

# Kaspersky Threat Intelligence

## The challenge

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.

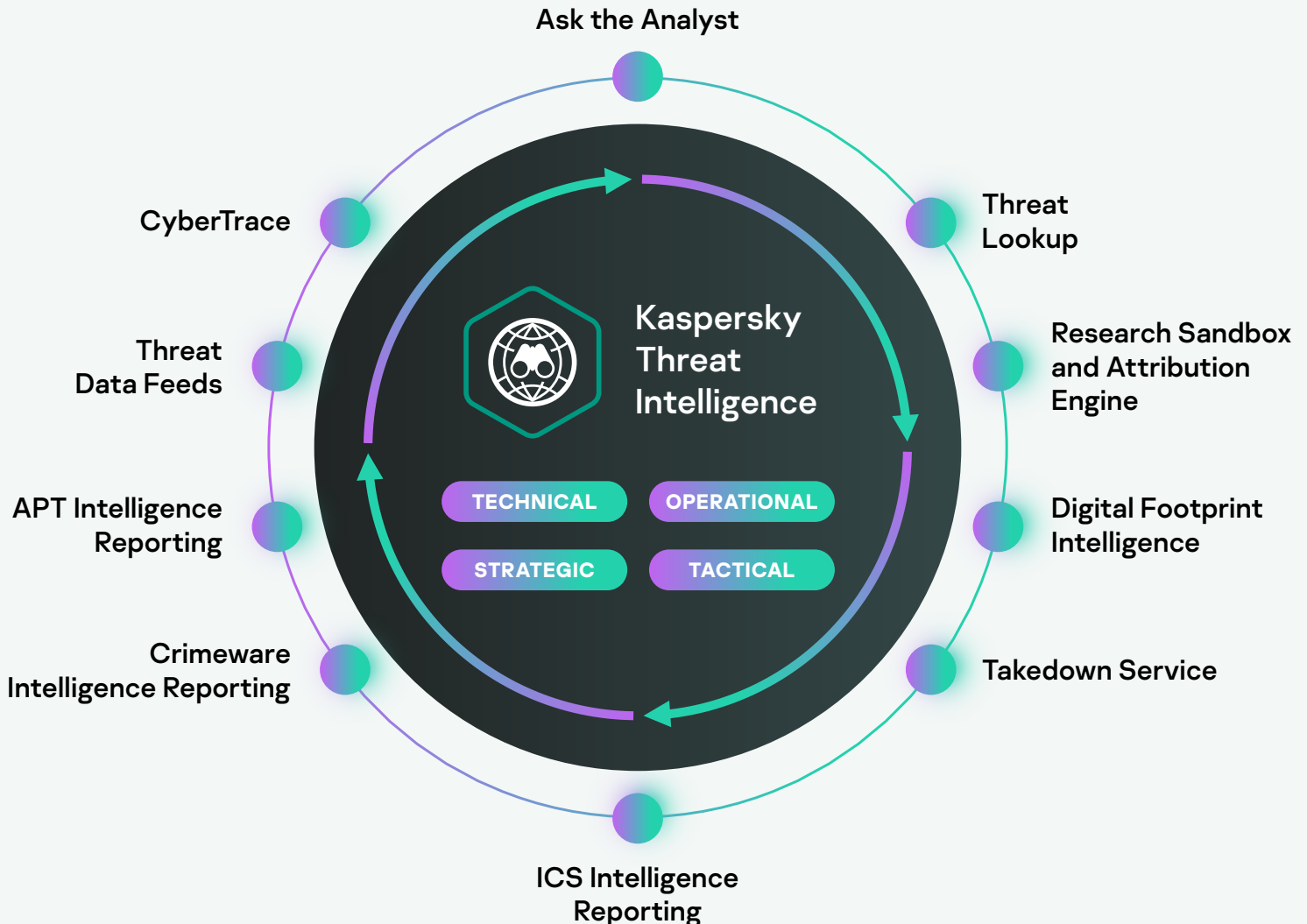
# Kaspersky Threat Intelligence

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 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. Kaspersky Threat Intelligence gives you instant access to technical, tactical, operational and strategic Threat Intelligence.

## The Kaspersky Threat Intelligence portfolio includes

Threat Data Feeds, CyberTrace (a Threat Intelligence platform), Threat Lookup, Cloud Research Sandbox, and a range of Threat Intelligence Reporting options





# 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. It's 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 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.

