Stay ahead of your adversaries

Kaspersky Threat Intelligence

kaspersky bring on the future

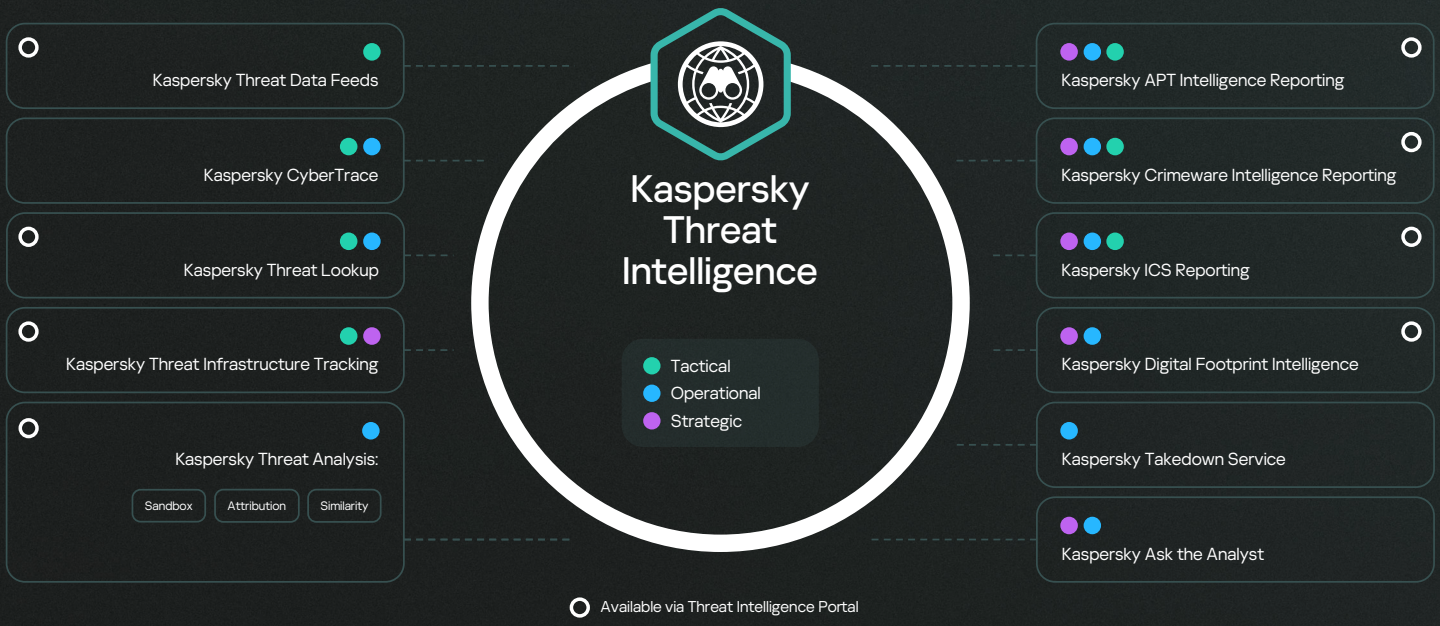
Kaspersky
Threat Intelligence

Kaspersky Threat Intelligence

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

Kaspersky's knowledge, experience and deep intelligence of every aspect of cybersecurity has made us the trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and leading CERTs. Kaspersky Threat Intelligence gives you instant access to tactical, operational and strategic Threat Intelligence.

Kaspersky Threat Intelligence delivers a comprehensive view of the global threat landscape, combining intelligence sources, threat data feeds, and in-house research, all analyzed by our team of experts to deliver actionable insights to help organizations protect against cyber threats.



Tactical

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

Roles:
- SOC Analyst

Systems:
- SIEM
- NGFW
- IPS
- IDS
- SOAR

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
- EDR/XDR
- TIP

Processes:
- Incident Response
- Threat Hunting

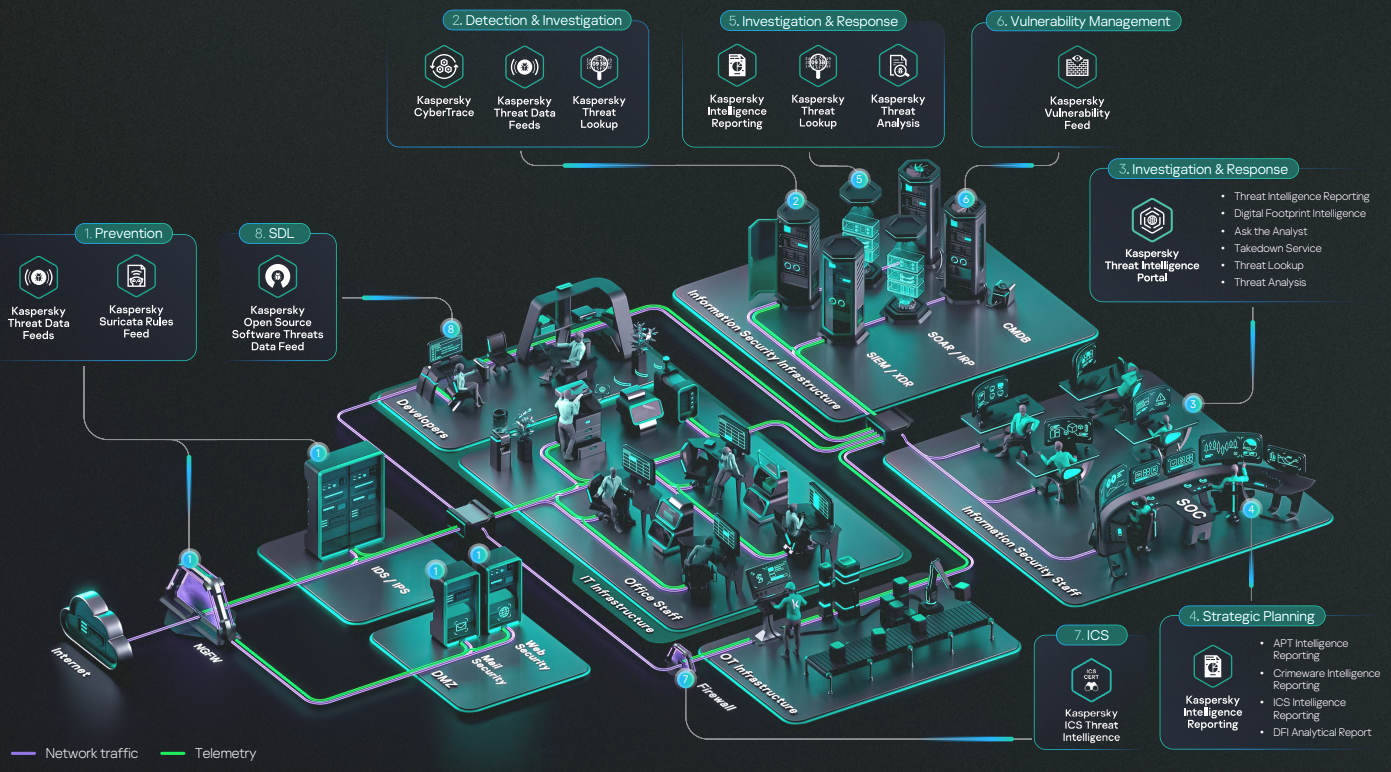
Strategic

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

Kaspersky Threat Intelligence application scheme



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.

