when used together they significantly strengthen your threat detection capabilities, empowering your security operations with global visibility into cyberthreats. With Kaspersky CyberTrace and Kaspersky Threat Data Feeds, Security Operations Center's analysts are able to:

- Effectively distill and prioritize sweeping amounts of security alerts
- Improve and accelerate triage and initial response processes
- Immediately identify alerts critical for the enterprise and make more informed decisions about which should be escalated to IR teams
- Form a proactive and intelligence-driven defense.

Kaspersky APT Intelligence Reporting provides:

- **Exclusive access** to technical descriptions of cutting edge threats during the ongoing investigation, before public release.
- **Insight into non-public APTs.** Not all high profile threats are subject to public notification. Some, due to the victims who are impacted, the sensitivity of the data, the nature of the vulnerability-fixing process or associated law enforcement activity, are never made public. But all are reported to our customers.
- **Detailed supporting technical data access.** Includes an extended list of Indicators of Compromise (IOCs), available in standard formats including openIOC or STIX, and access to our Yara rules.
- **Threat actor profiles** with summarized information on the specific threat actor, including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with their mapping to the MITRE ATT&CK framework.
- **MITRE ATT&CK.** All TTPs described in the reports are mapped to the MITRE ATT&CK framework, enabling improved detection and response through developing and prioritizing the corresponding security monitoring use cases, performing gap analyses and testing current defenses against relevant TTPs.
- **Continuous APT campaign monitoring.** Access to actionable intelligence during the investigation (information on APT distribution, IOCs, C&C infrastructure).
- **Retrospective analysis**. Access to all previously issued private reports is provided throughout the period of your subscription.
- **RESTful API** for seamless integration and automation of your security workflows.

APT Intelligence Reporting

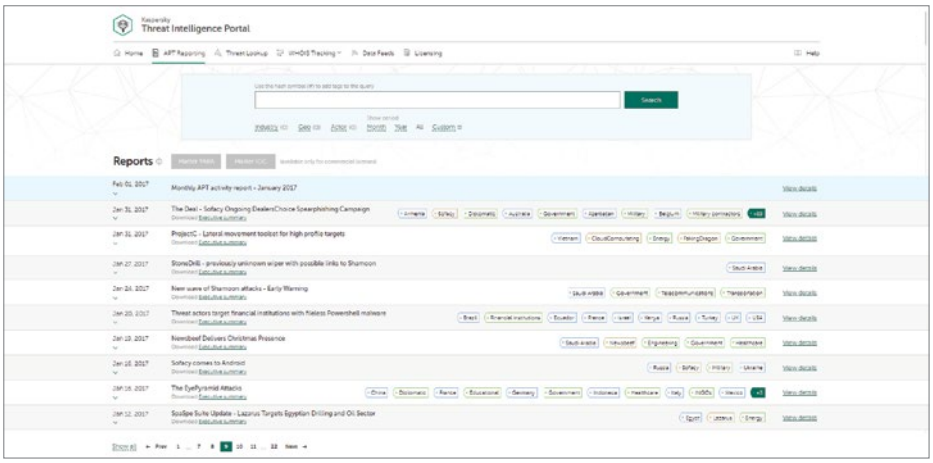
Increase your awareness and knowledge of high profile cyber-espionage campaigns with comprehensive, practical reporting from Kaspersky.

Leveraging the information provided in these reports, you can respond quickly to new threats and vulnerabilities – blocking attacks via known vectors, reducing the damage caused by advanced attacks and enhancing your security strategy, or that of your customers.

Kaspersky has discovered some of the most relevant APT attacks ever. However, not all Advanced Persistent Threat discoveries are reported immediately, and many are never publicly announced.

As a subscriber to Kaspersky APT Intelligence Reporting, we provide you with unique ongoing access to our investigations and discoveries, including full technical data, provided in a range of formats, on each APT as it's revealed, including all those threats that will never be made public. Each report contains an executive summary offering C-level oriented and easy to understand information describing the related APT. The executive summary is followed by a detailed technical description of the APT with the related IOCs and Yara rules, giving security researchers, malware analysts, security engineers, network security analysts and APT researchers actionable data to enable a fast, accurate response to the related threat.

Our experts, the most skilled and successful APT hunters in the industry, will also alert you immediately to any changes they detect in the tactics of cybercriminal groups. And you will have access to Kaspersky's complete APT reports database – a further powerful research and analysis component of your corporate security armory.