## IP REPUTATION FEED

HASH FEED (WIN / \*nix / MacOS / AndroidOS / iOS)

## ICS HASH FEED

INDUSTRIAL VULNERABILITY FEED IN OVAL

URL FEEDS (Malicious, Phishing and C&C)

## RANSOMWARE URL FEED

## APT IOC FEEDS

## CRIMEWARE FEEDS

## VULNERABILITY FEED

## PASSIVE DNS (pDNS) FEED

## IoT URL FEED

## SURICATA RULES

## TRANSFORMS FOR MALTEGO

## CLOUD ACCESS SECURITY BROKER (CASB) FEED

## OPEN SOURCE SOFTWARE THREATS

## REGION-SPECIFIC FEEDS

## AND MORE



## Kaspersky Threat Data Feeds



## 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. Set in context, the data can more readily be used to answer the 'who, what, where, when' questions to identify your adversaries, and help you make quick decisions and take action.

## Highlights

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

Ease of implementation. Supplementary documentation, samples, a dedicated technical account manager and technical support from Kaspersky all combine to enable straightforward integration

Hundreds of experts, including security analysts from across the globe, world-renowned security experts from GReAT and 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

## 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, similarity tools, behavior profiling, analyst validation and allowlisting verification.

Simple lightweight dissemination formats (JSON, CSV, OpenIOC, STIX) via HTTPS, TAXII or ad-hoc delivery mechanisms support easy integration of feeds into security solutions

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

All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability

## 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 to deliver insights into cyberattacks and provide a greater understanding of the intent, capabilities and targets of your adversaries. Leading SIEMs (including HP ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) and TI Platforms are fully supported

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

Prevent the exfiltration of sensitive assets and intellectual property from infected machines to outside the organization. Detect infected assets fast to protect your brand reputation, maintain your competitive advantage and secure business opportunities

As an MSSP, grow your 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

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. 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.

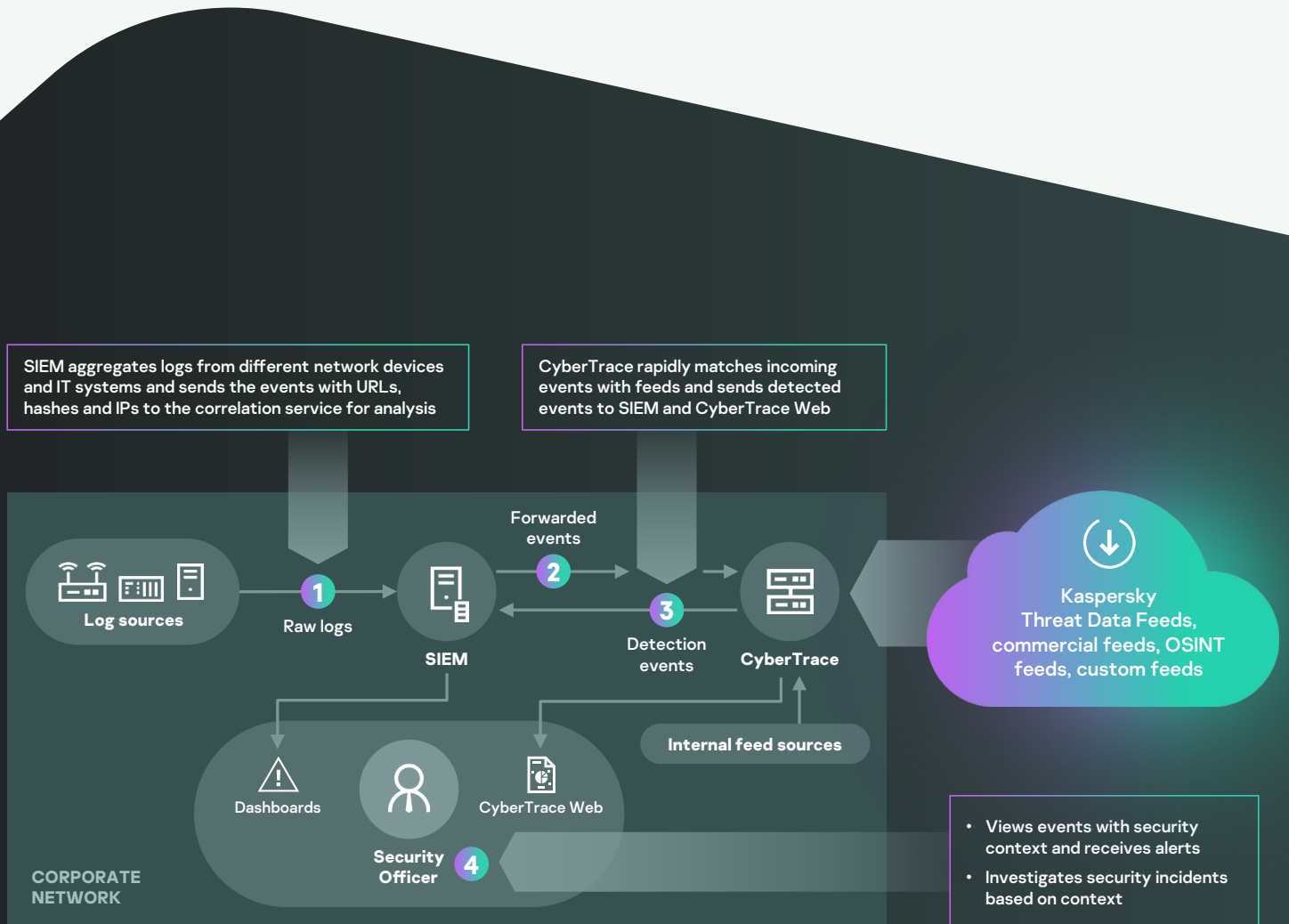
Kaspersky CyberTrace is a threat intelligence platform enabling seamless integration of threat data feeds with SIEM solutions to help analysts leverage threat intelligence in their existing security operations workflow more effectively. It integrates with any threat intelligence feed (from Kaspersky, 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.