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.

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.

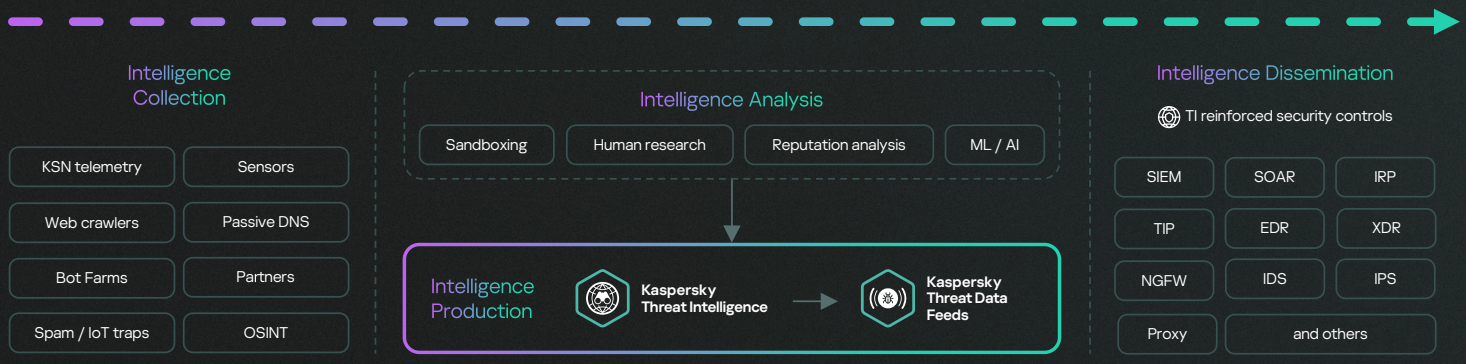
Kaspersky
Threat Data
Feeds

Kaspersky Threat Data Feeds

Cyberattacks happen every day. Cyberthreats are constantly growing in frequency, complexity and obfuscation, as they try to compromise your defenses. Adversaries use complicated intrusion kill chains, campaigns and customized Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your customers. Effective 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 systems like SIEM, SOAR and Threat Intelligence Platforms, 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 teams for further investigation and response.

Kaspersky Threat Data Feed delivers real-time threat intelligence information to help you protect your networks and systems from cyberthreats. Data feeds include information on known malware, phishing websites, the latest vulnerabilities and exploits, and other types of cyberthreats - information to help you block malicious traffic, update your security software, and take other measures to protect against cyberattacks.



1

Data is collected from a wide variety of trusted sources, including the Kaspersky Security Network and our own crawlers, botnet threat monitoring service (tracks botnets and their targets 24/7), spam traps, data from research groups, partners and much more.

2

All collected information is carefully checked and cleaned in real time using various pre-processing methods: sandboxing, statistical and heuristic analysis, similarity tools, behavioral profiling and expert analysis.

3

Data Feeds help to collect threat information about an alert or incident, and to dig into details. It also helps answer the questions 'Who? What? Where? Why?' and identify the source of an attack, enabling quick decision-making to protect your company from threats of any complexity.

Contextual data

Contextual data helps reveal the 'bigger picture', further validating and supporting the wide-ranging use of the data. Entries in feeds provided by Kaspersky contain the following contextual data that help you to quickly confirm and prioritize threats:

1. Threat names
2. IP addresses and domain names of malicious web resources
3. Hashes of malicious files
4. Vulnerable and compromised objects
5. Tactics, techniques and procedures of attacks according to MITRE ATT&CK classification
6. Timestamps
7. Geolocation
8. Popularity, and so on

Kaspersky Threat Data Feeds benefits

Improve and accelerate your incident response and forensic capabilities

by automating the initial triage process while providing your security analysts with enough context to immediately identify alerts that need to be investigated or escalated to incident response teams for further investigation and response.

Reinforce your security solutions

including SIEMs, Firewalls, IPS/IDS, Security Proxy, DNS solutions, Anti-APT, with continuously updated Indicators of Compromise (IOCs) and actionable context to get insights into cyberattacks and a greater understanding of the intent, capabilities and targets of your adversaries. Leading SIEMs (including ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) and TI Platforms are fully supported.

Prevent the exfiltration of sensitive assets and intellectual property

from infected machines to outside your organization. Detect infected assets fast to protect your brand reputation, maintain your competitive advantage and secure business opportunities.

Grow your MSSP business

by providing industry-leading threat intelligence as a premium service to your customers. As a CERT, enhance and extend your cyberthreat detection and identification capabilities.

Kaspersky CyberTrace

Kaspersky CyberTrace

The ongoing growth in the number of threat data feeds and available threat intelligence sources makes it difficult for companies to determine what information is relevant for them. At the same time, threat intelligence comes in many different formats and includes a huge number of Indicators of Compromise (IoCs), making it hard for SIEMs and other network security controls to digest them.

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 security analysts with enough context to immediately identify alerts that need to be investigated or escalated to incident response teams for further investigation and response.

Kaspersky CyberTrace is a threat intelligence platform 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 (from Kaspersky, other vendors, OSINT or your own customer feeds) in JSON, STIX, XML and CSV formats, and supports out-of-the-box integration with numerous SIEM solutions and log sources.

Highlights

Detailed information about each indicator to provide even deeper analysis. Each page presents all information about an indicator from all threat intelligence suppliers (deduplication) so analysts can discuss threats in the comments and add internal threat intelligence about each indicator

Feed usage statistics for measuring the effectiveness of the integrated feeds and the feeds intersection matrix help choose the most valuable threat intelligence suppliers

Tagging IoCs simplifies IoC management. Create any tag and specify its weight (importance) and use it to tag IoCs manually. You can also sort and filter IoCs based on these tags and their weights

A Research Graph lets you visually explore data and detections stored in CyberTrace and discover threat commonalities

The indicators export feature lets you export indicator sets to security controls such as policy lists (block lists) and share threat data between Kaspersky CyberTrace instances or with other TI platforms