Note – Subscriber Limitation

Due to the sensitive and specific nature of some of the information contained in the reports provided by this service, we are obliged to limit subscriptions to trusted government, public and private organizations only.

Digital Footprint Intelligence

As your business grows, the complexity and distribution of your IT environments grow too, presenting a challenging task: protecting your widely distributed digital presence without direct control or ownership. Dynamic and interconnected environments enable companies to derive significant benefits through optimizing processes, increasing product quality, improving customer experience and staying competitive. However, ever-increasing interconnectivity is also expanding the attack surface. As attackers become more skilled, it's vital not only to have an accurate picture of your organization's online presence, but also to track its changes and react to up-to-date information about exposed digital assets.

Organizations may use a wide range of security tools in their security operations but there are still digital threats that loom: capabilities to detect and mitigate insider activities, plans and attack schemes of cybercriminals located on the dark web forums, etc. To help security analysts explore the adversary's view of their company resources, promptly discover the potential attack vectors available to them and adjust defenses accordingly, Kaspersky has created Kaspersky Digital Footprint Intelligence.

What's the best way to mount an attack against your organization? What is the cost-efficient way to attack your organization? What information is available to an attacker targeting you? Has your infrastructure already been compromised?

Kaspersky Digital Footprint Intelligence answers these questions and more, as our experts piece together a comprehensive picture of your current attack status, identifying weak spots ripe for exploitation and revealing evidence of past, present and planned attacks.

Developed using OSINT techniques combined with automated and manual analysis of the surface, deep and dark webs, plus the internal Kaspersky knowledge base, these tailored reports provide actionable insights and recommendations, enabling you to minimize the number of potential attack vectors and reduce your digital risk. These include:

- Network perimeter inventory using non-intrusive methods to identify the customer's network resources and exposed services which are a potential entry point for an attack, such as management interfaces unintentionally left on the perimeter or misconfigured services, devices' interfaces, etc.
- Tailored analysis of their exiting vulnerabilities, with further scoring and comprehensive risk evaluation based on the CVSS base score, availability of public exploits, penetration testing experience and location of the network resource (hosting/infrastructure).
- Identification, monitoring and analysis of any active targeted attacks or attacks that are being currently planned, APT campaigns aimed at your company, industry and region of operations.
- Identification of threats targeting your customers, partners and subscribers, whose infected systems could then be used to attack you.
- Discreet monitoring of pastebin sites, public forums, social networks, instant messaging channels, restricted underground online forums and communities to discover compromised accounts, information leakages or attacks against your organization being planned and discussed there.