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 fields
- 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
- A Research Graph allows to visually explore data and detections stored in CyberTrace and discover threat commonalities
- The indicators export feature allows exporting of indicator sets to security controls such as policies lists (block lists) as well as sharing of threat data between Kaspersky CyberTrace instances or with other TI platforms
- Tagging IoCs simplifies their management. You can 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
- The historical correlation feature (retroscan) lets you analyze observables from previously checked events using the latest feeds to find previously uncovered threats
- A filter sends detection events to SIEM solutions, reducing the load on them as well as on analysts
- Multitenancy supports MSSPs and large enterprise use cases
- Feed usage statistics for measuring the effectiveness of the integrated feeds and feeds intersection matrix help choose the most valuable threat intelligence suppliers
- HTTP RestAPI allows you to look up and manage threat intelligence



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 diagram below:



With Kaspersky CyberTrace and Kaspersky Threat Data Feeds, security analysts are able to:

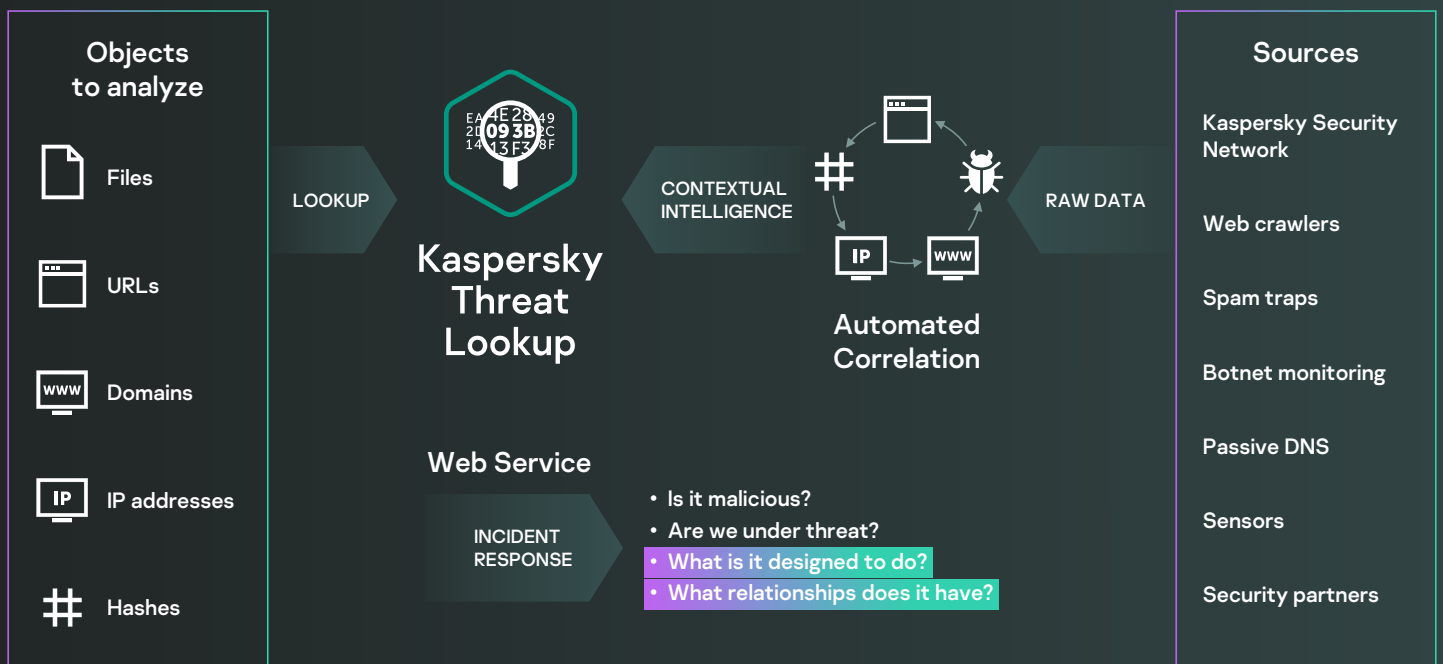
- Effectively distill and prioritize huge amounts of security alerts
- Improve and accelerate triage and initial response processes
- Immediately identify alerts critical for the enterprise and make more informed decisions about which should be escalated to IR teams
- Build a proactive and intelligence-driven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