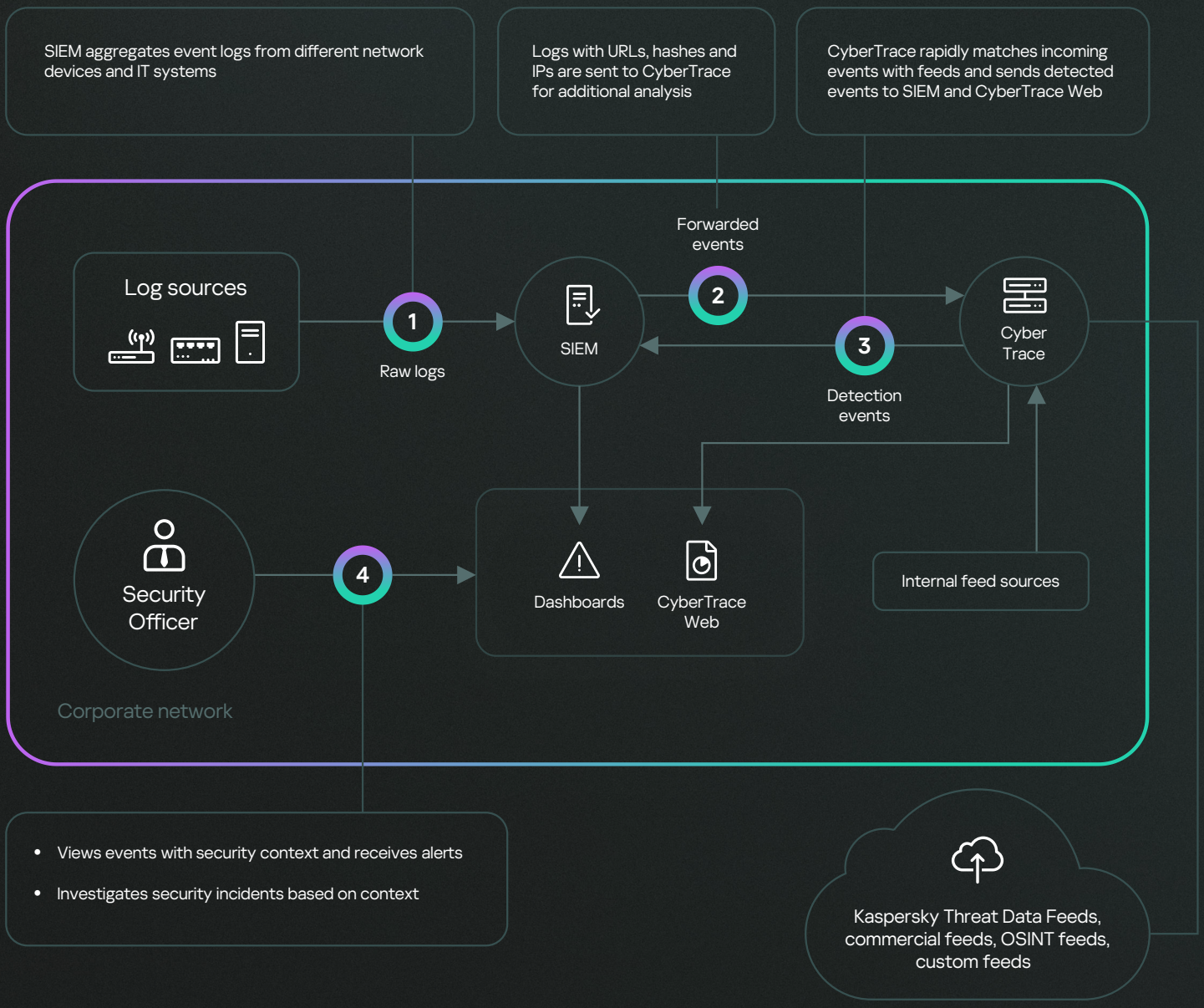
The historical correlation feature (retroscan) lets you analyze observables from previously checked events using the latest feeds to find previously discovered threats

Multitenancy supports MSSPs and large enterprise use cases

Sends detection events to SIEM solutions, reducing the load on SIEM as well as analysts

HTTP RestAPI lets you look up and manage threat intelligence

How it works



Kaspersky CyberTrace parses incoming logs and events, rapidly matches the resulting data to feeds, and generates its own threat detection alerts, significantly reducing the SIEM workload.

Benefits of using CyberTrace with Kaspersky Threat Data Feeds

Effectively distill and prioritize huge amounts of security alerts

Improve and accelerate triage and initial response processes

Build a proactive and intelligence-driven defense

Immediately identify alerts critical for your business and escalate to IR teams

Kaspersky
Threat Lookup

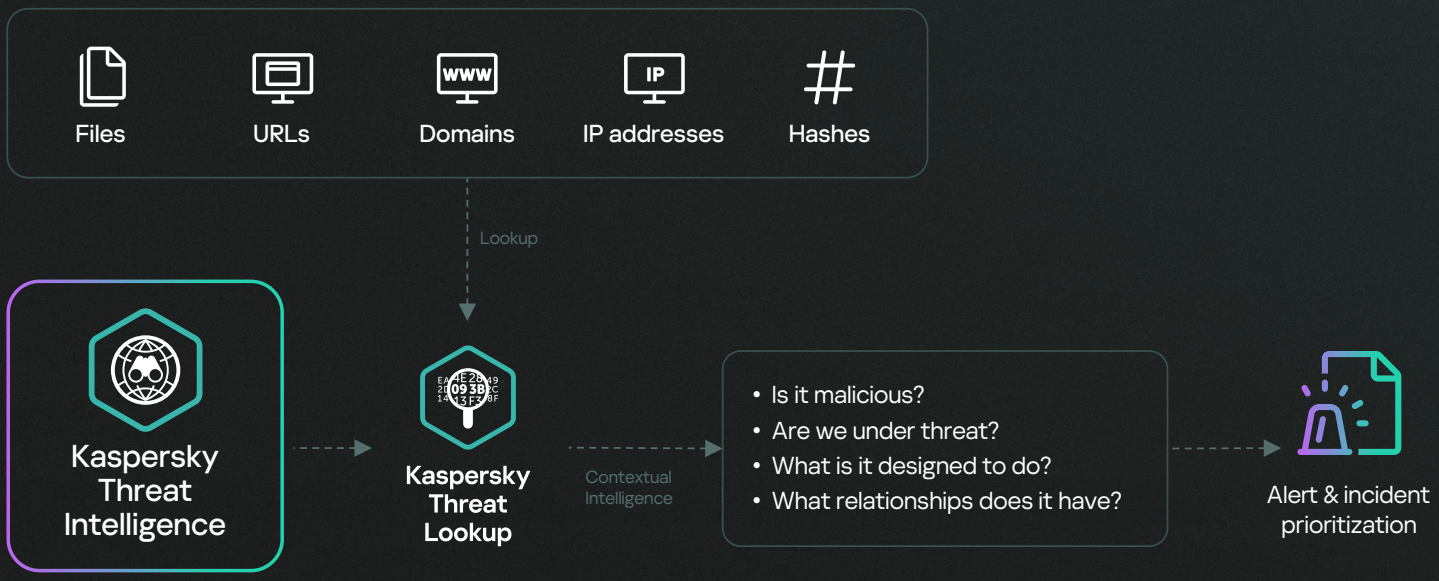
Kaspersky Threat Lookup

Cybercrime 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. Cyberthreats 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 cyberthreats and their relationships, brought together into single, powerful web service. The goal is to provide your security teams with as much data as possible, preventing cyberattacks 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.