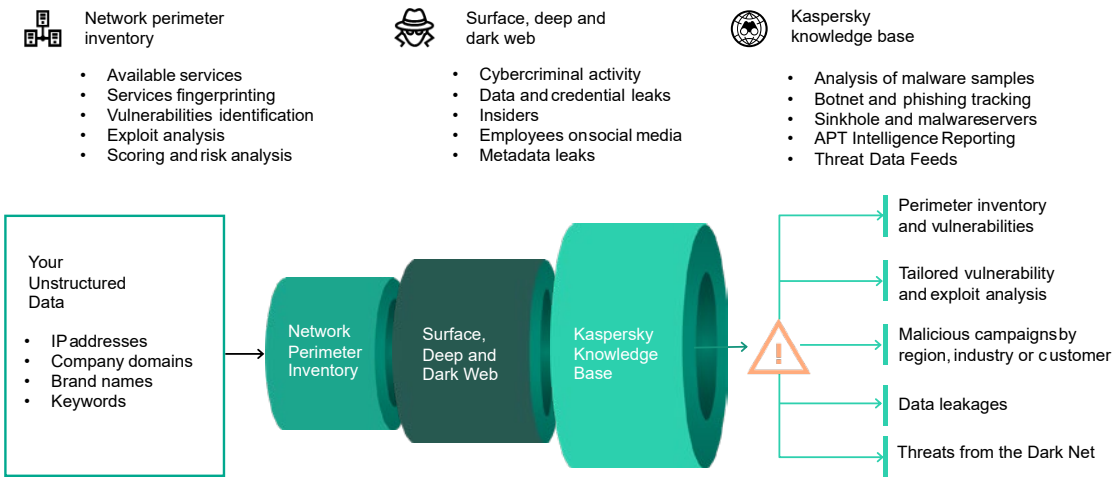
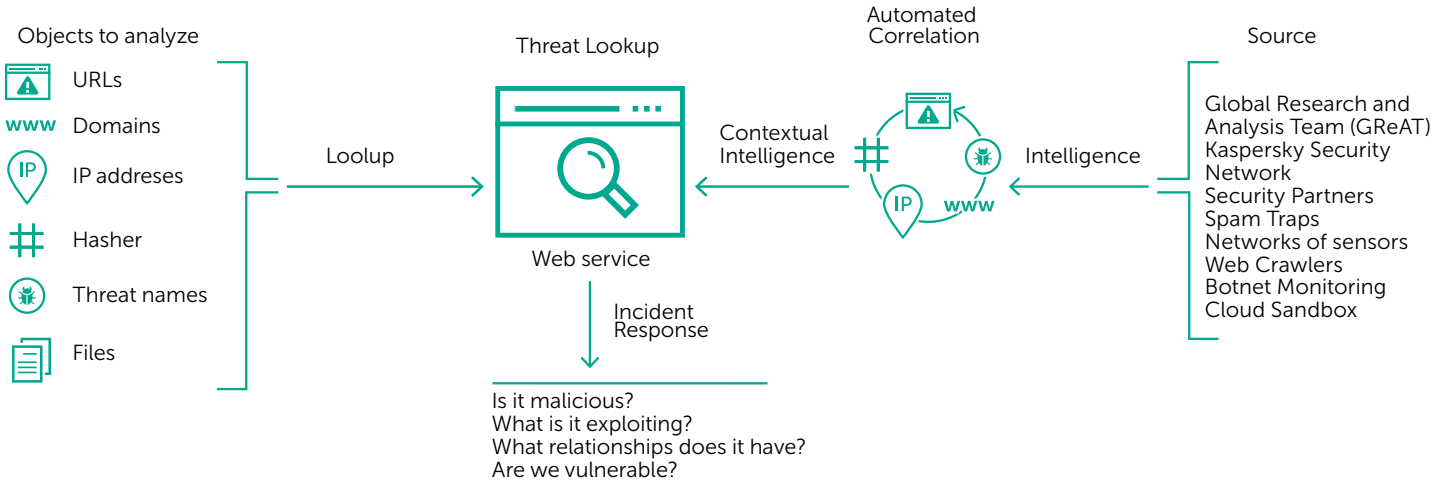


Figure 1. Kaspersky Digital Footprint Intelligence

Quick start – easy to use – no resources needed

Kaspersky Digital Footprint Intelligence has no impact on the integrity and availability of your network resources and services. The reports are available on the Kaspersky Threat Intelligence Portal, a single point of access for all threat intelligence we've gathered over more than 20 years, and supported by immediate notifications as soon as any new information is available. The provided API enables Kaspersky Digital Footprint Intelligence integration with third-party task management systems, which significantly cuts time required for workflow administration.

Threat Lookup



Service highlights

- **Trusted Intelligence:** A key attribute of Kaspersky Threat Lookup is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky products lead the field in anti-malware tests[1], demonstrating the unequalled quality of our security intelligence by delivering the highest detection rates, with near-zero false positives.
- **Threat Hunting:** Be proactive in preventing, detecting and responding to attacks, to minimize their impact and frequency. Track and aggressively eliminate attacks as early as possible. The earlier you can discover a threat – the less damage is caused, the faster repairs take place and the sooner network operations can get back to normal.
- **Sandbox Analysis:** Detect unknown threats by running suspicious objects in a secure environment, and review the full scope of threat behavior and artifacts through easy-to-read reports.
- **Wide Range of Export Formats:** Export IOCs (Indicators of Compromise) or actionable context into widely used and more organized machine-readable sharing formats, such as STIX, OpenIOC, JSON, Yara, Snort or even CSV, to enjoy the full benefits of threat intelligence, automate operations workflow, or integrate into security controls such as SIEMs.
- **Easy-to-use Web Interface or RESTful API:** Use the service in manual mode through a web interface (via a web browser) or access via a simple RESTful API as you prefer.