# 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 a 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.




## 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<sup>1</sup>, 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




**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 reap the full benefits of threat intelligence, automate operations workflow, or integrate with 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


## 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

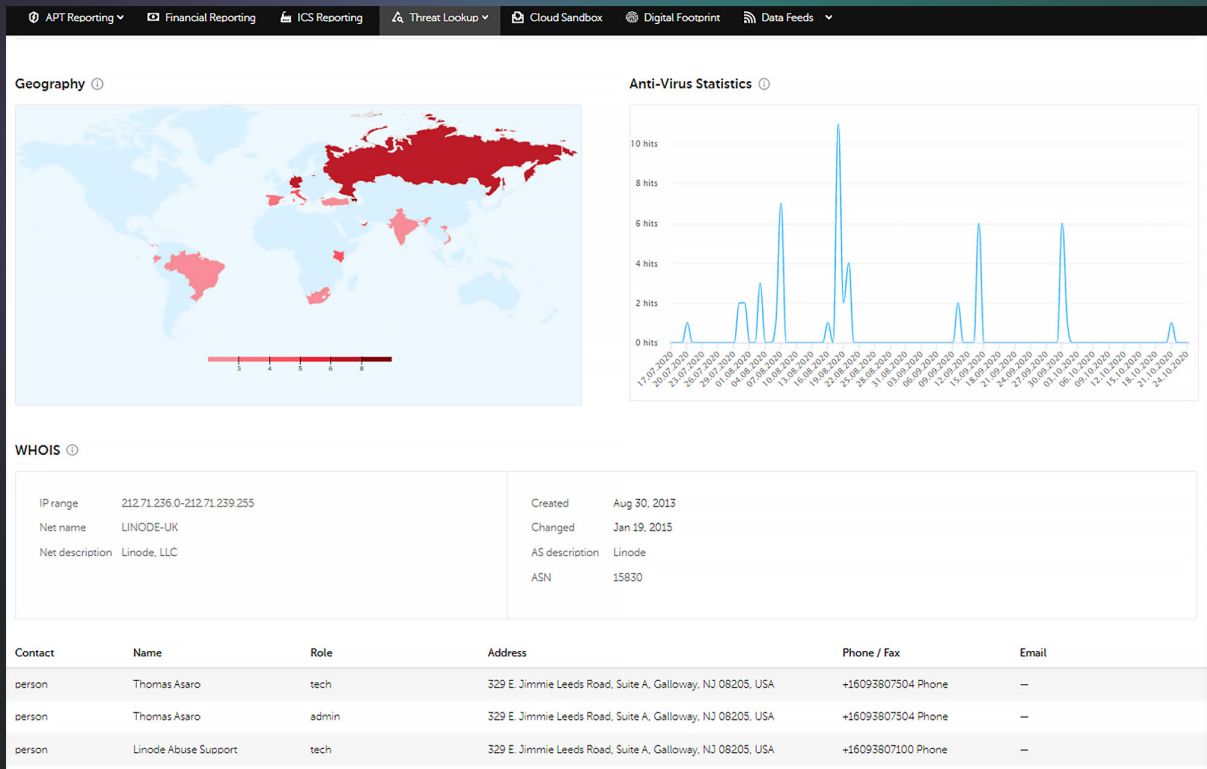


Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats



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





## Now you can

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

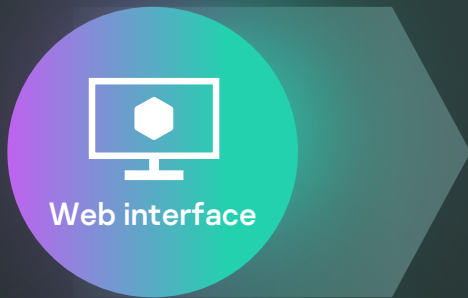
Understand why an object should be treated as malicious



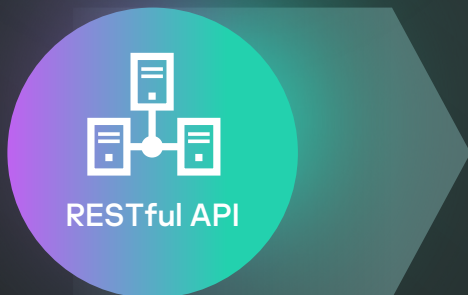