How it works

Objects to analyze



Highlights

Trusted Intelligence

A key attribute of Kaspersky Threat Lookup is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky leads the field in anti-malware tests, 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 discover a threat, the less damage it can cause, the faster repairs take place and the sooner network operations can get back to normal.

Easy-to-use

Web interface or RESTful API. Use the service in manual mode through a web interface (via a web browser) or access it via a simple RESTful API — whichever you prefer

Wide range of export formats

Export IOCs (Indicators of Compromise) or actionable context into widely used, more organized machine-readable sharing formats, such as STIX, OpenIOC, JSON, Yara, Snort or even CSV, to extract the maximum benefit of threat intelligence, automate operational workflow, or integrate with security controls such as SIEMs.

Kaspersky Threat Lookup benefits

1. Conduct deep searches into threat indicators with highly-validated threat context that lets you prioritize attacks and focus on mitigating the threats that pose the most risk to your business
2. Diagnose and analyze security incidents on hosts and the network more efficiently and prioritize signals from internal systems against unknown threats
3. Boost your incident response and threat hunting capabilities to disrupt the kill chain before critical systems and data are compromised
4. Look up threat indicators from a web-based interface or via the RESTful API
5. Examine advanced details including certificates, commonly used names, file paths, or related URLs to discover new suspicious objects
6. Check whether the discovered object is widespread or unique and understand why an object should be treated as malicious

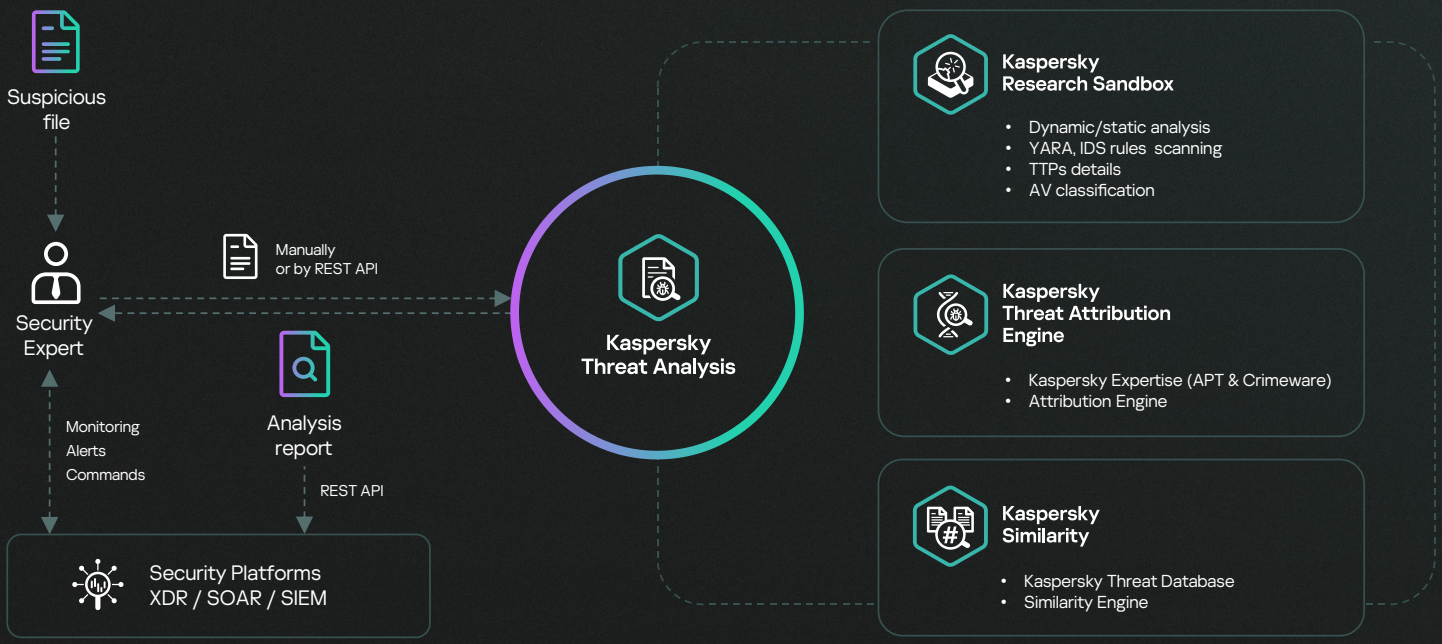
Kaspersky
Threat Analysis

Kaspersky Threat Analysis

Faced with a potential cyberthreat, the decisions you make, and how well you can make them, can both prove critical. It is impossible to prevent today's targeted attacks solely with traditional anti-virus tools. Anti-virus engines are capable of stopping only known threats and their variations, while sophisticated threat actors use all means at their disposal to evade automatic detection. The number of security alerts processed by SOCs every day is growing exponentially. With the amount of malware samples generated every day, effective alert prioritization, triage, and validation becomes nearly unfeasible.

To help security researchers stay informed about existing and emerging threats, Kaspersky provides a single resilient framework to automate routine analysis of suspicious files. In addition to traditional threat analysis technologies like sandboxing, Kaspersky Threat Analysis arms you with state-of-the-art attribution and related similarity technologies — a hybrid approach that delivers efficient threat analysis, so you can make fully informed decisions and keep your infrastructure secure. Kaspersky Threat Analysis is provided via both a united web and RESTful interfaces.