Cybercrime today knows no borders, and technical capabilities are improving fast: we're seeing attacks becoming increasingly sophisticated as cybercriminals use dark web resources to threaten their targets. Cyber-threats are constantly growing in frequency, complexity and obfuscation, as new attempts are made to compromise your defenses. Attackers are using complicated kill chains, and customized Tactics, Techniques and Procedures (TTPs) in their campaigns to disrupt your business, steal your assets or damage your clients.

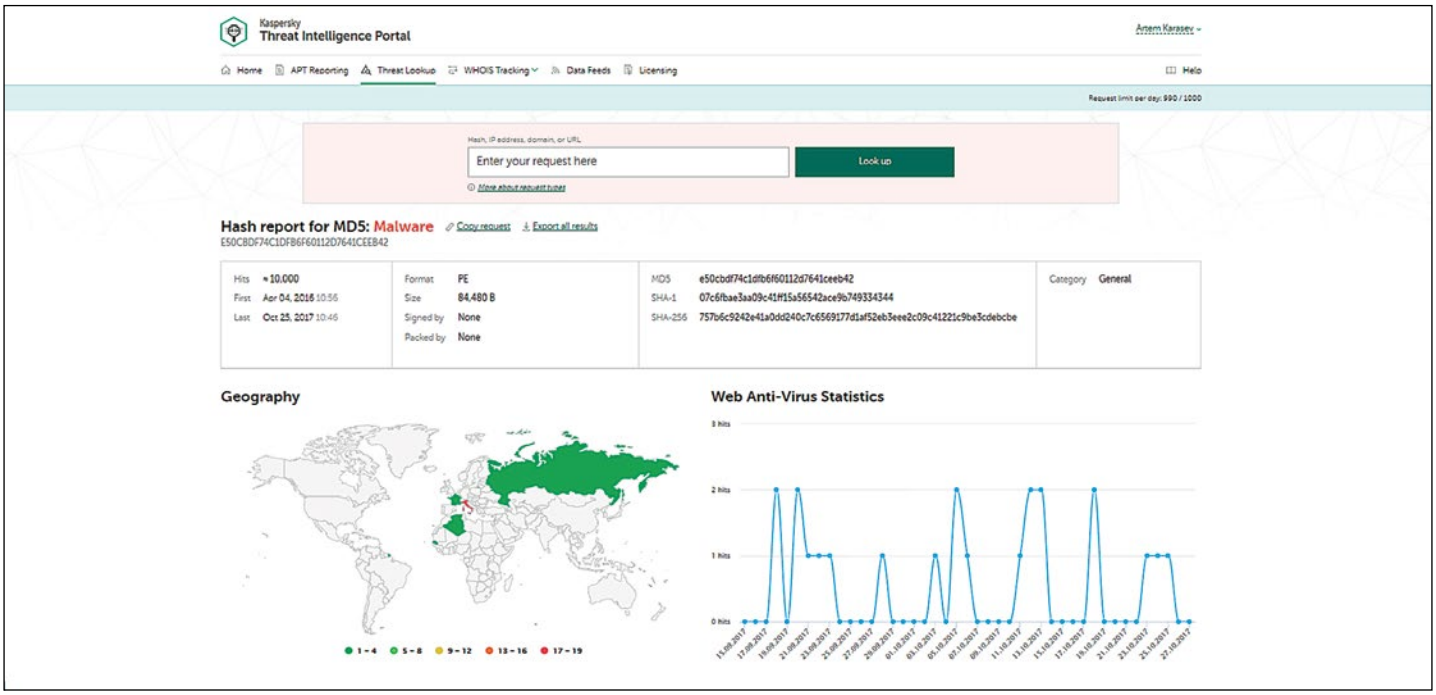
Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky about cyber-threats and their relationships, brought together into a single, powerful web service. The goal is to provide your security teams with as much data as possible, preventing cyber-attacks before they impact your organization. The platform retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, file attributes, geolocation data, download chains, timestamps etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.

Threat intelligence delivered by KasperskyThreat Lookup is generated and monitored in real time by a highly fault-tolerant infrastructure ensuring continuous availability and consistent performance. Hundreds of experts, including security analysts from across the globe, world-famous security experts from our GReAT team and leading-edge R&D teams, all contribute to generating valuable real-world threat intelligence.

