Stay ahead of your adversaries

Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

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.

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

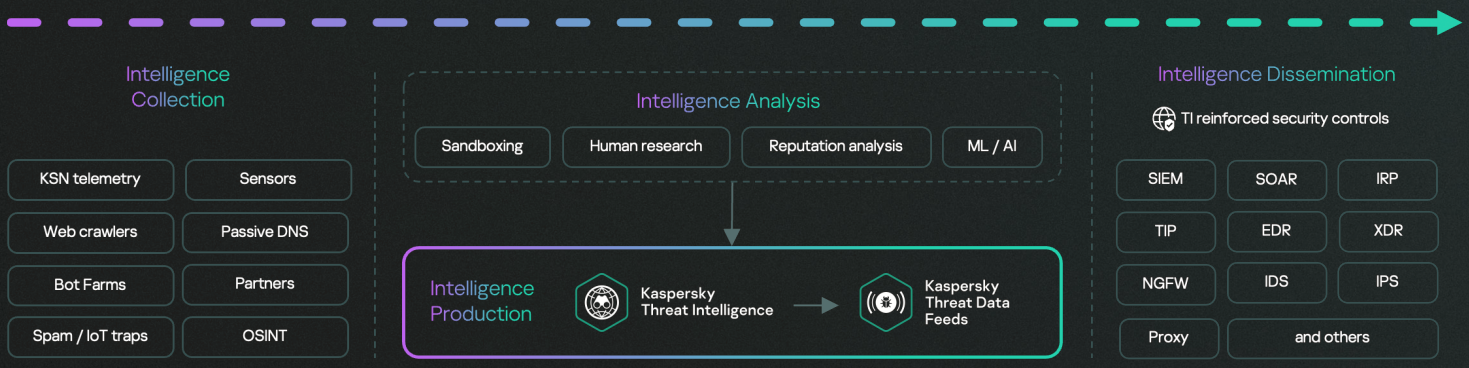
Kaspersky's team of experts are among the most experienced and respected researchers in the industry, bringing a wealth of knowledge and expertise to your Information Security teams.

Kaspersky Threat Data Feeds

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.



Contextual data

Every record in each Data Feed is enriched with actionable context (threat names, timestamps, geolocation, resolved IP 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. Put in context, the data can more readily be used to answer the 'who, what, where, when' questions to identify your adversaries, help you make quick decisions and act.

How it works

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.

Entries in feeds provided by Kaspersky contain contextual data that help you to quickly confirm and prioritize threats:

- Threat names
- IP addresses and domain names of malicious web resources
- Hashes of malicious files
- Vulnerable and compromised objects
- Tactics, techniques and procedures of attacks according to MITRE ATT&CK classification
- Timestamps
- Geolocation
- 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

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.

Instruments

Kaspersky CyberTrace provides a set of instruments to effectively operationalize threat intelligence:

A database of indicators with full text search and the ability to search using advanced search queries enables complex searches across all indicator fields, including context