Kaspersky Threat Analysis components



Kaspersky
Research Sandbox

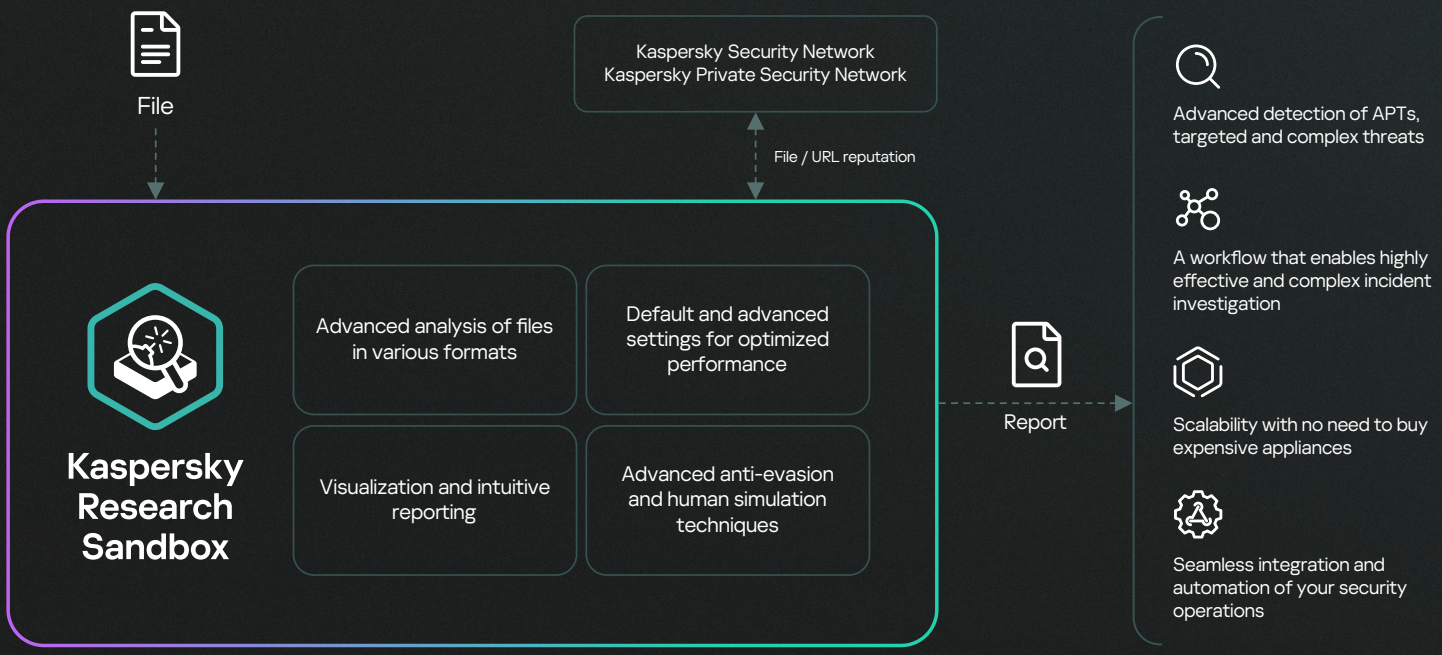
Kaspersky Research Sandbox

Kaspersky Research Sandbox has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over two decades. It incorporates all the knowledge about malware behaviors we have acquired throughout our continuous threat research, allowing us to detect 420 000+ new malicious objects every day.

Kaspersky Research Sandbox enables to investigate the origins of file samples, collect IOCs based on behavioral analysis, and detect malicious objects not previously seen. It offers a hybrid approach, combining behavioral analysis and rock- solid anti-evasion techniques, with human-simulating technologies, such as auto clicker, document scrolling, and dummy processes.

Deployed on-premise, the technology prevents exposure of data outside the organization. Kaspersky Research Sandbox on-premise also allows to create custom execution environments for analysis tailoring them to real environments, which increases the accuracy of threat detection and the speed of investigation.

How it works



Product highlights

- Patented technology
- Automated object analysis in Windows, Linux and Android environments
- Support analysis of 200+ file types with detailed analysis reports
- 1000+ unique hunts for extracting TTPs by MITRE ATT&CK
- Advanced anti-evasion techniques and human-simulating technologies
- The threat score based on metrics and data obtained during file execution shows the danger level of analyzed object
- Preconfigured Suricata rules to inspect the network traffic generated during file execution
- Manual sample upload and an enhanced REST API for integration with automated workflows

Kaspersky
Threat Attribution
Engine

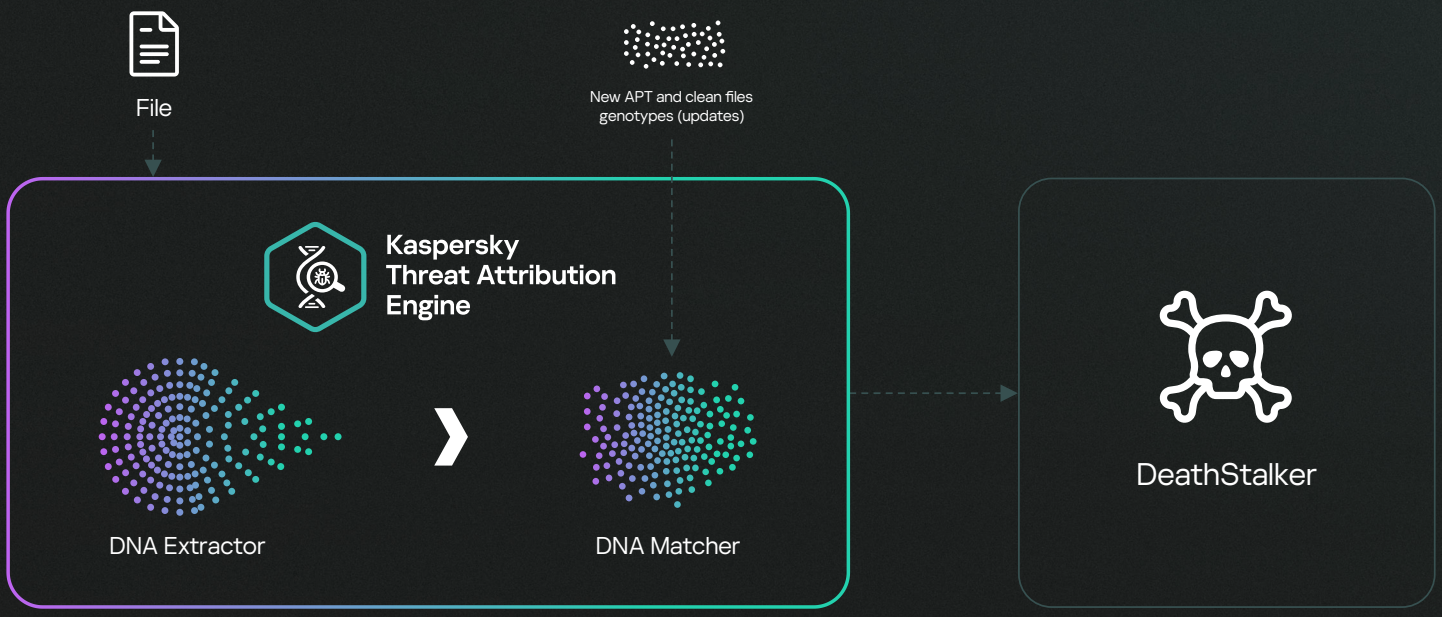
Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine is a unique threat analysis tool providing insights into the origin of high-profile malware and its possible authors. It quickly connects a suspicious file to known APT threats, actors, campaigns, using a unique algorithm and a special database comprising APT malware samples and the industry's largest collection of clean files gathered by Kaspersky experts over the last 25 years and more.

We track 1100+ threat actors and campaigns and release 200+ threat intelligence reports a year. Our ongoing research supports an APT collection which contains more than 100 000 files that, in conjunction with the use of automated tools, results in outstandingly accurate level of attribution.

The product offers a unique approach to comparing similar samples while ensuring near-zero false positive rates. Any new attack can quickly be linked to known APT malware, previous targeted attacks and hacker groups, helping you to distinguish high-risk threats from less serious incidents, so you can take timely protective measures to prevent an attacker from gaining a foothold in your system. Kaspersky Threat Attribution Engine can be deployed in secure, air-gapped environments, restricting any 3rd party from accessing the processed information and submitted objects. On-premise deployment provides additional functionality to add own actors and samples to detect samples that are similar to files in your private collection as well as export YARA rules for further automated search for similar files in your infrastructure an integration with third-party solutions.