Key Benefits

- **Improve and accelerate your incident response and forensic capabilities** by giving security/SOC teams meaningful information about threats, and global insights into what lies behind targeted attacks. Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats, minimizing incident response time and disrupting the kill chain before critical systems and data are compromised.
- **Conduct deep searches into threat indicators** such as IP addresses, URLs, domains or file hashes, with highly-validated threat context that allows you to prioritize attacks, improve staffing and resource allocation decisions, and focus on mitigating the threats that pose the most risk to your business.
- **Mitigate targeted attacks.** Enhance your security infrastructure with tactical and strategic threat intelligence by adapting defensive strategies to counter.

1 http://www.kaspersky.com/top3



Now You Can

- Look up threat indicators via a web-based interface or via the RESTful API.
- Understand why an object should be treated as malicious.
- Check whether the discovered object is widespread or unique.
- Examine advanced details including certificates, commonly used names, file paths, or related URLs to discover new suspicious objects.

These are just examples. There are so many ways you can leverage this rich, continuous source of relevant, granular intelligence data.

Know your enemies and your friends. Recognize proven non-malicious files, URLs and IP addresses, increasing investigation speed. When every second could be critical, don't waste precious time analyzing trusted objects.

Our mission is to save the world from all types of cyber-threat. To achieve this, and to make the Internet safe and secure, it's vital to share and access threat intelligence in Real Time. Timely access to information is central to maintaining the effective protection of your data and networks. Now, Kaspersky Threat Lookup makes accessing this intelligence more efficient and straightforward than ever.

Key Features:

- Loaded and run DLLs
- Created mutual extensions (mutexes)
- Modified and created registry keys
- External connections with domain names and IP addresses
- HTTP and DNS requests and responses
- Processes created by the executed file
- Created, modified and deleted files
- Process memory dumps and network traffic dumps (PCAP)
- Screenshots
- Detailed threat intelligence with actionable context for every revealed indicator of compromise (IOC)
- RESTful API
- and much more

Key Benefits:

- Advanced detection of APTs, targeted and complex threats
- A workflow allowing the running of highly effective and complex incident investigations
- Scalability without the need to purchase costly appliances or worry about system resources
- Seamless integration and automation of your security operations

Cloud Sandbox

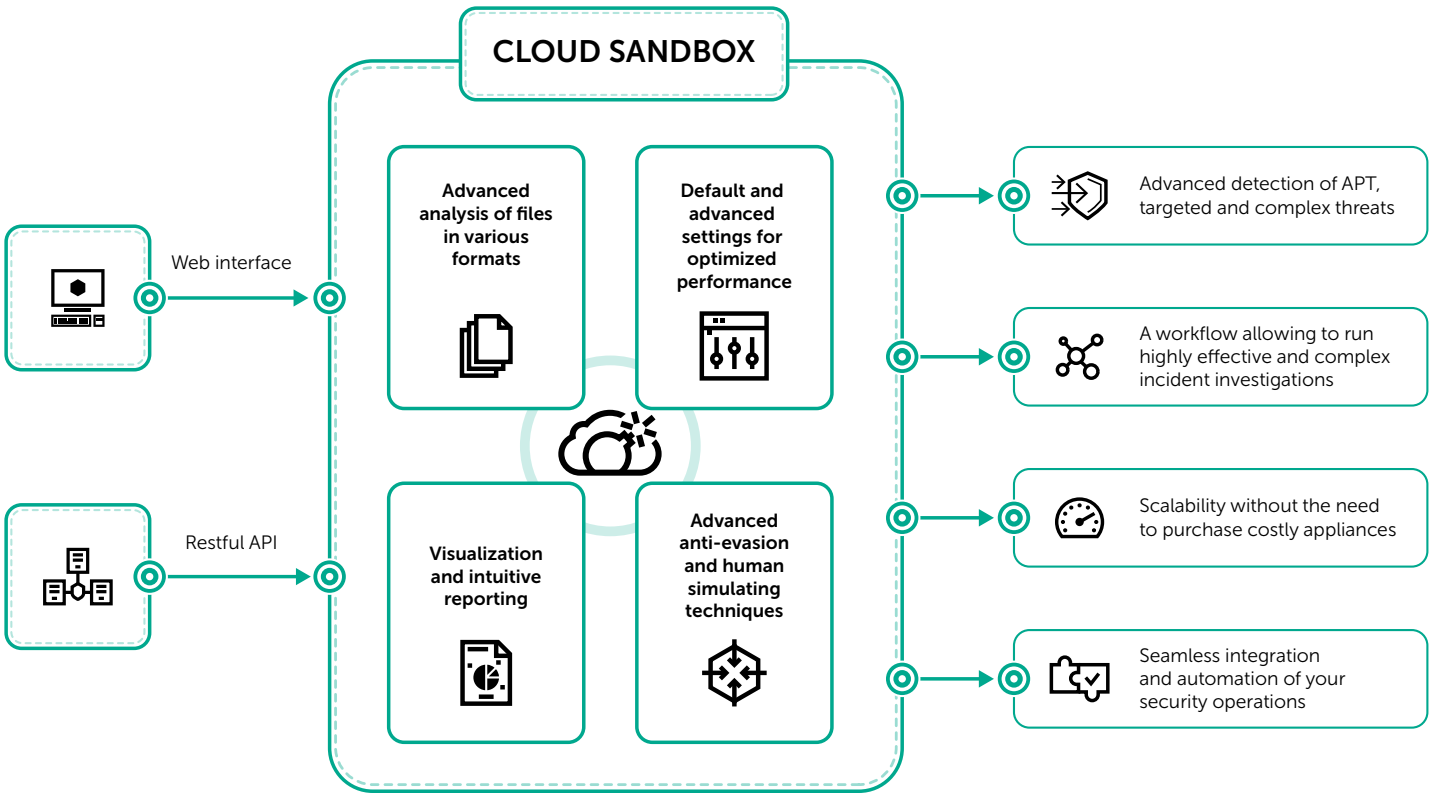
It's impossible to prevent today's targeted attacks purely with traditional AV tools. Antivirus engines are capable of stopping only known threats and their variations, while sophisticated threat actors use all the means at their disposal to evade automatic detection. Losses from information security incidents continue to grow exponentially, highlighting the increasing importance of immediate threat detection capabilities to ensure rapid response and counter the threat before any significant damage is done.