# Kaspersky Cloud Research Sandbox

It's impossible to prevent today's targeted attacks just 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 threats before any significant damage is done.

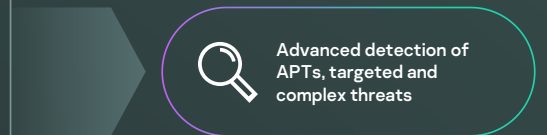
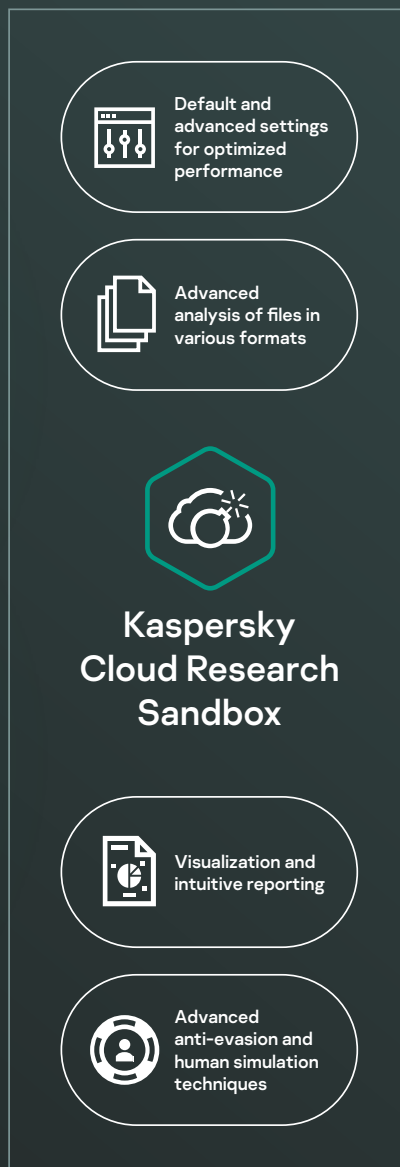
Making an intelligent decision based on a file's behavior while simultaneously analyzing the process memory, network activity, etc., is the optimal approach to understanding the latest sophisticated targeted and tailored threats. While statistical data may lack information on recently modified malware,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



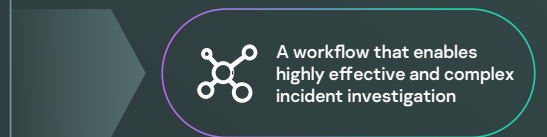
Web interface



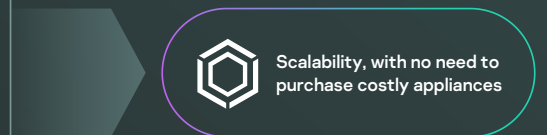
RESTful API



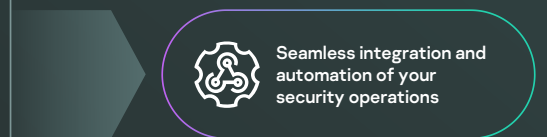
Advanced detection of APTs, targeted and complex threats



A workflow that enables highly effective and complex incident investigation



Scalability, with no need to purchase costly appliances



Seamless integration and automation of your security operations

## Comprehensive reporting

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

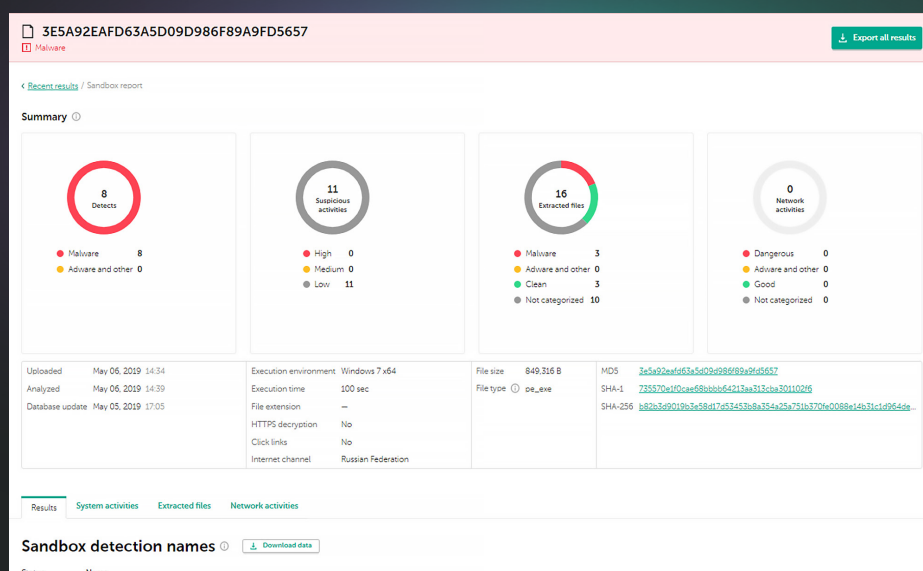
## Proactive threat detection and mitigation

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 the malicious code to execute, the sandboxing environment must be capable of accurately mimicking normal end-user behavior.

Kaspersky Cloud Research 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.

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 20 years of continuous threat research. This allows us to detect over 360 000 new malicious objects every day to provide our customers with industry-leading security solutions.

As part of Threat Intelligence Portal, Cloud 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., Cloud Research Sandbox links that knowledge with 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 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 Cloud 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 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 also 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.

## Benefits

### MITRE ATT&CK

All TTPs described in the reports are mapped to the 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

### Information about non-public APTs

For various reasons, not all high profile threats are made known to the general public. But we share them all with our customers

### 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, and access to our YARA 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

### Continuous APT campaign monitoring

Access to actionable intelligence during investigation with (information on APT distribution, IOCs, command and control infrastructures, etc.

### RESTful API

Seamless integration and automation of your security workflows

## Evolving threats

The world of crimeware threats is constantly evolving. Crimeware refers to malicious programs specifically designed to commit financially-motivated cybercrime. The most infamous example is ransomware – programs which block access to data or disrupt a computer's performance. There are no limits to the imagination of cybercriminals who are coming up with ever-more sophisticated ways to gain and monetize their access to their target's systems, accounts and data.

# 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. We should not underestimate the growing sophistication of crimeware threats.

Kaspersky Crimeware Intelligence Reporting enables organizations to inform their defensive strategies by providing 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.

## The service delivers:



Detailed descriptions of popular, widespread and highly-publicized hyped malware



Information on dangerous, widespread malware campaigns



Researcher notes/early warnings, including information on new and updated malware threats



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

## Service benefits



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



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, and access to our YARA rules



RESTful API. Seamless integration and automation of your security workflows



# 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 by 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 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 their defenses accordingly, Kaspersky has created Kaspersky Digital Footprint Intelligence.

What's the best way to launch an attack against your organization? What is the most cost-efficient way to attack you? What information is available to an attacker targeting your business? Has your infrastructure already been compromised without your knowledge?