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

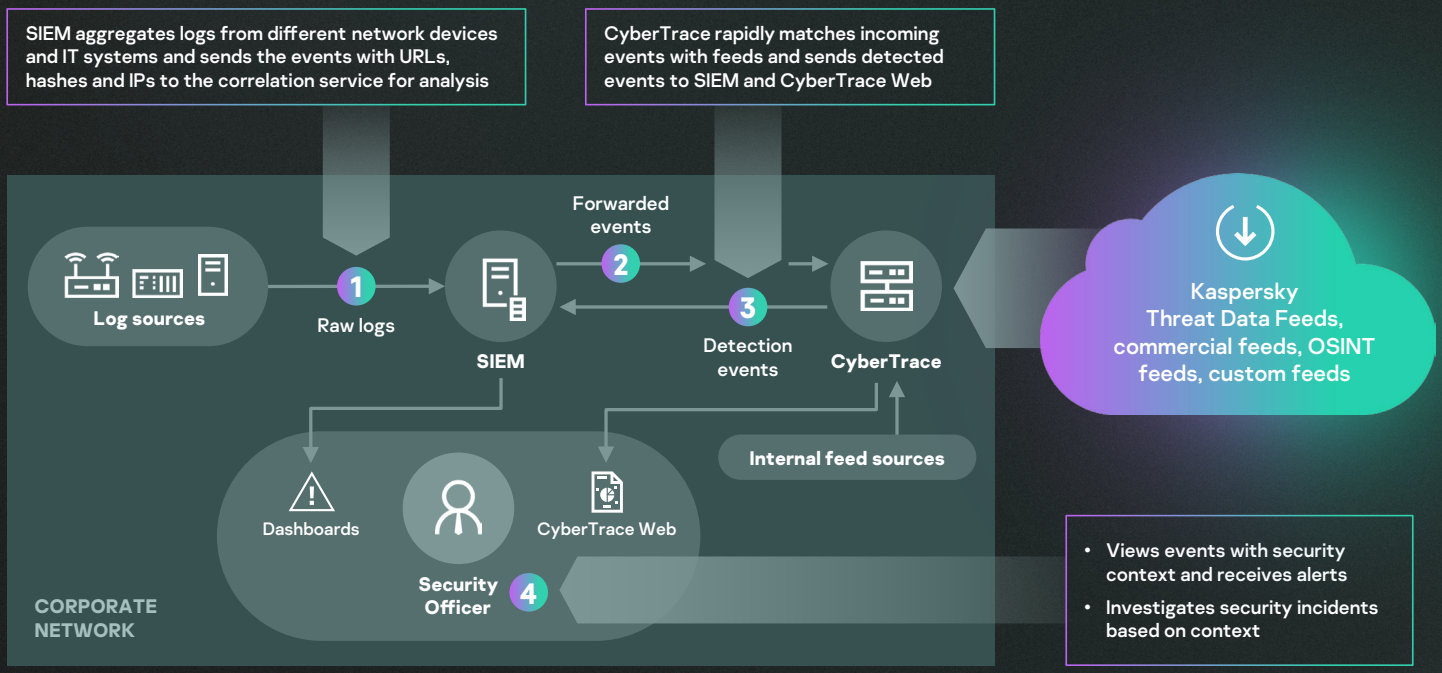
A filter sends detection events to SIEM solutions, reducing the load on SIEM as well as analysts

HTTP RestAPI lets you look up and manage threat intelligence

Pages with detailed information about each indicator 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 the indicator

The tool uses an internalized process of parsing and matching incoming data, which significantly reduces the SIEM workload. Kaspersky CyberTrace parses incoming logs and events, rapidly matches the resulting data to feeds, and generates its own threat detection alerts.

Architecture



Kaspersky CyberTrace and Kaspersky Threat Data Feeds enable your security analysts to:

Effectively distill and prioritize huge amounts of security alerts

Improve and accelerate triage and initial response processes

Build a proactive and intelligence-driven defense

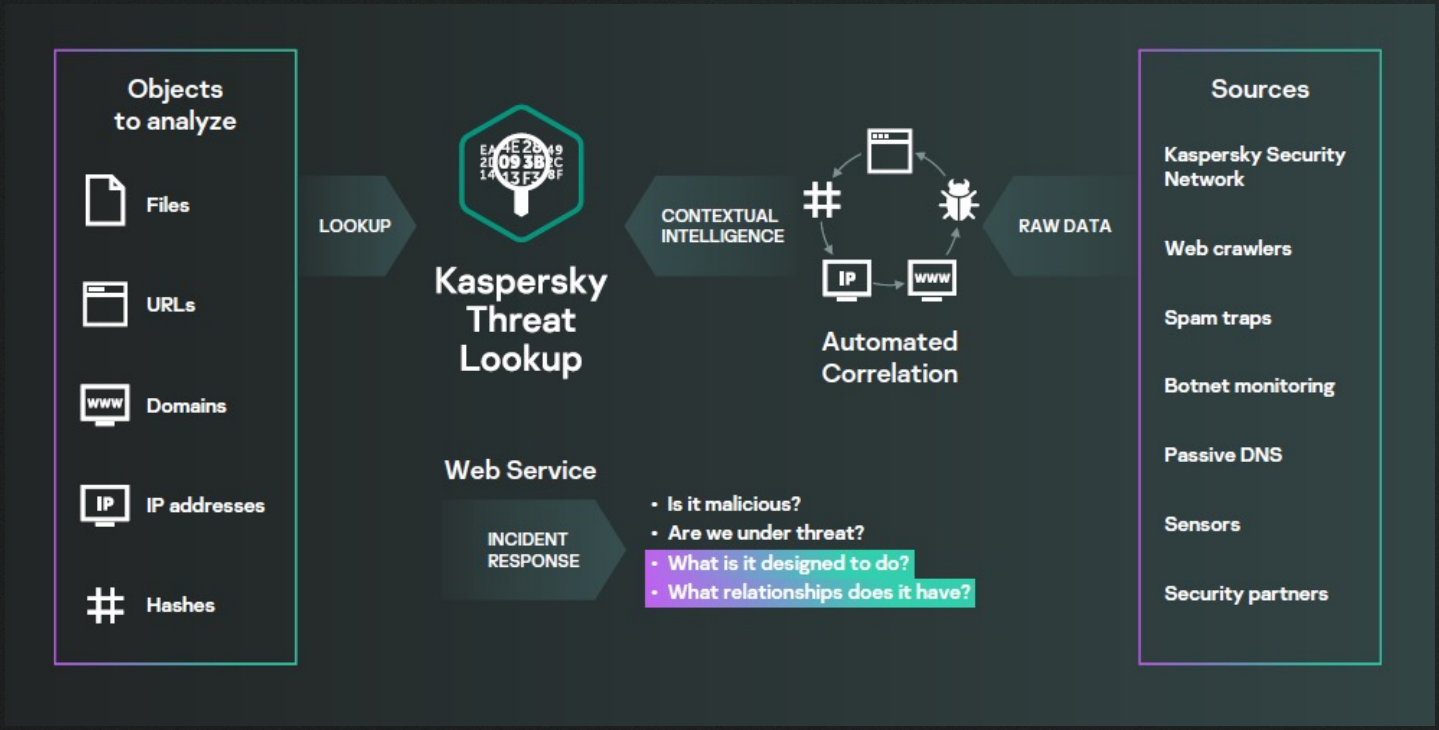
Immediately identify alerts critical for your business and make more informed decisions about which should be escalated to IR teams

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



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

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

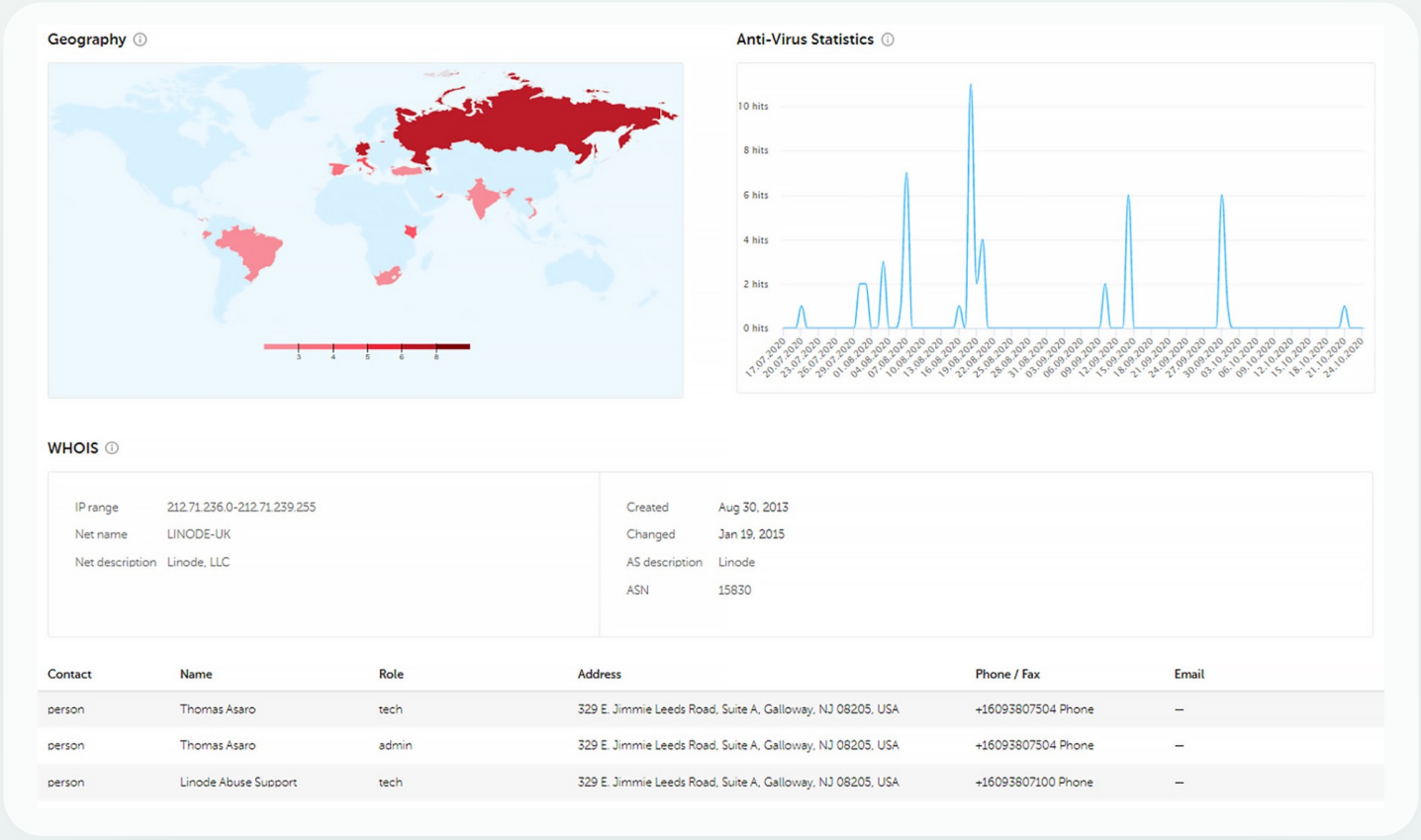
Diagnose and analyze security incidents on hosts and the network more efficiently and prioritize signals from internal systems against unknown threats

Boost your incident response and threat hunting capabilities to disrupt the kill chain before critical systems and data are compromised

Look up threat indicators from a web-based interface or via the RESTful API

Examine advanced details including certificates, commonly used names, file paths, or related URLs to discover new suspicious objects

Check whether the discovered object is widespread or unique and understand why an object should be treated as malicious



Kaspersky Research Sandbox

It's impossible to prevent targeted attacks with traditional AV tools alone. Antivirus engines can only stop known threats and their variations, while sophisticated threat actors use a huge variety of techniques to evade automatic detection. Losses from information security incidents continue to grow, stressing the importance of immediate threat detection capabilities to ensure rapid response and the ability to counter threats before they can cause damage.

Making an intelligent decision based on a file's behavior while simultaneously analyzing the process memory, network activity, etc., is the optimal approach to understanding the latest 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.

Kaspersky Research Sandbox enables you 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 threat intelligence gathered 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.

Proactive threat detection and mitigation

Malware uses a variety of methods to disguise its execution from being detected. If the system does not meet the required parameters, the malicious program will almost certainly destroy itself, leaving no trace. For malicious code to execute, the sandboxing environment must be capable of accurately mimicking normal end-user behavior.

Kaspersky Research Sandbox offers a hybrid approach combining threat intelligence gathered 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.

This service has been developed in our in-house sandboxing lab, evolving for over a decade. The technology incorporates all our knowledge of malware behavior gained over 25 years of continuous threat research. This allows us to detect over 400 000 new malicious objects every day to provide our customers with industry-leading security solutions.

Kaspersky Research Sandbox can be managed from a cloud-based central management platform and from an offline console in air-gapped environments, leveraging threat intelligence and incorporating customizable analysis.

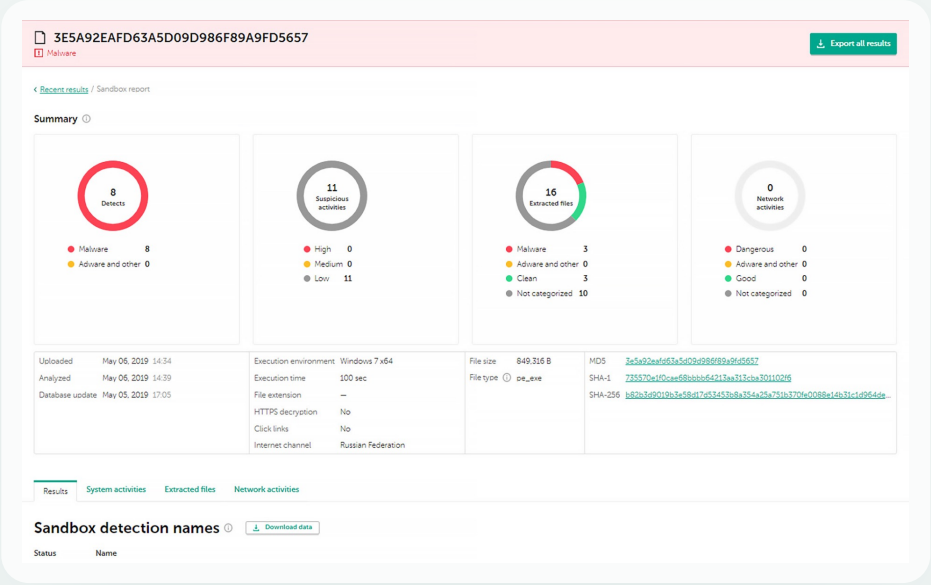
As part of Threat Intelligence Portal, Kaspersky Research Sandbox is the final component in your threat intelligence workflow. While Threat Lookup retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, etc., Research Sandbox links that knowledge with the IOCs generated by the analyzed file.

Comprehensive reporting

- Unified threat score
- Suspicious system activities with detailed descriptions
- Loaded and run DLLs
- Created, modified and deleted files
- Process memory dumps and network traffic dumps (PCAP)
- Created mutual extensions (mutexes)
- Modified and created registry keys
- Processes created by the executed file
- Network activities (SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, SOCKS sessions; HTTP(s), requests and responses)
- Detailed threat intelligence with actionable context for every revealed indicator of compromise (IOC)
- Detailed execution map with highlighted MITRE ATT&CK techniques
- YARA detects and triggered IDS rules (including custom ones)
- Downloading and analyzing a file hosted on certain URL
- Clicking links in documents for Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) and Adobe Reader
- Possibility to export the analysis details in STIX, JSON, CSV formats
- Variety of environments including Mobile OS (Android) and environment customization capabilities
- Custom file execution parameters
- Different Internet channels, the possibility to route traffic via custom VPN channel
- RESTful API
- Screenshots and much more

With Kaspersky Research Sandbox you can run highly effective and complex incident investigations, gaining an immediate understanding of the nature of the threat and 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 Research Sandbox boosts your incident response and forensic activities, providing you with the scalability for processing files automatically without having to buy expensive appliances or worrying about system resources.



Kaspersky Threat Attribution Engine

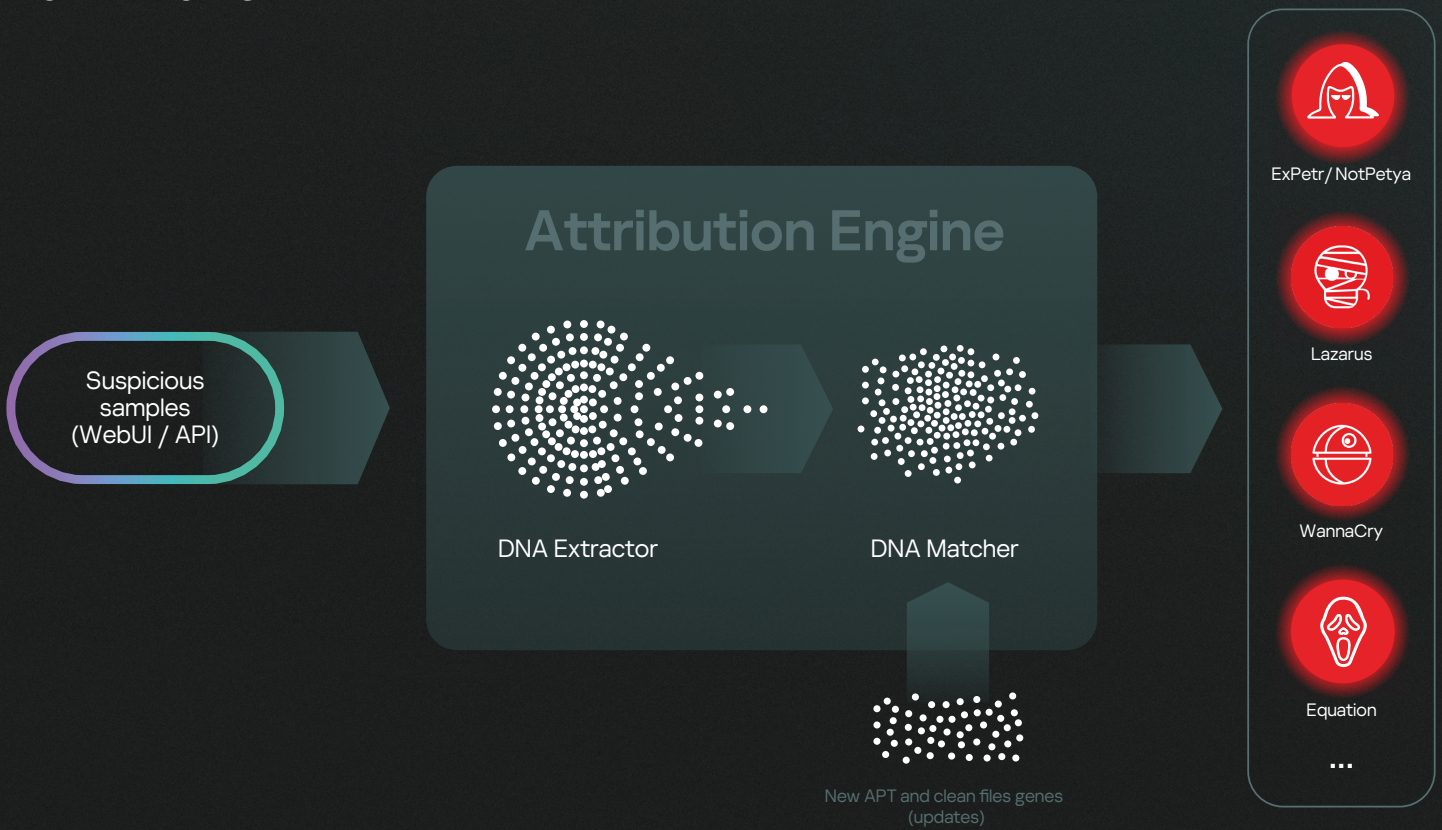
There's a good reason why threat attribution plays such a significant role in cybersecurity. The average time lag between detecting and responding to highly sophisticated threats can be frustratingly protracted, due to the complex investigation and reverse engineering processes involved. In many cases, this delay can give attackers enough time to reach their goals. Correct and timely attribution helps not only to shorten incident response times from hours to minutes, but also to reduce the number of false positives.

Identifying a targeted attack, profiling the attackers and creating attribution factors for the different threat actors is a long and complex job, which can take years. Creating a working attribution also requires a large amount of data accumulated over time, as well as a highly-skilled team of researchers with the relevant investigation experience. These researchers will commonly follow the activity of different groups, and populate a database with all the pieces of information accrued. This database then becomes a valuable resource that can be shared as a tool.

Kaspersky Threat Attribution Engine incorporates a database comprising APT malware samples and clean files gathered by Kaspersky experts over the last 25 years and more. We track 1100+ threat actors and campaigns and release 120+ threat intelligence reports a year. Our ongoing research supports an APT collection which contains some 83,000 files. This improves false flag detection and, in conjunction with the use of automated tools, results in outstandingly accurate levels 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.

How it works



To link malware to attribution entities, Kaspersky Threat Attribution Engine uses a unique proprietary method of searching for similarities 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.

The product can be deployed in secure, air-gapped environments, restricting any 3rd party from accessing the processed information and submitted objects. An API connects the Engine to other tools and frameworks in order to implement attribution into existing infrastructure and automated processes.

Product highlights

- Provides instant access to a repository of curated data about thousands of APT actors, samples and broader threats (via the anti-virus engine)
- Enables efficient automated or manual threat prioritization and alert triage
- Supports adding of private actors and samples, educating the product to detect samples that are similar to files in your private collection
- Allows manual samples uploads, and offers enhanced REST API functionality for integration with automated workflows
- Supports deployment on Amazon Web Services (AWS), enabling quick product setup while also saving costs – no need to invest in hardware upfront
- Easy exports to YARA rules for further automated search/scanning for similar files or integration with third-party solutions
- Easy exports to STIX 2.1 format (TXT and JSON formats are also supported) for further automated analysis of security logs or integration with third-party solutions/security controls
- Allows unpacking of password-protected archives with custom passwords
- Provides quick access to documentation and End User License Agreement (EULA) in the web interface
- Sends attributes in parallel files for analysis in a single request

Kaspersky Threat Attribution Engine benefits

Kaspersky Threat Attribution Engine calculates the reputation score

of the sample and reveals its genetics and code attribution. This provides insights into the origin of the sample and can enable its attribution to possible authors.

Your security team can add your own private attribution entities

and related samples to the Kaspersky Threat Attribution Engine database. The team can then educate the application to attribute submitted samples to these private attribution entities and samples.

The attribution process takes only seconds

With Kaspersky Threat Attribution Engine, the attribution process takes only seconds, compared to the months and years required in the past.

Kaspersky Threat Attribution Engine extends and strengthens

the Kaspersky portfolio for commercial Security Operations Centers (SOCs) and national cybersecurity agencies by supporting them in establishing an effective incident management process.

Kaspersky APT Intelligence Reporting

Kaspersky APT Intelligence Reporting customers receive unique ongoing access to our investigations and discoveries, including full technical data (in a range of formats) on every APT as it's discovered, as well as on threats that will never be made public. Reports contain an executive summary offering C-level oriented and easy to understand information describing the related APT together with a detailed technical description of the APT with related IOCs and YARA rules to give security researchers, malware analysts, security engineers, network security analysts and APT researchers actionable data that enables a fast, accurate response to the threat.

Our experts will alert you immediately to any changes they detect in the tactics of cybercriminal groups. You will also have access to Kaspersky's complete APT reports database, another powerful research and analysis component in your security defenses.

300+
threat actors

160+
private reports a year

12 000+
IoCs

400+
campaigns

700+
Yara rules

Kaspersky APT Intelligence Reporting provides

Threat actor profiles

Mapping to MITRE ATT&CK

Executive summary

C-level oriented information

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

Conclusions and recommendations

Indicators of Compromise (IOCs) and YARA rules

Kaspersky APT Intelligence Reporting benefits

Information about non-public APTs

For various reasons, not all high-profile threats are made known to the general public — but we'll share them with you

Privileged access

Receive technical descriptions about the latest threats during ongoing investigations, before release to the general public

Retrospective analysis

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

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 rules

Intel on 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

Seamless integration and automation

Seamless integration and automation of your security workflows with RESTful API

Continuous APT campaign monitoring

Get access to actionable intelligence during investigations with information on APT distribution, IOCs, command and control infrastructures, etc.

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

Kaspersky Crimeware Intelligence Reporting

Financially-motivated cybercrime is not limited to specific industries. And while attacks on financial infrastructures like ATMs and PoS (Point of Sale) devices continue, all enterprises in every sector are at risk from ransomware. Over the last couple of years, there has been a blurring of boundaries between different types of threats and different types of threat actors. This includes the emergence of advanced persistent threat (APT) campaigns focused not on cyberespionage, but on theft – stealing money to finance other activities that the ATP group is involved in. The growing sophistication of crimeware threats should not be underestimated.

Kaspersky Crimeware Intelligence Reporting boosts your defensive strategies with timely information on malware campaigns, attacks targeting financial institutions and information on crimeware tools used to attack banks, payment processing companies and their specific infrastructures.

Kaspersky Crimeware Intelligence Reporting delivers

- Detailed descriptions of popular, widespread and highly-publicized hyped malware
- Researcher notes/early warnings, including information on new and updated malware threats
- Information on dangerous, widespread malware campaigns
- Detailed descriptions of threats targeting financial infrastructures and the corresponding attack tools being developed or sold by cybercriminals on the Dark Web in various geographies

Kaspersky Crimeware Intelligence Reporting benefits

Privileged access

Receive technical descriptions about the latest threats during ongoing investigations, before release to the general public

Retrospective analysis

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

Seamless integration and automation

Seamless integration and automation of your security workflows with RESTful API

Access to technical data

including an extended list of IOCs, available in standard formats including openIOC or STIX, as well asaccess to our YARA rules

Intel on crimeware 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

Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat 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 are delivered via Kaspersky Threat Intelligence Portal, which means you can start using the service immediately.

All ICS-related threat intelligence research is conducted by a dedicated team — Kaspersky ICS CERT:

- Established in 2016
- The first CERT team created by a commercial organization
- Around 20 highly qualified experts in ICS threat and vulnerability research, incident response and security analysis

Reports included in your subscription

APT reports

Reports on new APT and high-volume attack campaigns targeting industrial organizations, and updates on active threats

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

Vulnerability analysis and mitigation

Our advisories provide actionable recommendations from Kaspersky experts to help identify and mitigate vulnerabilities in your infrastructure

Evolution of the 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

Threat intelligence data empowers you to

Detect and prevent

Reported threats to safeguard critical assets, including software and hardware components and ensure the safety and continuity of technological process

Assess vulnerabilities

Assessment of your industrial environments and assets based on accurate assessments of the scope and severity of a vulnerability, to make informed decisions on patch management and implement other preventative measures recommended by Kaspersky

Correlate

Any malicious and suspicious activity you detect in industrial environments with Kaspersky's research results to attribute your detection to the malicious campaign in question, identify threats and promptly respond to incidents

Leverage information

On attack technologies, tactics and procedures, recently discovered vulnerabilities and other important threat landscape changes to:

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

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

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).

Brand protection

Monitoring and blocking unauthorized use of a company's brand online. Identification of fake social media accounts and applications, phishing websites, and other fraudulent activities that can damage a company's reputation and/or deceive customers. Takedown of fake social networks accounts and fake applications in mobile marketplaces.

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.

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 perimeter inventory

Surface, deep and dark web

Kaspersky Knowledge Base

Analytical reports

Threat alerts

10 takedown requests a year

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

How it works

Configure	Collect	Filter	React
Information discovery about the company's digital assets	Automated data collection from surface, deep and dark webs, and the Kaspersky threat intelligence database	Threat detection, analysis and prioritization managed by analysts	Delivery of completed intelligence

Business values

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

Protect your brand

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.

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

Integration with Kaspersky Digital Footprint Intelligence

Kaspersky Takedown Service can be purchased separately, but its integration with Kaspersky Digital Footprint Intelligence makes the most of the natural synergy between these services. Kaspersky Digital Footprint Intelligence provides real-time notifications about phishing and malware domains which can be immediately submitted to Kaspersky Takedown Service for further blocking.

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.

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

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