Making an intelligent decision based on a file's behavior while simultaneously analyzing the process memory, network activity etc. is the optimal approach to understand current sophisticated targeted and tailored threats. While statistical data may lack information on recently modified malware, sandboxing technologies are powerful tools that allow the investigation of file sample origins, the collection IOCs based on behavioral analysis and the detection of malicious objects not previously seen.

Proactive mitigation for threats circumventing your security barriers

Today's malware uses a whole variety of methods to avoid executing its code if this could lead to the exposure of its malicious activity. If the system does not meet the required parameters, the malicious program will almost certainly destroy itself, leaving no traces. For the malicious code to execute, the sandboxing environment must therefore be capable of accurately mimicking normal end-user behavior.

Kaspersky Cloud Sandbox offers a hybrid approach combining threat intelligence gleaned from petabytes of statistical data (thanks to Kaspersky Security Network and other proprietary systems), behavioral analysis, and rock-solid anti-evasion, with human-simulating technologies such as auto clicker, document scrolling, and dummy processes. The result is an instrument of choice for the detection of unknown threats.



This service has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over a decade. This technology incorporates all the knowledge about malware behaviors acquired by Kaspersky during 20 years of continuous threat research, allowing us to detect 350 000+ new malicious objects each day and to provide our clients with industry-leading security solutions.

As part of our Threat Lookup, Kaspersky Cloud Sandbox is the final component that completes your threat intelligence workflow. While Threat Lookup retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, etc., Cloud Sandbox allows that knowledge to be linked to the IOCs generated by the analyzed sample.

Now you can run highly effective and complex incident investigations, gaining an immediate understanding of the nature of the threat, then connecting the dots as you drill down to reveal interrelated threat indicators.

Inspection can be very resource intensive, especially when it comes to multi-stage attacks. Kaspersky Cloud Sandbox is an ideal tool to boost incident response and forensic activities, providing you with the scalability for processing files automatically without purchasing costly appliances or worrying about system resources.

What you get in the reports

- **Executive summary:**
  - {Threat urgency} / {vulnerability severity} assessment
  - Threat / vulnerability description
  - Timeline
  - Distribution across regions, countries and industries
  - Recommendations on risk mitigation
- **Detailed description of analysis results**
- **For reports on threats:**
  - Attack methods
  - Exploits used (if any)
  - Malware description(s)
  - C&C infrastructure and protocol descriptions
  - Victim analysis
  - Data exfiltration analysis
  - Attribution
- **For reports on vulnerabilities:**
  - Public availability of exploits
  - Signs of exploitation in real-world attacks
  - Methodology used to identify the vulnerability
  - Technical analysis of security issues that made it possible to exploit the vulnerability
  - Possible attack vectors (possibly in conjunction with other vulnerabilities and security flaws)
  - Evaluation of products / product versions affected
  - Estimates of vulnerable product distribution across regions / countries / industries
- **Conclusions**
- **Appendix**
  Technical analysis, important IOCs and any additional relevant information

Industrial Control Systems (ICS) Threat Intelligence Reporting

The **Kaspersky ICS Threat Intelligence Reporting Service** provides the customer with 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 are delivered via a web-based portal, which means you can start using the service immediately.

Report types you get with the subscription

1. **APT reports.** Reports on new APT and high-volume attack campaigns targeting industrial organizations, and updates on active threats.
2. **Threat landscape.** Reports on significant changes to the threat landscape for industrial control systems, newly discovered critical factors affecting ICS security levels and ICS exposure to threats, including regional, country- and industry-specific information.
3. **Vulnerabilities found.** Reports on vulnerabilities identified by Kaspersky in the most popular products used in industrial control systems, the industrial internet of things, and infrastructures in various industries.
4. **Vulnerability analysis and mitigation.** Our advisories provide well-thought actionable recommendations from Kaspersky experts to identify and mitigate vulnerabilities in your infrastructure.

What you can do with threat intelligence data

Detect and prevent reported threats to safeguard critical assets, including software and hardware components and to ensure safety and continuity of technological process.

Correlate malicious and suspicious activity you detect in industrial environments with Kaspersky's research results to attribute your detection to the reported malicious campaigns, identify threats and promptly respond to incidents.

Perform a vulnerability assessment of your industrial environments and assets based on accurate assessments of vulnerability scope and severity and make informed decisions on patch management or the implementation of the other preventative measures we recommend.

Leverage information on attack technologies, tactics and procedures, recently discovered vulnerabilities and other important threat landscape changes we report to:

- Identify and assess the risks posed by the reported threats and other similar threats;
- Plan and design changes to industrial infrastructure to ensure the safety of production and continuity of technological process;
- Perform security awareness activities based on analysis of real-world cases to create personnel training scenarios and plan red team vs. blue team exercises;
- Make informed strategic decisions to invest in cybersecurity and to ensure resilience of operations.

Service Benefits

Exclusive

- **Insight into non-public information:** as a cybersecurity professional you get information that might be essential for planning and performing cybersecurity activities, but which is not publicly available due to responsible disclosure policies.
- **Early access to technical information on threats** while research and investigation is still ongoing, and before information is made public.
- **Exclusive access to information** that may never be released into the public domain due to the risk of malicious actors abusing it (does not include software sent exclusively to vendors to demonstrate vulnerabilities).

Actionable

- **Early response to emerging threats:** the information and tools provided allow you to quickly respond to new threats and vulnerabilities, to mitigate risks associated with advanced attacks and those that use known vectors.
- Technical information for ICS cybersecurity operations: the subscription includes **access to technical artifacts,** such as indicators of compromise (IOCs) that can be integrated into a customer's automated tools and used to support vulnerability assessment, incident detection, response and investigation activities.

Complete

- **Retrospective analysis:** access to all previously released private reports during the subscription period.
- **Continuous malicious campaign monitoring:** access to actionable intelligence during an investigation and updates on new findings, including TTP changes and IOCs of newly detected toolsets.

Easy to use

- **Automation:** report information can be automatically parsed and integrated into automated cybersecurity processes.
- **Support for multiple industrial standards:** IOCs are provided in industrial-grade formats, such as OpenIOC, STIX, YARA and SNORT rules.

Try our service

You can request **demo access** to the Kaspersky ICS Threat Intelligence Reporting at https://tip.kaspersky.com. The demo version contains **around 10 example reports** that include data on attacks on industrial companies, the results of research into vulnerabilities in industrial solutions, as well as information on the threat landscape facing industrial automation systems.

Request more information at ics-cert-query@kaspersky.com.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky BRING ON THE FUTURE