How it works



Proprietary searching method

To link malware to attribution entities, Kaspersky Threat Attribution Engine uses a unique proprietary method of searching for similar genotypes and strings between files. This method involves:

1

Analyzing the genetics of a sample by extracting the following elements from its code:

- Genotypes — distinctive pieces of binary code.
- Strings — distinctive strings of characters.

2

Automatically searching the analyzed files for genotypes and strings which are similar to genotypes and strings of APT samples previously analyzed, or already linked to attribution entities.

3

Based on similar genotypes and strings found in APT samples, providing a report on the origin of the analyzed sample, related attribution entities, and any similarities between this sample and known APT samples.

Product highlights

- Patented technology
- Instant access to a repository of curated data about thousands of APT actors, samples and campaigns
- Manual sample upload and an enhanced REST API for integration with automated workflows
- Functionality for unpacking password protected archives with custom passwords
- Export to STIX 2.1 format (TXT and JSON are also supported) for further automated analysis of security logs or integration with third- party solutions
- Supports deployment on cloud infrastructures such as Amazon Web Services (AWS) enabling quick product setup and saving costs as no need to invest in hardware upfront

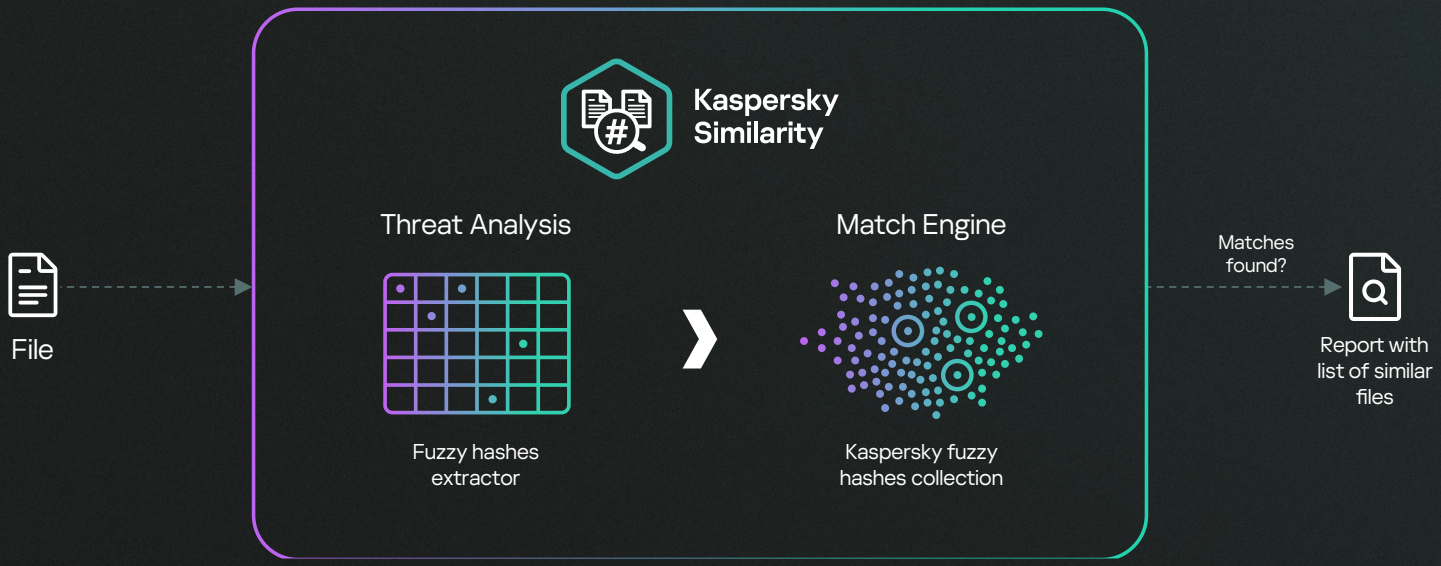
Kaspersky Similarity

Kaspersky Similarity

Kaspersky Similarity is a handy tool for identifying files with similar functionality based on the technology developed by Kaspersky experts to protect against unknown and hidden threats. The technology uses more than 50 unique types of special hashes and a database of malware samples accumulated by Kaspersky over 25 years and containing millions of malicious files to ensure the highest accuracy and reliability of results.

Kaspersky Similarity enables to find similar (e.g. evasive) malware samples and look for them in the infrastructure to make you confident that even a slight change of the sample, made by the adversary, is still on your security radar.

How it works



Similarity reports

Kaspersky experts have created a set of hashes to determine the similarity between different files based on these attributes.

Kaspersky Similarity allows users to submit a suspicious file, extract its hashes and compare them with hashes of files existing in Kaspersky threat database. In case the matches are found it generates the list of hashes for TOP similar malicious files, already known to Kaspersky and sorted by similarity score. The report contains the additional context with metadata for each similar file:

- Similarity confidence
- File status (malware, adware or other)
- Threat name
- Timestamps of first and last detection
- Quantity of hits (detections)
- File hash
- File type
- File size

Product highlights

- Patented technology
- Leverages one of the largest in the industry database of malicious and clean files, collected by latest 25+ years, enabling maximum coverage for highest comparison accuracy
- Manual sample upload and an enhanced REST API for integration with automated workflows
- The technology has long been used by Kaspersky experts for exploring new threats to deliver even higher threat protection in our products which is regularly confirmed by regular top rates according to independent tests:

Learn more

Kaspersky Threat Analysis benefits

1

Boost your incident response and forensic activities with Kaspersky Research Sandbox, providing you with the cutting-edge dynamic analysis of suspicious files with ability to find 0-day threats and results mapped to MITTRE ATT&ACK TTPs.

2

Correct and timely attribution with Kaspersky Threat Attribution Engine helps to define threat actor with the full list of TTPs providing comprehensive view of attack vector with clear mitigation steps enabling to shorten incident response times from months to minutes.

3

Reveal evasive threats with Kaspersky Similarity enabling to find malicious samples, that have been specially created to bypass traditional anti-malware technologies, thus to detect the most sophisticated APT-attacks which can last for years untracked.

Kaspersky Intelligence Reporting

Kaspersky Threat Intelligence Reporting

Counteracting modern cyberthreats requires a 360-degree view of the tactics, techniques and procedures used by threat actors. While the C&Cs and tools used in attacks change frequently, it's difficult for attackers to change their behavior and methods during attack execution. Identifying and exposing these patterns promptly helps deploy effective defensive mechanisms in advance, disarming cybercriminals and disrupting the kill chain.

Subscribing to Kaspersky Threat Intelligence Reporting provides ongoing exclusive access to our research, providing up-to-date information on the most dangerous threats, enabling you and your security team to proactively apply an effective strategy for attack detection in a timely manner, as well as minimizing the damage from similar threats.