Kaspersky Digital Footprint Intelligence answers these and other questions as our experts piece together a comprehensive picture of your attack status, identifying weak spots ripe for exploitation and revealing evidence of past, present and even 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 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).
- Identification, monitoring and analysis of any active targeted attacks or attacks that are being 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.
- Brand protection functionality with alert types: Targeted Phishing, Social Network and Mobile Marketplace monitoring.



## Highlights

Kaspersky Digital Footprint Intelligence uses OSINT techniques combined with automated and manual analysis of the Surface, Deep and Dark Web, plus the internal Kaspersky knowledge base to provide actionable insights and recommendations.

The product is available on the Kaspersky Threat Intelligence Portal. You can purchase four quarterly reports with annual real-time threat alerts or purchase a single report with alerts active for six months.

Search the Surface and Dark Web for near real-time information on global security events that are threatening your assets as well as for exposed sensitive data on restricted underground communities and forums. Annual license includes 50 searches a day across external sources and Kaspersky's knowledge base.

Kaspersky Digital Footprint Intelligence forms a single solution with the Kaspersky Takedown Service. Annual license includes 10 requests for taking down malicious and phishing domains a year.

### Network perimeter inventory (including cloud)

- Available services
- Service fingerprinting
- Identification of vulnerabilities
- Exploit analysis
- Scoring and risk analysis

### Surface, deep and dark web

- Cybercriminal activity
- Data and credential leaks
- Insiders
- Employees on social media
- Metadata leaks

### Kaspersky knowledge base

- Analysis of malware samples
- Botnet and phishing tracking
- Sinkhole and malware servers
- APT Intelligence Reporting
- Threat Data Feeds

### Your unstructured data

- IP addresses
- Company domains
- Brand names
- Keywords



Network Perimeter Inventory



Surface, Deep and Dark Web



Kaspersky Knowledge Base



Real-time search across Kaspersky's, Surface and Dark Web sources

Analytical reports

10 takedown requests a year

Threat alerts



# 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 a web-based portal, which means you can start using the service immediately.

## Reports included in your subscription

- 1. APT reports.** Reports on new APT and high-volume attack campaigns targeting industrial organizations, and updates on active threats.
- 2. 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.
- 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 actionable recommendations from Kaspersky experts to help identify and mitigate vulnerabilities in your infrastructure.

## 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



### 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



### Perform

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



### 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 infrastructure to ensure the safety of production and the 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 ensure resilience of operations



## 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

## Ask the Analyst Deliverables

(Unified request-based subscription)



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.

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



### APT and Crimeware

Additional information on published reports and ongoing research (on top of APT or Crimeware Intelligence Reporting service)<sup>1</sup>



### Malware Analysis

- Malware sample analysis
- Recommendations on further remediation actions



### 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)



### Dark Web Intelligence<sup>2</sup>

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



### 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

<sup>1</sup> Available to customers with active APT and/or Crimeware Intelligence Reporting only

<sup>2</sup> Already included in the Kaspersky Digital Footprint Intelligence subscription

---

# How it works

## Service benefits



### Augment 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

Kaspersky Ask the Analyst can be purchased separately or on top of 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.

## Service use cases:



Clarify any details in previously published threat intelligence reports



Get additional intelligence for already provided IoCs



Obtain details on vulnerabilities and recommendations on how to protect against their exploitation



Get additional details on the specific Dark Web activities you're interested in



Get an overview malware family report including the malware behavior, its potential impact and details about any related activity Kaspersky has observed



Effectively prioritize alerts/incidents with detailed contextual information and categorization for related IoCs provided via short reports



Request assistance in identifying if detected unusual activity relates to an APT or a crimeware actor



Submit malware files for comprehensive analysis to understand the behavior and functionality of the provided sample(s)

---

## 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 augment your existing capabilities with our unique knowledge and resources.



## Service benefits



### 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.



### End-to-end management

We will manage the entire takedown process and minimize your involvement.



### Complete visibility

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



### Integration with 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

## Challenge

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.

## Solution

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.

## Key benefits

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

Prevents analyst burnout and helps focus your workforce on genuine threats

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

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

# 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 at Kaspersky work to support our customers with the latest threat intelligence from around the world, helping them maintain immunity to even previously unseen cyberattacks.

## FORRESTER®

Kaspersky is positioned as a Leader in Forrester Wave: External Threat Intelligence Services, 2021



**Kaspersky  
Threat  
Intelligence**

[Learn more](#)

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

© 2021 AO Kaspersky Lab.  
Registered trademarks and service marks  
are the property of their respective owners.