While only a small percentage of our investigations are made public, Kaspersky Intelligence Reporting gives you privileged access to the most up-to-date information on the latest threats. Our experts continuously monitor the activities of cybercriminals, identifying the most sophisticated and dangerous targeted attacks, cyber espionage campaigns, malware and encryption samples, and the latest cybercrime trends around the world.

200+
private reports a year

300+
threat actors

500+
campaigns

2500+
YARA rules

170 000+
IoCs

Analytical reports include:

Threat actor profiles

Mapping to MITRE ATT&CK

Executive summary (C-level oriented information)

Deep technical analysis including:

- Attack methods
- Exploits used
- Malware description
- C&C infrastructure and protocols description
- Victim analysis
- Data exfiltration analysis
- Attributions

Indicators of Compromise (IOCs) and YARA / SIGMA / Suricata rules

Recommendations from Kaspersky experts

We offer several different commercial reporting tracks based on your needs and the specifics of your organization:

Kaspersky APT Intelligence Reporting

Provides insights into sophisticated, long-term targeted cyber threats that often originate from well-organized and well-funded groups. It includes information on various APT groups worldwide and their tactics, techniques, and procedures (TTPs), as well as the sectors and regions they target. This reporting track focuses on espionage activities, spanning from supply-chain attacks to hacktivist and destructive activities. These reports are ideal if your organization is a large corporation, government agency or an organization involved in critical infrastructure, and are also particularly relevant to organizations holding sensitive data that may be a subject of interest to government entities.

Kaspersky Crimeware Intelligence Reporting

Focuses on attacks and campaigns with financial gain as their primary goal. It includes information on the latest trends in cybercrime, including stolen data sold on the darkweb, financial fraud, ransomware, and ATM/PoS malware. They provide details on new crimeware varieties, their distribution methods and the types of data they target. This reporting track is particularly relevant if your organization conducts a substantial amount of business online, or you hold sensitive customer data - perhaps as a financial institution or ecommerce platform.

Kaspersky ICS Threat Intelligence

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. This reporting track is delivered by Kaspersky ICS CERT – a dedicated team of 30+ highly qualified experts in ICS threat and vulnerability research, incident response and security analysis, established in 2016. These reports provide actionable insights and guidance to safeguard your critical assets - including software and hardware component - and ensure the safety and continuity of your technological processes.

You may wish to consider the following related Kaspersky ICS Threat Intelligence services:

ICS Threat Intelligence Reporting

Subscription to our regular publications on industrial cybersecurity threats and vulnerabilities:

- Alerts about 0-day threats
- Detailed technical reports
- Monthly reviews
- Recommendations on vulnerability mitigations
- Statistics and trends

ICS Threat Data Feeds

Machine-readable data streams about industrial cybersecurity threats and vulnerabilities.

Simple data distribution formats (JSON, CSV, OpenIoC, STIX) via HTTPS, TAXII and specialized delivery methods for integration into information security solutions.

Ask the Analyst

Consultation with Kaspersky ICS CERT experts, providing you with individual advice on the industrial cybersecurity threats and vulnerabilities, threat statistics and landscape, industry standards, etc most relevant to you.

Kaspersky Threat Intelligence Reporting gives you:

Privileged access

For various reasons, not all high-profile threats are made known to the general public. However, we provide this kind of exclusive information to our customers during the investigation process, even before the official public announcement.

Access to technical data

Including an extended list of IOCs, available in standard formats including openIOC or STIX, as well as access to our YARA / Sigma / Suricata rules.

Threat actor profiles

Including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with mapping to MITRE ATT&CK.

MITRE ATT&CK

All TTPs described in the reports are mapped to MITRE ATT&CK, 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.

Retrospective analysis

Access to all previously issued private reports is available throughout your subscription.

RESTful API support

Seamless integration and automation of your security workflows.

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

As your business grows, the complexity and distribution of your IT environments grow too, presenting a challenge: protecting your widely distributed digital presence without direct control or ownership. Dynamic and interconnected environments enable companies to derive significant benefits. 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 be able to track its changes and react to external threats aimed at exposed digital assets.

Organizations use a wide range of security tools in their security operations but there are still digital threats that loom which require very specific capabilities - to detect and mitigate data leakages, monitor plans and attack schemes of cybercriminals located on dark web forums, etc. To help your security analysts explore the adversaries' view of your company resources, promptly discover the potential attack vectors available to them and adjust your defenses accordingly, Kaspersky has created Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence provides

Threats Detection

Monitoring of fraudulent activities that can damage a company's reputation and/or deceive customers.

Network reconnaissance

Identification of the customer's network resources and exposed services which are a potential entry point for an attack.
Tailored analysis of existing 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).

Dark Web monitoring

Continuous monitoring of dark web resources (forums, ransomware blogs, messengers, tor sites, etc.), detecting any references and threats relating to your company, clients and partners. Analysis of active targeted attacks or attacks that are being planned, APT campaigns aimed at your company, industry and regions of operation.

Discovery of data leaks

Detection of compromised employees, partner and client credentials, bank cards, phone numbers and other sensitive information that can be used to carry out an attack or pose reputational risks for your company.

Multitenancy support

Enhanced capabilities for managed security service providers (MSSPs) and large organizations with a multi-branch structure.

Intelligence sources

It's essential that you have a comprehensive understanding of your business's external security posture. To provide this information, Kaspersky security analysts collect and aggregate information from the following intelligence sources:

Your unstructured data

- IP addresses
- Company domains
- Brand names
- Keywords
- Network ranges
- BIN/IIN card numbers
- Employee information

Network perimeter inventory

Surface, deep and dark web search

Kaspersky Knowledge Base search

Threat alerts

Real-time search across Kaspersky's, surface and dark web sources

Analytical reports*

How it works

Configure	Collect	Filter	Notification
Information discovery about the company's digital assets	Automated data collection from surface, deep and dark webs, and the Kaspersky knowledgebase	Threat detection, analysis and prioritization managed by analysts	Providing promtly threat notifications on Kaspersky Threat Intelligence Portal or via API

* Add-on service

Digital Footprint Intelligence business values

Kaspersky Digital Footprint Intelligence delivers powerful benefits and significant value to your organization:

Threats detection

Detect potential threats in real-time to protect your brand reputation, preserve customer trust, reduce the risk of financial loss and damage to business operations.

Reduce cyber risks

Equip your key stake holders (CxO and Board) with information on where to focus cybersecurity spending by revealing gaps in the current setup and the risks they bring.

React faster

Additional context for security alerts improves incident response and reduces your Mean Time To Respond (MTTR)

Reduce the attack surface

Manage your company's digital presence and control external network resources to minimize attack vectors and vulnerabilities that can be used for an attack.

Understand your adversaries

Forewarned is forearmed - know what cybercriminals are planning and discussing about your company on the dark web so that you're prepared for it.

Know the unknown

Improve your ability to withstand cyberattacks and identify threats outside the jurisdiction of your internal security teams.

Service delivery efficiency

Rapid start and easy scaling in multitenancy mode saves time both for managed security service providers (MSSP) and their customers, as well as large multi-affiliate organizations.

Kaspersky Takedown Service

Kaspersky Takedown Service

Cybercriminals create malicious and phishing domains which are used to attack your company and your brands. The inability to quickly mitigate these threats, once identified, can lead to a loss of revenue, brand damage, loss of customer trust, data leaks, and more. But managing takedowns of these domains is a complex process that requires expertise and time.

Kaspersky Takedown Service quickly mitigates threats posed by malicious and phishing domains before any damage can be caused to your brand and business. End-to-end management of the entire process saves customers valuable time and resources. The service is delivered globally.

Kaspersky blocks more than 15 000 phishing/scam URLs and prevents over a million attempts clicking such URLs every single day. Our many years of experience in analyzing malicious and phishing domains means we know how to collect all the necessary evidence to prove that they are malicious. We'll take care of your takedown management and enable swift action to minimize your digital risk so your team can focus on other priority tasks.

Kaspersky provides its customers with effective protection of their online services and reputation by working with international organizations, national and regional law enforcement agencies (e.g. INTERPOL, Europol, Microsoft Digital Crimes Unit, The National High-Tech Crime Unit (NHTCU) of the Netherlands' Police Agency and The City of London Police), as well as Computer Emergency Response Teams (CERTs) worldwide.

Complete visibility

You will be notified at each stage of the process, from registration of your request to a successful takedown

End-to-end management

We will manage the entire takedown process and minimize your involvement

Global coverage

It doesn't matter where a malicious or phishing domain is registered, Kaspersky will request its takedown from the regional organization with the relevant legal authority

How it works

You can submit your requests via Kaspersky Company Account, our corporate customer support portal. We will prepare all the necessary documentation and will send the request for takedown to the relevant local/regional authority (CERT, registrar, etc.) that has the necessary legal rights to shut down the domain. You will receive notifications at every step of the way until the requested resource is successfully taken down.

Effortless protection

The Kaspersky Takedown Service quickly mitigates threats posed by malicious and phishing domains before any damage can be caused to your brand and business. End-to-end management of the entire process saves you valuable time and resources.

Kaspersky
Ask the Analyst

Kaspersky Ask the Analyst

Cybercriminals are constantly developing sophisticated ways of attacking businesses. Today's volatile and fast-growing threat landscape features increasingly agile cybercrime techniques. Organizations face complex incidents caused by non-malware attacks, fileless attacks, living-off-the-land attacks, zero-day exploits — and combinations of all of these built into complex threats, APT-like and targeted attacks.

In an age of business-crippling cyberattacks, cybersecurity professionals are more important than ever, but finding and retaining them isn't easy. And even if you have a well-established cybersecurity team, your experts can't always be expected to fight the war against sophisticated threats alone — they need to be able to call on expert third-party assistance. External expertise can shed light on the likely paths of complex attacks and APTs, and deliver actionable advice on the most decisive way to eliminate them.

Continuous threat research enables Kaspersky to discover, infiltrate and monitor closed communities and dark forums worldwide frequented by adversaries and cybercriminals. Our analysts leverage this access to proactively detect and investigate the most damaging and notorious threats, as well as threats tailored to target specific organizations.

Kaspersky Ask the Analyst extends our Threat Intelligence portfolio, enabling you to request guidance and insights into specific threats you're facing or interested in. The service tailors Kaspersky's powerful threat intelligence and research capabilities to your specific needs, enabling you to build resilient defenses against threats targeting your organization.

Kaspersky Ask the Analyst Deliverables (Unified request-based subscription)

APT and Crimeware

Additional information on published reports and ongoing research (on top of APT or Crimeware Intelligence Reporting service)

Descriptions of threats, vulnerabilities and related IoCs

- General description of a specific malware family
- Additional context for threats (related hashes, URLs, CnCs, etc.)
- Information on a specific vulnerability (how critical it is, and the corresponding protection mechanisms in Kaspersky products)

ICS-related requests

- Additional information on published reports
- ICS Vulnerability information
- ICS threat statistics and trends for region / industry
- ICS Malware Analysis Information on regulations or standards

Dark Web intelligence

- Dark Web research on particular artefacts, IP addresses, domain names, file names, e-mails, links or images
- Information search and analysis

Malware analysis

- Malware sample analysis
- Recommendations on further remediation actions

How it works

Kaspersky Ask the Analyst can be purchased separately or in addition to any of our threat intelligence services. You can submit your requests via Kaspersky Company Account, our corporate customer support portal. We will respond by email, but if necessary and agreed on by you, we can organize a conference call and/or screen-sharing session. Once your request has been accepted, you'll be informed of the estimated timeframe for processing it.

Use cases

1. Clarify any details in previously published threat intelligence reports
2. Get additional intelligence for already provided IoCs
3. Obtain details on vulnerabilities and recommendations on how to protect against their exploitation
4. Receive additional details on the specific Dark Web activities you're interested in
5. Get an overview malware family report that includes the malware's behavior, its potential impact and details about any related activity Kaspersky has observed
6. Effectively prioritize alerts/incidents with detailed contextual information and categorization for related IoCs provided via short reports
7. Request assistance in identifying if detected unusual activity relates to an APT or crimeware actor
8. Submit malware files for comprehensive analysis to understand the behavior and functionality of the provided sample(s)

Kaspersky Ask the Analyst benefits

Expand your expertise

Get on-demand access to industry experts without having to search for and invest in hiring hard to find full-time specialists

Accelerate investigations

Effectively scope and prioritize incidents based on tailored and detailed contextual information

Respond fast

Respond to threats and vulnerabilities fast using our guidance to block attacks via known vectors

Extend your knowledge and resources

Kaspersky Ask the Analyst gives you access to a core group of Kaspersky researchers on a case-by-case basis. The service delivers comprehensive communication between experts to expand your existing capabilities with our unique knowledge and resources.

Conclusion

Counteracting today's cyberthreats requires a 360-degree view of the tactics and tools used by threat actors. Generating this intelligence and identifying the most effective countermeasures requires constant dedication and high levels of expertise. With petabytes of rich threat data to mine, advanced machine-learning technologies and a unique pool of world experts, we work to support our customers with the latest threat intelligence from around the world, helping them maintain immunity to even previously unseen cyberattacks.

Key benefits

Enables global threat visibility, timely detection of cyberthreats, prioritization of security alerts and an effective response to information security incidents

The unique insights into the tactics, techniques and procedures used by threat actors across different industries and regions enable proactive protection against targeted and complex threats

A comprehensive overview of your security posture with actionable recommendations on mitigation strategies enables you to focus your defensive strategy on areas identified as prime cyberattack targets

Prevents analyst burnout and helps focus your workforce on genuine threats

Improved and accelerated incident response and threat hunting capabilities help to reduce attack 'dwell time' and significantly minimize possible damage

Kaspersky Threat Intelligence

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture