Kaspersky Cybersecurity Services

kaspersky

Learn more on kaspersky.com
#bringonthefuture

Cybercrime today knows no borders, and its technical capabilities are improving fast: we're seeing how attacks are becoming increasingly sophisticated. Our mission is to save the world from all types of cyberthreats. To achieve this, and to make using the Internet safe and secure, it's vital to share threat intelligence in real time. Timely access to information is central to maintaining effective protection of data and networks.

Eugene Kaspersky
Chairman and CEO, Kaspersky

Introduction

More cyberthreats are appearing every day, in all their different guises and through many different attack vectors.

There is no single solution that offers comprehensive protection. However, even in our bigdata world, knowing where to look for danger is a large part of being able to combat the latest threats.

As a business manager, it`s your responsibility to protect your organization against today's threats, and to anticipate the dangers that lie ahead in the coming years. This needs more than just smart operational protection against known threats; it demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

At Kaspersky, we understand that it takes long-lasting relationships to bring long-term prosperity to a business.

Kaspersky is a valuable business partner, always available to share its up-to-the-minute intelligence with your team via different channels. Our broad range of delivery methods helps your security operation center (SOC)/IT security team remain fully equipped to protect the organization from any online threat.

Even if your organization does not use Kaspersky products, you can still benefit from Kaspersky Cybersecurity Services.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

Security with a difference

World-leading security intelligence is built into our DNA – helping us deliver the most powerful antimalware protection on the market and influencing everything we do.

We're a technology-driven company – from top to bottom – starting with our CEO, Eugene Kaspersky.

Our Global Research & Analysis Team (GReAT), an elite group of IT security experts, has led the way in uncovering many of the world's most dangerous malware threats and targeted attacks.

Many of the world's most respected security organizations and law enforcement agencies – including INTERPOL and leading CERTs – have actively sought our assistance.

Kaspersky develops and perfects all of its own core technologies in-house, so our products and intelligence are naturally more reliable and efficient.

The most widely respected industry analysts – including Gartner, Forrester Research and International Data Corporation (IDC) – rate us as a Leader within many key IT security categories.

Over 130 OEMs – including Microsoft, Cisco, Blue Coat, Juniper Networks, Alcatel Lucent and more – use our technologies within their own products and services.

Kaspersky Threat Intelligence

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

Kaspersky Cybersecurity Services

Kaspersky Threat Intelligence

Threat Data Feeds
Kaspersky CyberTrace
APT Intelligence Reporting
Tailored Threat Intelligence Reporting
Kaspersky ~~Lookup~~
Kaspersky Cloud Sandbox

Kaspersky Threat Hunting

Kaspersky Cybersecurity Training

Kaspersky Incident Response

Kaspersky Security Assessment

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

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

Kaspersky Threat Intelligence Services include:

- Threat Data Feeds
- CyberTrace
- APT Intelligence Reporting
- Tailored Threat Intelligence Reporting
- Kaspersky ~~Threat Intelligence Portal~~
- Kaspersky Cloud Sandbox

Threat Data Feeds

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

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

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

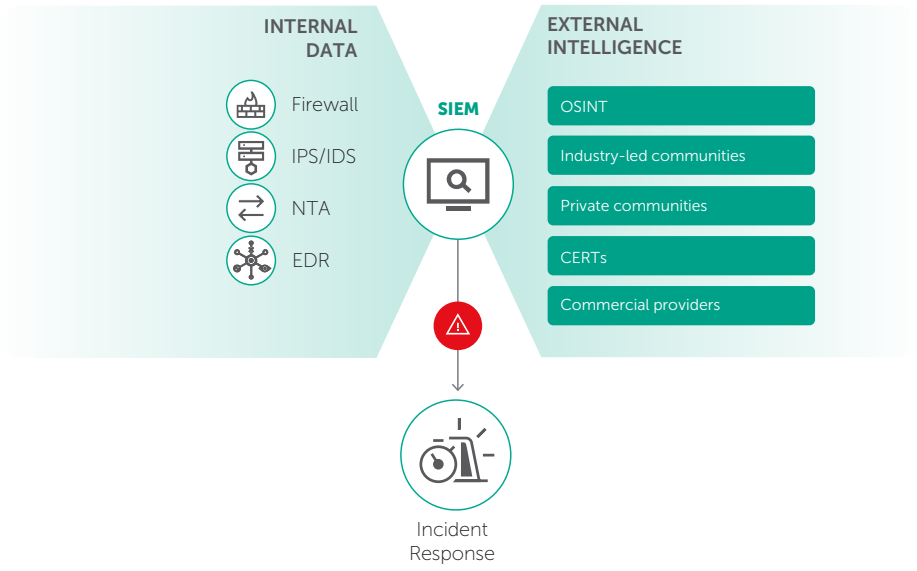


Figure 1. Operationalizing External Threat Intelligence

Contextual Data

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

The Data Feeds

Feeds comprise sets of:

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

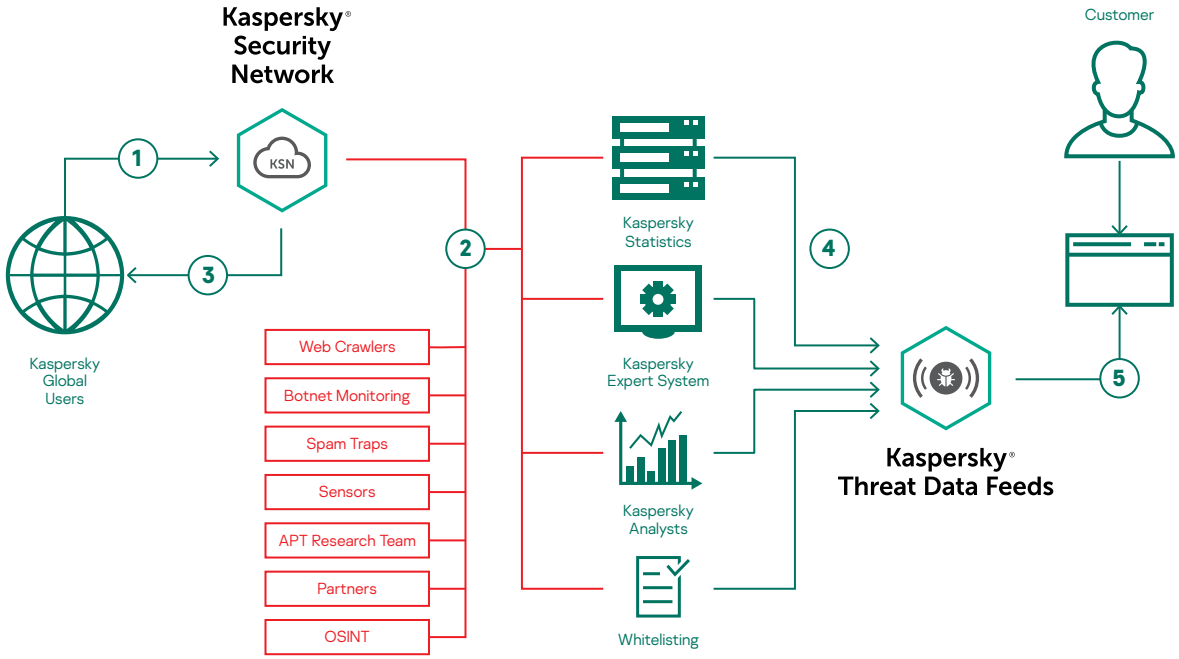


Figure 2. Kaspersky Threat Intelligence Sources

Services Highlights

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

Collection and processing

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

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

Benefits

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

Kaspersky CyberTrace

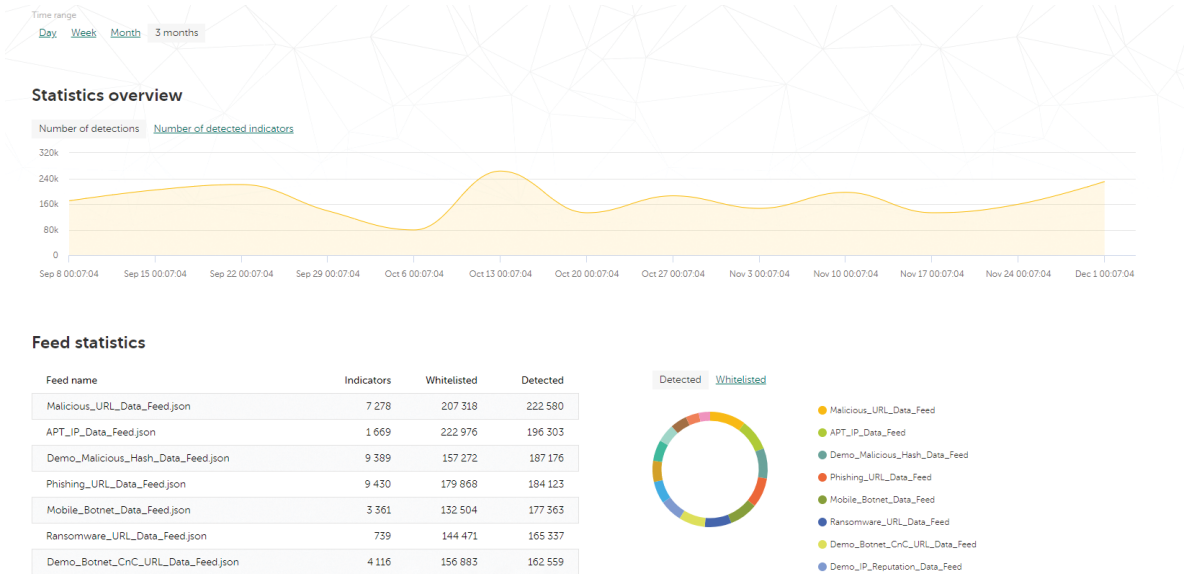
The number of security alerts processed by Security Operations Center's Tier 1 analysts every day is growing exponentially. With this amount of data being analyzed, effective alert prioritization, triage and validation becomes nearly impossible. There are too many blinking lights coming from numerous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

Enabling effective alert triage and analysis

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

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

Figure 3. Kaspersky CyberTrace statistics



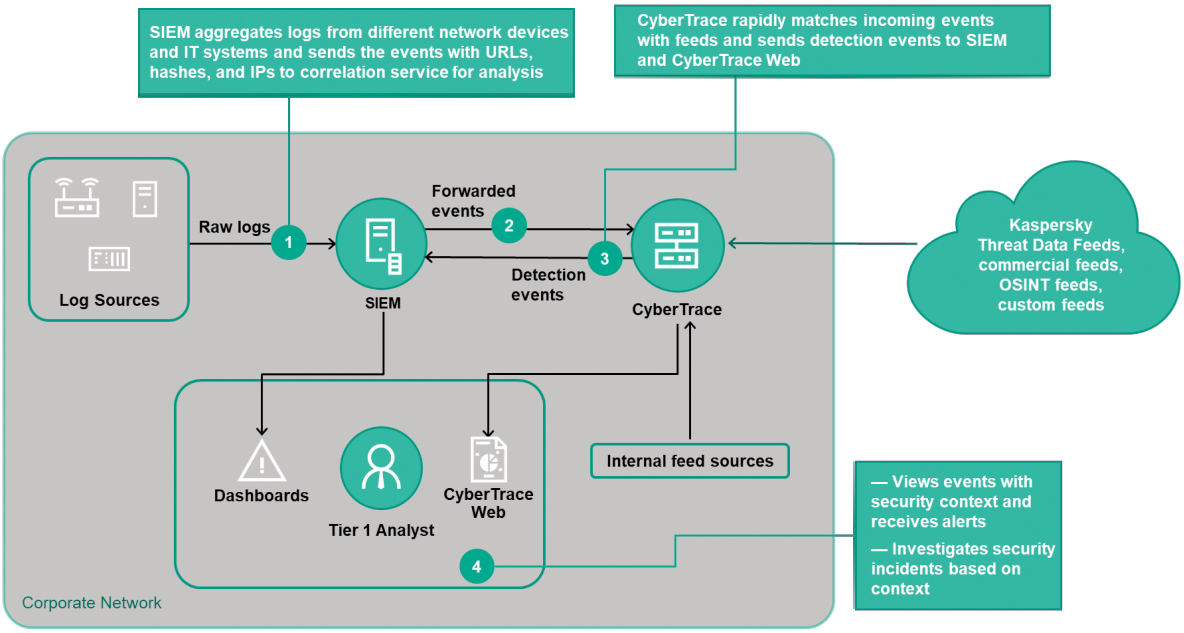
Kaspersky CyberTrace provides a set of instruments to operationalize threat intelligence for conducting effective alert triage and initial response:

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

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

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

Figure 4. Kaspersky CyberTrace integration scheme



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

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

Kaspersky APT Intelligence Reporting provides:

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

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

APT Intelligence Reporting

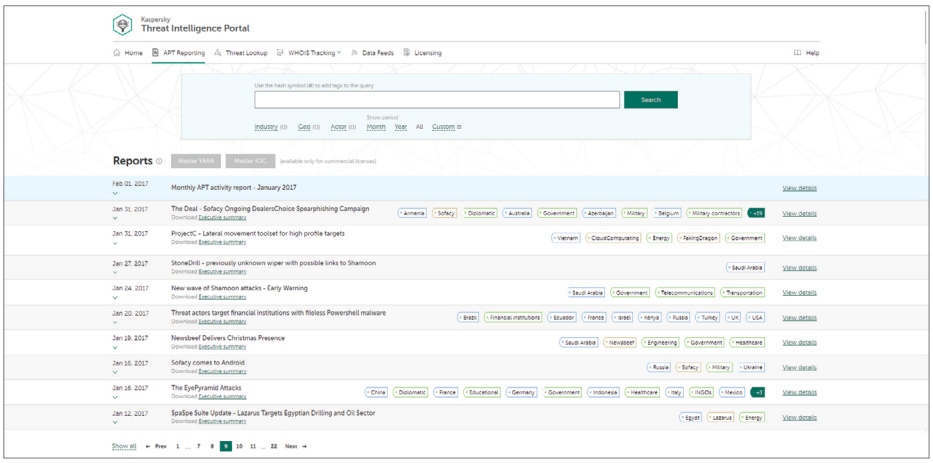
Increase your awareness and knowledge of high profile cyber-espionage campaigns with comprehensive, practical reporting from Kaspersky.

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

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

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

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



Tailored Threat Intelligence Reporting

Customer-specific Threat Intelligence Reporting

What's the best way to mount an attack against your organization? Which routes and what information is available to an attacker specifically targeting you? Has an attack already been mounted, or are you about to come under threat?

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

Empowered by this unique insight, you can focus your defense strategy on areas pinpointed as cybercriminals' prime targets, acting quickly and with precision to repel intruders and minimize the risk of a successful attack.

Developed using open source intelligence (OSINT), deep analysis of Kaspersky's expert systems and databases and our knowledge of underground cybercriminal networks, these reports cover areas including:

- **Identification of threat vectors:** Identification and status analysis of externally available critical components of your network –including ATMs, video surveillance and other systems using mobile technologies, employee social network profiles and personal email accounts – that are potential targets for attack.

- **Malware and cyber-attack tracking analysis:** Identification, monitoring and analysis of any active or inactive malware samples targeting your organization, any past or present botnet activity and any suspicious network based activity.

Third-party attacks: Evidence of threats and botnet activity specifically targeting your customers, partners and subscribers, whose infected systems could then be used to attack you.

Information leakage: through discreet monitoring of underground online forums and communities, we discover whether hackers are discussing attack plans with you in mind or, for example, if an unscrupulous employee is trading information.

Current attack status: APT attacks can continue undetected for many years. If we detect a current attack affecting your infrastructure, we provide advice on effective remediation.

Quick Start – Easy To Use – No Resources Needed

Once parameters and preferred data formats are established, no additional infrastructure is needed to start usingthis Kaspersky service.

Kaspersky Tailored Threat Reporting has no impact on the integrity and availability of resources,including network resources.

The service can be provided as a one-time project or periodically under a subscription (for example, quarterly).

Country-specific Threat Intelligence Reporting

Cybersecurity of a country comprises protection of all its major institutions and organizations. Advanced persistent threats (APT) against government authorities can affect national security; possible cyberattacks against manufacturing, transportation, telecommunication, banking and other pivotal industries potentially can lead to significant damage on the state level, like financial losses, production accidents, blockage of network communications, and popular discontent.

Having an overview of the current attack surface and the current trends in malware and hacker attacks targeting your country, you can focus your defense strategy on areas pinpointed as cybercriminals' prime targets, acting fast and with precision to repel intruders and minimize the risk of successful attacks.

Created using approaches ranging from open source intelligence (OSINT) to deep analysis of Kaspersky's expert systems and databases, and our knowledge of the underground cybercriminal networks, Country-specific Threat reports cover areas including:

- **Identification of threat vectors:** identification and status analysis of externally available critical IT resources of the country – including vulnerable government applications, telecommunication equipment, industrial control systems' components (such as SCADA, PLCs, etc.), ATMs, etc.

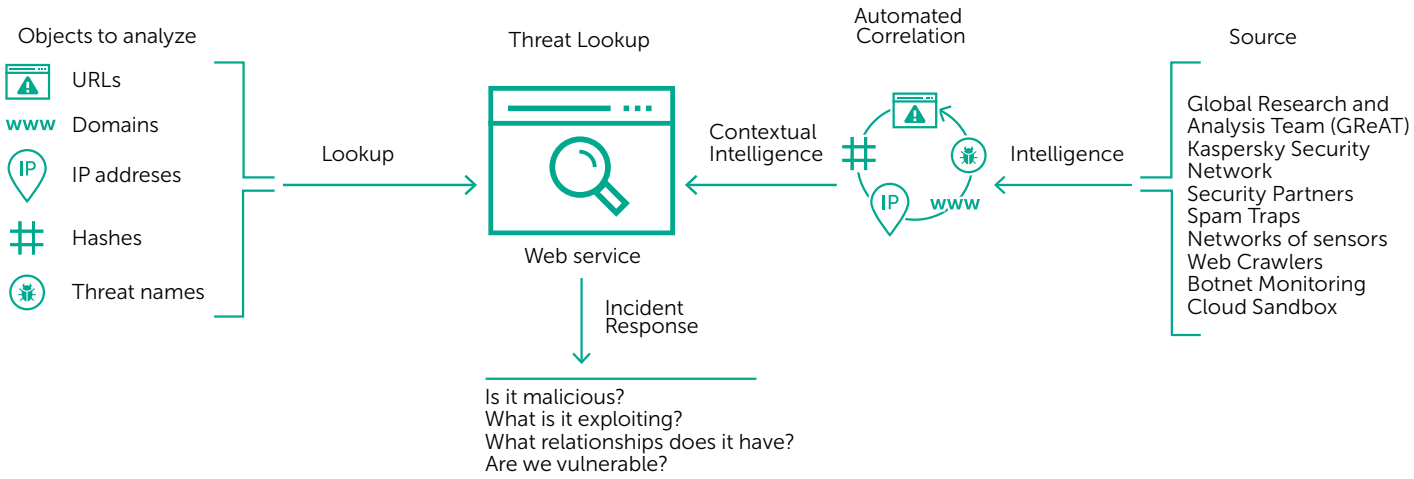
- **Malware and cyber-attack tracking analysis:** identification and analysis of APT campaigns, active or inactive malware samples, past or present botnet activity, and other notable threats targeting your country, based on data available in our unique internal monitoring resources.

- **Information leakages:** through clandestine monitoring of underground forums and online communities, we discover whether hackers are discussing attack plans with certain organizations in mind. We also reveal notable compromised accounts, which could pose risks to suffered organizations and institutions (for instance, accounts belonging to government agencies' employees available in the Ashley Madison breach, which could be used for blackmailing).

Kaspersky Threat Intelligence Reporting has no impact on the integrity and availability of the network resources being inspected. The service is based on non-intrusive network reconnaissance methods, and analysis of information available in open sources and resources of limited access.

As the conclusion of the service you will be provided with a report containing description of notable threats for different state industries and institutions, as well as additional information on detailed technical analysis results. Reports are delivered via encrypted email messages.

Threat Lookup



Service highlights

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

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

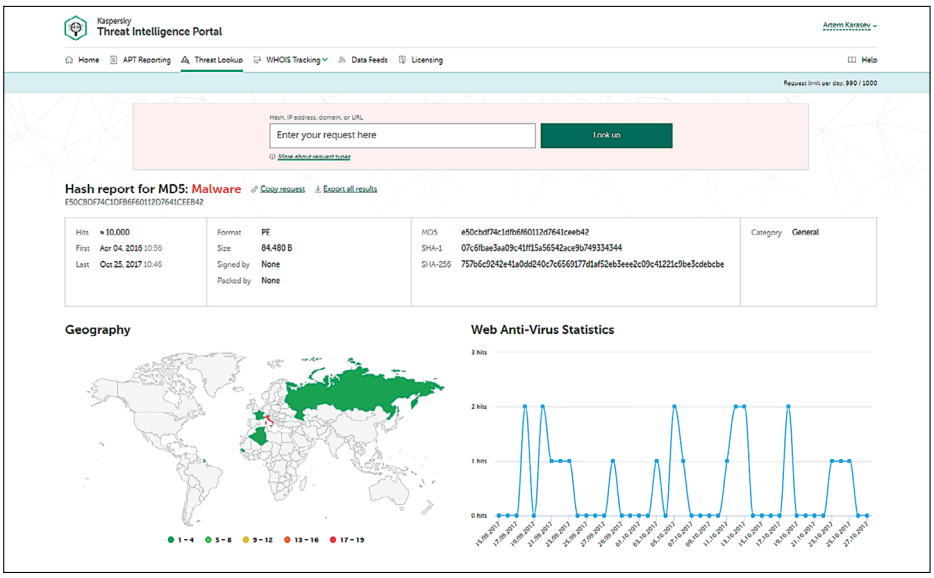
Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky about cyber-threats and their relationships, brought together into a single, powerful web service. The goal is to provide your security teams with as much data as possible, preventing cyber-attacks before they impact your organization.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

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

Key Benefits

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

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



Now You Can

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

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

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

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

Cloud Sandbox

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

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

Key Features:

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

Key Benefits:

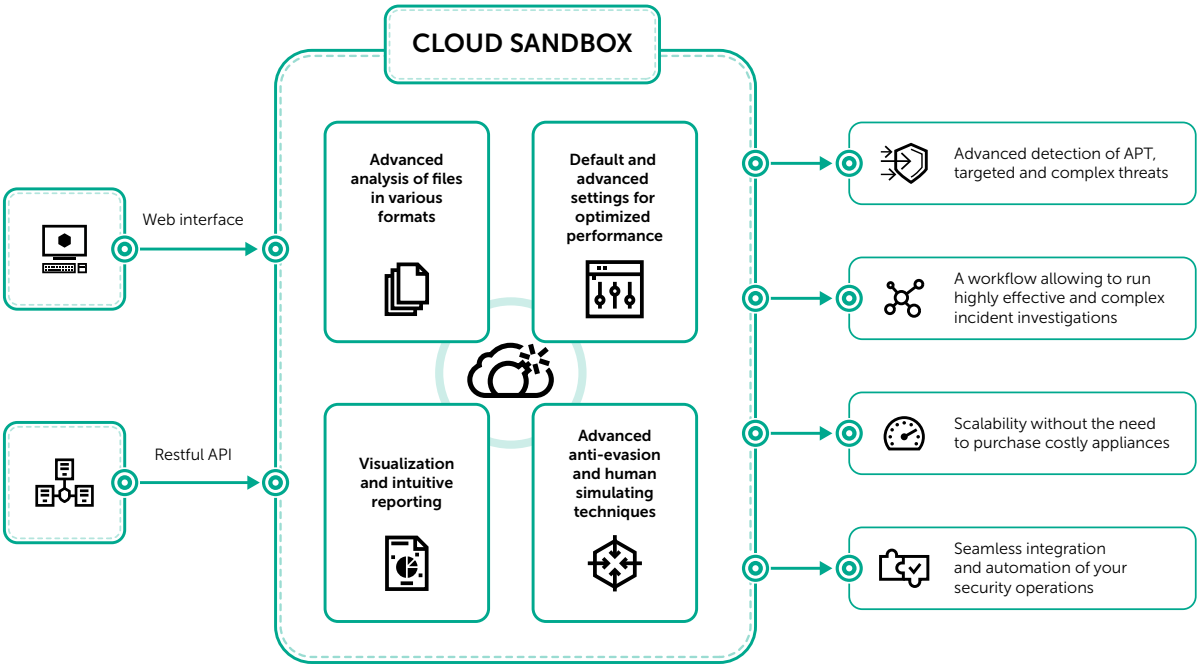
- Advanced detection of APTs, targeted and complex threats
- A workflow allowing the running of highly effective and complex incident investigations
- Scalability without the need to purchase costly appliances or worry about system resources
- Seamless integration and automation of your security operations

Proactive mitigation for threats circumventing your security barriers

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

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

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



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

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

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

Kaspersky Threat Hunting

Security teams across all industries are working hard building systems to provide comprehensive protection against rapidly evolving cyber threats. But most of these take an «alert» driven approach to cybersecurity incidents, reacting only after an incident has already taken place.

According to recent research, a large proportion of security incidents still goes undetected. These threats move in under the radar, giving businesses, quite literally, a false sense of security. As a result, organizations are increasingly recognizing the need to proactively hunt out threats that are lying undiscovered but still active within their infrastructures. Kaspersky Threat Hunting Services help to uncover advanced threats hiding within the organization, using proactive threat hunting techniques carried out by highly qualified and experienced security professionals.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
  - Kaspersky Managed Protection
  - Targeted Attack Discovery
- **Kaspersky Cybersecurity Training**
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

Kaspersky Managed Protection

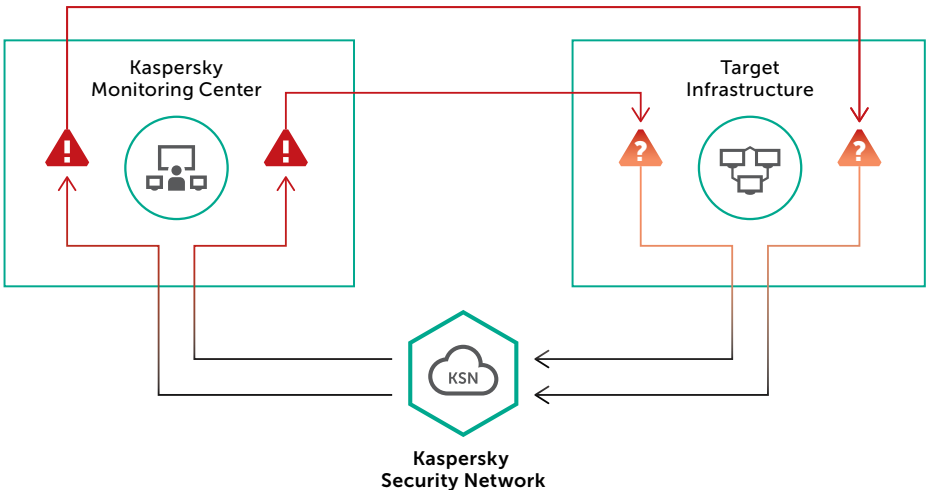
The Kaspersky Managed Protection service offers Kaspersky Endpoint Security and Kaspersky Anti Targeted Attack Platform users a fully managed service, deploying a unique range of advanced technical measures to detect and prevent targeted attacks on your organization. The service includes round-the-clock monitoring by Kaspersky experts and the continuous analysis of cyberthreat data, ensuring the real-time detection of both known and new cyberespionage and cybercriminal campaigns targeting critical information systems.

Service highlights

- A continuously high level of protection against targeted attacks and malware, with 24x7 monitoring and support from your own 'crack team' of Kaspersky experts, drawing on a deep pool of specialist skills and ongoing threat intelligence.
- The timely and accurate detection of non-malware attacks, attacks involving previously unknown tools and attacks exploiting zero-day vulnerabilities.
- Immediate protection against any detected threat through automatic antivirus database updates.
- Retrospective analysis of incidents and threat hunting, including the methods and technologies used by threat actors against your organization.
- An integrated approach – The Kaspersky portfolio includes all the technologies and services you need to implement a complete cycle of protection against targeted attacks: Preparation – Detection-Investigation – Data Analysis – Automated Protection.

Service benefits

- Fast, efficient detection, enabling faster and more effective mitigation and remediation.
- No time-wasting false positives, thanks to the clear, immediate identification and classification of any suspicious activity.
- Reduced overall security costs. No need to employ and train a range of different in-house specialists you may need.
- The reassurance of knowing that you are continuously protected against even the most complex and innovative non-malware threats.
- Insights into attackers, their motivation, their methods and tools, and the potential damage they could inflict, supporting the development of your fully informed, effective protection strategy.



The service in more detail
Kaspersky Targeted Attack Discovery includes the following activities:

Gathering and analyzing data on attacks from external sources. The aim at this stage is to obtain a snapshot of the attack surface of a company whose assets are, or were, being targeted by intruders. We tap into a variety of intelligence sources, including underground cybercriminal communities, as well as internal Kaspersky monitoring systems. Analyzing this intelligence allows us to identify weaknesses in a company's infrastructure that are of interest to cybercriminals, compromised accounts, stolen data and much more.

Onsite data collection. This stage sees data collected from workstations, servers, SIEM systems and other equipment in the customer's infrastructure. Some of the data is collected using software provided to the customer within the framework of the service.

Data analysis. Kaspersky experts use the data collected at the previous stage to identify incidents in the corporate network. The main purpose of this stage is to determine the type of incident and assess its impact on the infrastructure, which allows the appropriate remediation measures to be implemented. At this stage, data from workstation logs, network activity data, and other contextual and historical intelligence is used; no additional data is collected directly from compromised systems.

Early incident response. At this stage we provide interim recommendations for initial incident response. In some cases, to confirm and classify an incident, Kaspersky experts may require additional data, such as various files from operating systems, applications and network equipment, network traffic dumps, hard disk images, memory dumps or other types of data. The customer may be asked to provide additional data (via email or various network resources, depending on the type and amount of data requested).

Report preparation. The work carried out within the framework of the service culminates in a final report. It contains the results of data analysis from external sources, as well as descriptions of detected attacks based on analysis of the data collected in the customer's infrastructure. The report also contains remediation recommendations for the detected attacks.

Additional services
You can also ask our experts to analyze the symptoms of an incident, perform deep digital analysis for certain systems, identify a malware binary (if any) and conduct malware analysis. These optional services report separately, with further remediation recommendations.

We can also, on request, deploy the **Kaspersky Anti Targeted Attack (KATA) Platform** onto your network, permanently or as a 'proof of concept' exercise. This platform combines the latest technologies and global analytics in order to detection and respond promptly to targeted attacks, counteracting the attack at all stages of its lifecycle in your system.

Targeted Attack Discovery

Kaspersky experts provide proactive Targeted Attack Discovery service to ensure the true security of your business assets.

Targeted Attack Discovery results will let you identify current cybercriminal and cyberespionage activity in your network, understand the reasons behind and possible sources of these incidents, and effectively plan mitigation activities that will help avoid similar attacks in future. If you are concerned about attacks directed at your industry, if you have noted possible suspicious behavior in your own systems, or if your organization simply recognizes the benefits of regular preventative inspections, Kaspersky Targeted Attack Discovery services are designed to tell you:

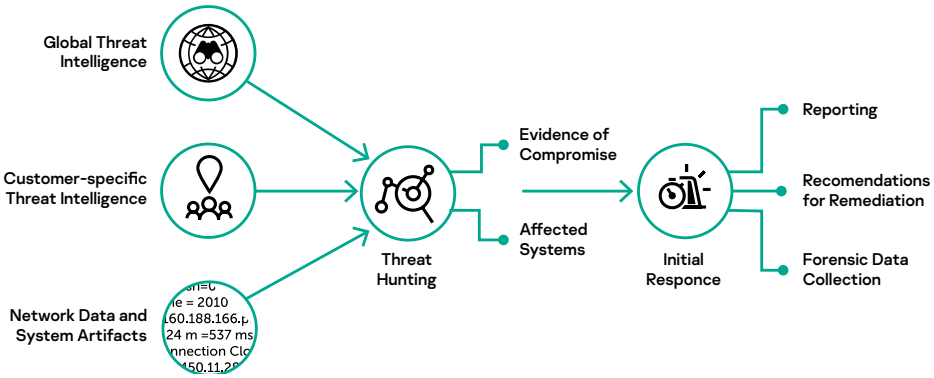
- Whether you are currently under attack, how, and by whom
- How this attack is affecting your systems, and what you can do about it
- How best to prevent further attacks

How the service works

Our globally-recognized independent experts will reveal, identify and analyze ongoing incidents, advanced persistent threats (APTs), cybercriminal and cyber-espionage activities in your network. They will help you to uncover malicious activities, understand the possible sources of incidents, and to plan the most effective remedial actions.

We do this by:

- Analyzing threat intelligence sources to understand your organization's specific threat landscape
- Conducting in-depth scans of your IT infrastructure and data (such as log files) to uncover possible signs of compromise
- Analyzing your outgoing network connections for any suspicious activity
- Uncovering probable sources of the attack, and other potentially compromised systems



The results

Our findings are delivered in a detailed report covering:

- **General information** confirming your network is compromised or signs that it may be;
- **Analysis of the intelligence** gathered about threats and indicators of compromise (IOC);
- **Description of possible attack sources** and compromised network components;
- **Remediation recommendations** to mitigate the impact of an incident and protect your resources from similar attacks in future.

Kaspersky Cybersecurity Training

Cybersecurity education is the critical tool for enterprises faced with an increasing volume of constantly evolving threats. IT Security staff need to be skilled in the advanced techniques that form a key component of effective enterprise threat management and mitigation strategies.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
  - Windows Digital Forensics
  - Malware Analysis and Reverse Engineering
  - Advanced Windows Digital Forensics
  - Advanced Malware Analysis and Reverse Engineering
  - Windows Incident Response
  - Efficient Threat Detection with Yara
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

These courses offer a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert. All are available either in-class on customer premises or at a local or regional Kaspersky office, if applicable.

Courses are designed to include both theoretical classes and hands-on 'labs'. On completion of each course, attendees will be invited to complete an evaluation to validate their knowledge.

Service Benefits

Windows Digital Forensics and Advanced Windows Digital Forensics

Improve the expertise of your in-house digital forensics and incident response team. Courses are designed to fill experience gaps – developing and enhancing practical skills in searching for digital cybercrime tracks and in analyzing different types of data for restoring attack timelines and sources. Having completed the course, students will be able to successfully investigate computer incidents and improve the security level of the business.

Malware Analysis and Reverse Engineering and Advanced Malware Analysis and Reverse Engineering

These courses are intended for security researchers and incident response personnel, malware analysts, security engineers, network security analysts, APT hunters and IT security staff. Students will become familiar with the scope of reverse engineering applications, assembly language, corresponding tools, common techniques used by malware authors to maintain persistence, avoid detection, inject into system processes memory etc. The advanced course will cover most of the steps required to analyze a modern APT toolkit, from receiving the initial sample, all the way to producing a deep technical description with IOCs.

Windows Incident Response

Course will guide your in-house team through all of the stages of the incident response process and equip them with the comprehensive knowledge needed for successful incident remediation.

Efficient Threat Detection with Yara

Will help to learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats that nothing else does.

Hands-On Experience

From a leading security vendor, working and learning alongside our global experts who inspire participants through their own experience at the 'sharp end' of cybercrime detection and prevention.

Program Description

Topics	Duration	Skills gained
Windows Digital Forensics		
Through a real-life simulated cyber targeted attack incident, the course will cover the following topics: · Introducing digital forensics · Live response and evidence acquisition · Post-mortem analysis of Windows machines · Windows OS registry internals · Windows OS events · Windows OS artifacts analysis · Browsers artifacts forensics · Email analysis · Forensics challenges with SSD disks · Recommendations when building a digital forensics lab · Testing the newly gained skills with a practical challenge using different Windows artifacts	5 days	· Acquiring various digital evidence and dealing with it in forensically sound environment · Find traces of incident-related malicious activities from the Windows OS artifacts · Utilizing time stamps from different Windows artifacts to reconstruct an incident scenario · Finding and analyzing browser and email history · Be able be apply the tools and instruments of digital forensics · Understating the process of creating a digital forensics lab
Malware Analysis & Reverse Engineering		
· Basic analysis using IDA Pro · Dynamic analysis using popular virtualization solutions and debuggers · Malicious documents analysis · Unpacking · Decryption · Shellcodes analysis · Exploit analysis · Reversing tips and tricks	5 days	· Get preliminary knowledge about OS and assembly language · Conduct static and dynamic malware analysis obtaining full understanding of its behavior and functionality · Deal with malware anti-analysis tricks, self-protective techniques and protection software bypasses · Identify and reverse engineer standalone and embedded shellcodes · Be able to analyze PDF exploits from scratch
Advanced Windows Digital Forensics		
Through a real-life simulated cyber targeted attack incident, the course will cover the following topics: · Numerical systems · FAT file system · NTFS file system · Deep Windows forensics · Data and file recovery from file system, shadow copies and using file carving · Forensics challenges in Cloud computing · Memory forensics · Network forensics · Timeline vs SuperTimeline analysis · Testing the newly gained skills with a practical challenge with acquired digital evidence	5 days	· Conducting deep file system analysis · Identifying and recovering deleted files using different techniques · Analyzing network traffic with different tools · Identifying and tracking malicious activities in memory dump · Identifying and dumping interesting parts from memory for further analysis · Reconstructing the incident timeline using file system timestamps · Creating one timeline for all Windows OS artifacts for a better understating of the incident scenario
Advanced Malware Analyisis & Reverse Engineering		
· Unpacking · Decryption · Developing own decryptors for common scenarios · Byte code decompilation · Code decomposition · Disassembly · Reconstruction of modern APT architectures · Recognizing typical code constructs · Identification of cryptographic and compression algorithms · Classification and attribution based on code and data · Class and structure reconstruction · APT plugin architectures (based on recent APT samples)	5 days	· Be able to analyze a modern APT toolkit, from receiving the initial sample, all the way to producing a technical description of the attacker's TTPs with IOCs · Producing static decryptors for real-life scenarios and then continuing with in-depth analysis of the malicious code · Be able to analyze malicious documents that are typically used to deliver initial payloads and know how to extract them · Ensuring damage assessment and incident response efforts are accurate and effective
Windows Incident Response		
In a real-life simulated environment, an incident will take place and the course will cover the following topics on that scenario: · Introducing the incident response process and its workflow · Explaining the difference between normal threats and APTs · Explaining APT Cyber Kill Chain · Applying the incident response process to different incident scenarios · Applying Cyber Kill Chain on the simulated environment · Applying live analysis on victim machines for first responders · Forensically sound evidence-acquisition techniques · Introducing post-mortem analysis and digital forensics · Introducing memory forensics · Log file analysis with regular expressions and ELK · Introducing cyber threat intelligence · Creating IoCs (Indicators of Compromise), with YARA and SNORT · Introducing malware analysis and sandboxing · Introducing network traffic forensics · Discussing incident analysis reporting and recommendations on building CSIRT · Testing the newly gained skills with a practical challenge in another simulated scenario	5 days	· Understanding the phases of incident response · What to consider while responding to a cyber incident · Understanding various attack techniques and targeted attack anatomy through the Cyber Kill Chain · Responding to different incidents with appropriate actions · The ability to differentiate APTs from other threats · Confirming cyber incidents using live analysis tools · Understanding the difference between live analysis and post-mortem – and when to apply each of them · Identifying digital evidence; HDD, memory and network traffic with an introduction on their forensics analysis · Writing YARA and SNORT IOCs for the detected attack · Log file analysis · Understanding the process involved in building an IR team
Efficient Threat Detection with Yara		
· Brief intro into Yara syntax · Tips & tricks to create fast and effective rules · Yara-generators · Testing Yara rules for false positives · Hunting new undetected samples on VT · Using external modules within Yara for effective hunting · Anomaly search · Lots (!) of real-life examples · A set of exercises for improving your Yara skills	2 days	· Create effective Yara rules · Test Yara rules · Improve them to the point where they find threats that nobody else does

Kaspersky Incident Response

While your IT and security specialists work hard to ensure that every network component is both secure against intruders and fully available to legitimate users, a single vulnerability can offer an open door to any cybercriminal intent on gaining control over your information systems. No one is immune: however effective your security controls, you can become a victim.

It's becoming increasingly difficult to prevent information security incidents. But while it may not always be possible to halt an attack before it penetrates your security perimeter, it's absolutely in our power to limit the resultant damage and to prevent the attack from spreading.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
- **Kaspersky Incident Response**
  Incident Response
  Malware Analysis
  Digital Forensics
- **Kaspersky Security Assessment**

The overall aim of Incident Response is to reduce the impact of a security breach or an attack on your IT environment. The service covers the entire incident investigation cycle, from the onsite acquisition of evidence to the identification of additional indications of compromise, preparing a remediation plan and completely eliminating the threat to your organization.

We do this by:

- Identifying compromised resources.
- Isolating the threat.
- Preventing the attack from spreading.
- Finding and gathering evidence.
- Analyzing the evidence and reconstructing the incident's chronology and logic.
- Analyzing the malware used in the attack (if any malware is found).
- Uncovering the sources of the attack and other potentially compromised systems (if possible).
- Conducting tool-aided scans of your IT infrastructure to reveal possible signs of compromise.
- Analyzing outgoing connections between your network and external resources to detect anything suspicious (such as possible command and control servers).
- Eliminating the threat.
- Recommending further remedial actions you can take.

Depending on whether or not you have your own incident response team, you can ask our experts to execute the complete investigation cycle, to simply identify and isolate compromised machines and prevent dissemination of the threat, or to conduct Malware Analysis or Digital Forensics.

Kaspersky's Incident Response Services are carried out by highly experienced cyber-intrusion detection analysts and investigators. The full weight of our global expertise in Digital Forensics and Malware Analysis can be brought to bear on the resolution of your security incident.

Malware Analysis

Malware Analysis offers a complete understanding of the behavior and objectives of the specific malware files that are targeting your organization. Kaspersky's experts carry out a thorough analysis of the malware sample you provide, creating a detailed report that includes:

- **Sample properties:** A short description of the sample and a verdict on its malware classification.
- **Detailed malware description:** An in-depth analysis of your malware sample's functions, threat behavior and objectives – including IOCs – arming you with the information required to neutralize its activities.
- **Remediation scenario:** The report will suggest steps to fully secure your organization against this type of threat.

Digital Forensics

Digital Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky experts piece together the evidence to understand exactly what's going on, including the use of HDD images, memory dumps and network traces. The result is a detailed elucidation of the incident. You as the customer initiate the process by gathering evidence and providing an outline of the incident. Kaspersky experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

Delivery options

Kaspersky's Incident Response Services are available:

- By subscription
- In response to a single incident

Both options are based on the amount of time our experts spend resolving the incident – this is negotiated with you prior signing the contract. You can specify the number of working hours you wish us to spend, or follow our experts' recommendations based on the specific incident and your individual requirements.

Kaspersky Security Assessment

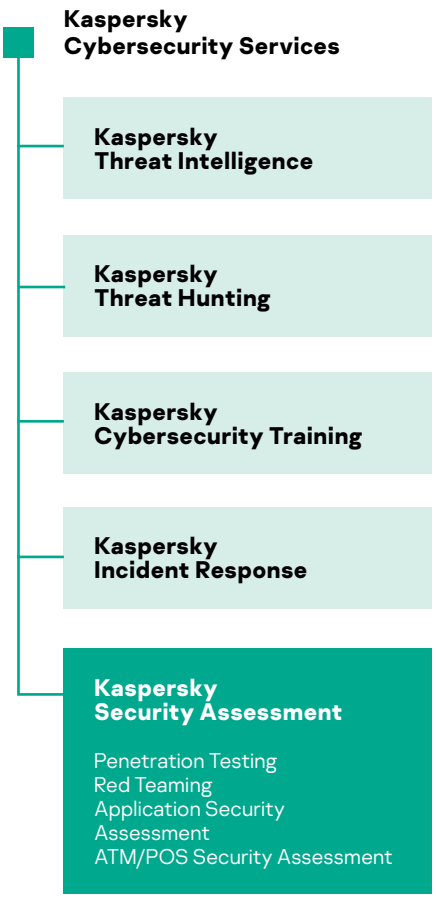
Security Assessment Services from Kaspersky are the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

Because no two IT infrastructures are exactly the same, and because the most powerful cyberthreats are tailor-made to exploit the specific vulnerabilities of the individual organization, our expert services are also tailor-made. The services described on the following pages form a part of our professional toolkit – some or all of these services, in part or in full, may be applied as we work with you.

Our objective, above all, is to work with you, one on one, as your expert advisors, helping to evaluate your risk, harden your security and mitigate against future threats.

Security Assessment Services include:

- **Penetration Testing**
- **Red Teaming**
- **Application Security Assessment**
- **ATM/POS Security Assessment**



Penetration Testing

Ensuring that your IT infrastructure is fully secured against potential cyberattack is an ongoing challenge for any organization, but even more so for large enterprises with perhaps thousands of employees, hundreds of information systems, and multiple locations worldwide.

Penetration testing is a practical demonstration of possible attack scenarios where a malicious actor may attempt to bypass security controls in your corporate network to obtain high privileges in important systems.

Kaspersky's Penetration Testing gives you a greater understanding of security flaws in your infrastructure, revealing vulnerabilities, analyzing the possible consequences of different forms of attack, evaluating the effectiveness of your current security measures and suggesting remedial actions and improvements.

Penetration Testing from Kaspersky helps you and your organization to:

- **Identify the weakest points in your network,** so you can make fully informed decisions about where best to focus your attention and budget in order to mitigate future risk.
- **Avoid financial, operational and reputational losses caused by cyber-attacks** by preventing these attacks from ever happening through proactively detecting and fixing vulnerabilities.
- **Comply with government, industry or internal corporate standards** that require this form of security assessment (for example Payment Card Industry Data Security Standard (PCI DSS)).

Penetration testing results
The Service is designed to reveal security shortcomings which could be exploited to gain unauthorized access to critical network components. These could include:

- Vulnerable network architecture, insufficient network protection
- Vulnerabilities leading to network traffic interception and redirection
- Insufficient authentication and authorization in different services
- Weak user credentials
- Configuration flaws, including excessive user privileges
- Vulnerabilities caused by errors in application code (code injections, path traversal, client-side vulnerabilities, etc.)
- Vulnerabilities caused by usage of outdated hardware and software versions without latest security updates
- Information disclosure

Results are given in a final report including detailed technical information on the testing process, results, vulnerabilities revealed and recommendations for remediation, as well as an executive summary outlining test results and illustrating attack vectors. Videos and presentations for your technical team or top management can also be provided if required.

Service scope and options

Depending on your needs and your IT infrastructure, you may choose to employ any or all of these Services:

- **External penetration testing:** Security assessment conducted through the Internet by an 'attacker' with no preliminary knowledge of your system.
- **Internal penetration testing:** Scenarios based on an internal attacker, such as a visitor with only physical access to your offices or a contractor with limited systems access.
- **Social engineering testing:** An assessment of security awareness among your personnel by emulating social engineering attacks, such as phishing, pseudo-malicious links in emails, suspicious attachments, etc.
- **Wireless networks security assessment:** Our experts will visit your site and analyze WiFi security controls.

You can include any part of your IT infrastructure into the scope of penetration testing, but we strongly recommend you consider the whole network or its largest segments, as test results are always more worthwhile when our experts are working under the same conditions as a potential intruder.

About Kaspersky's approach to penetration testing

While penetration testing emulates genuine hacker attacks, these tests are tightly controlled; performed by Kaspersky security experts with full regard to your systems' confidentiality, integrity and availability, and in strict adherence to international standards and best practices including:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Project team members are experienced professionals with a deep, current practical knowledge of this field, acknowledged as security advisors by industry leaders including Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens and SAP.

Delivery options

Depending on the type of security assessment service, your systems specifics and working practices, security assessment services can be provided remotely or onsite. Most services can be performed remotely, and internal penetration testing can even be performed through VPN access, while some services (like wireless networks security assessment) require an onsite presence.

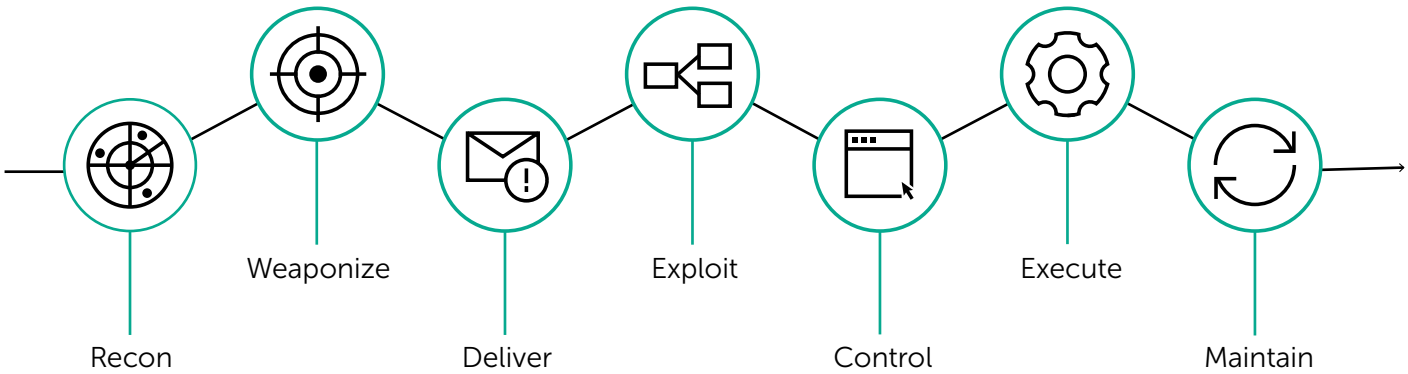
Red Teaming

The service includes the following:

- **Threat Intelligence.** The service starts with a discussion of the customer's known threats and Blue Team's experience. The aim is to identify highly critical business assets and understand how project deliverables can be tailored towards TTPs used by the company's defense. However, during these discussions, Kaspersky will not request any information about the target resources, as the Red Team will also conduct independent information gathering activities like real adversaries would do. The information gathering phase will include both analysis of publically available information (open-source intelligence), and analysis of data available in underground communities.

- **Adversary Simulation.** This stage starts with preparation of attack scenarios and tools based on the results of the Threat Intelligence stage. Preparation may include deep research into the systems used in the customer's environment to reveal new vulnerabilities, developing custom tools aimed at bypassing the customer's security systems, or readying spear-phishing attacks. When the preparation is complete, Kaspersky will perform the active phase of Adversary Simulation. These tests may include the following:

  - Passive information gathering,
  - Active information gathering (network discovery), including port scanning, identifying available services and manual requests to certain services (DNS, mail),
  - External vulnerability scanning, and analyzing
  - Web application security (using both automated and manual approaches) to identify the following types of vulnerabilities:
    - Code injection (SQL Injection, OS Commanding, etc.)
    - Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
    - Flaws in authentication and authorization
    - Insecure data storage
    - Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and OWASP Top Ten
  - Manual vulnerability analysis, including identification of resources without authentication, important publically available information, insufficient access control
  - Guessing credentials
  - Social engineering testing
  - Exploitation of one or more of the vulnerabilities found and privilege escalation (if possible)
  - Develop an attack using the obtained privileges and techniques listed above until the Service Provider can access the LAN or important network resources (e.g. Active Directory domain controller, business systems, DBMSes, etc.) or until all attack methods available during testing have been exhausted.



The above tests are carried out according to the prepared customer-specific scenarios, using special techniques to evade detection from the Blue Team. Once the Red Team has accomplished all its objectives, activities that trigger incident detection and response are carried out to ensure Blue Team involvement in the exercise.

- **Report Preparation.** During this stage, Kaspersky will analyze the Adversary Simulation results, prepare a report with detailed description of the attacks (including timestamps and indicators of compromise) and recommendations.
- **Testing Results Overview.** A post-assessment workshop with the company's Blue Team can be arranged to discuss the project results, reasons for anything not detected or prevented, and possible further defense improvements.

Approach and Methodology

Red Teaming has much in common with a real hacker attack and makes it possible to assess the effectiveness of the protection measuresin practice. However, unlike a hacker attack, the service is performed by experienced security experts from Kaspersky who take special care of system confidentiality, integrity and availability in strict adherence to the following **international standards and best practices:**

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC)
- Threat Classification Open Web Application Security Project (OWASP)
- Testing Guide Common Vulnerability Scoring System (CVSS)
- And other standards, depending on your organization's business and location

The analysis is performed using automated tools as well as manually by experts.
The following security assessment tools can be used:

- Information gathering tools (Maltego, theHarvester and others)
- Various general-purpose and specialized scanners (NMap, MaxPatrol, Nessus, Acunetics WVS, nbtscan and others)
- Complex security assessment solutions (Kali Linux)
- Credentials guessing tools (Hydra, ncrack, Bruter, and others)
- Specialized solutions for web application security assessment (OWASP dirbuster, BurpSuite, ProxyStrike, various plug-ins for Mozilla Firefox)
- Network traffic analyzers (Wireshark, Cain and Abel)
- Credentials extraction and management tools (Mimikatz, WCE, pwdump and others)
- Specialized tools for various types of attacks (Yersinia, Loki, Responder, SIPVicious and others)
- Disassembling and debugging tools (IDA Pro, OllyDbg)
- And others, including limited access exploits and custom exploitation tools developed by the Service Provider.

For Red Teaming to be legal and safe, the customer must provide a point of contact (a representative) for all project communications, including scope negotiations and, resolving access issues, as well as giving confirmation for active works.
The representative must be an official employee of the customers with an e-mail address belonging to the customer's domain name (not a third-party intermediary).

The confidentiality, integrity and availability of your IR resources are our top priority. Kaspersky's experts will take all necessary precautions to avoid any harm to your environment. All sensitive technical information related to the project (important data, credentials, assessment results, etc.) will be stored and transferred using strong encryption, and can be deleted on your request after the project has been completed.

Our expert team members are experienced professionals in security assessment with deep knowledge of this field, constantly improving their skills. They have been acknowledged for their security research by such industry leaders as Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens, SAP, and others (see section 7 for description of the project team). You can find resumes of the project team members in the attachment to this proposal.

Outcome

Following the service, customers receive a report containing the following:

- High-level conclusions on the identified defensive capabilities, and recommendations to improve them;
- A detailed description of detected vulnerabilities, including severity level, exploitation complexity, possible impact on the vulnerable system, and evidence of the existence of vulnerabilities (where possible);
- A detailed description of activities (including timestamps and indicators of compromise) for analysis and improvement of the defensive team;
- Recommendations for eliminating vulnerabilities;
- Recommendations on improving the incident response processes;
- Recommendations on mitigating the identified prevention and detection issues.

The Red Teaming Testing Service from Kaspersky will help you evaluate the effectiveness of your monitoring capabilities and incident response procedures.

Application Security Assessment

Whether you develop corporate applications internally, or purchase them from third parties, you'll know that a single coding error can create a vulnerability exposing you to attacks resulting in considerable financial or reputational damage. New vulnerabilities can also be generated during an application's lifecycle, through software updates or insecure component configuration, or can arise through new attack methods.

Kaspersky's Application Security Assessment uncover vulnerabilities in applications of any kind, from large cloud-based solutions, ERP systems, online banking and other specific business applications, to embedded and mobile applications on different platforms (iOS, Android and others).

Combining practical knowledge and experience with international best practices, our experts detect security flaws which could expose your organization to threats including:

- Syphoning off confidential data
- Infiltrating and modifying data and systems
- Initiating denial of service attacks
- Undertaking fraudulent activities

Following our recommendations, vulnerabilities revealed in applications can be fixed, and such attacks prevented.

Service benefits

Kaspersky Application Security Assessment Services help application owners and developers to:

- **Avoid financial, operational and reputational loss**, by proactively detecting and fixing the vulnerabilities used in attacks against applications
- **Save remediation costs** by tracking down vulnerabilities in applications still in development and test, before they reach the user environment where fixing them may involve considerable disruption and expense.
- **Support a secure software development lifecycle** (S-SDLC) committed to creating and maintaining secure applications.
- **Comply with government, industry or internal corporate standards** covering application security, such as PCI DSS or HIPAA

Vulnerabilities which may be identified:

- Flaws in authentication and authorization, including multi-factor authentication
- Code injection (SQL Injection, OS Commanding, etc.)
- Logical vulnerabilities leading to fraud
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Use of weak cryptography
- Vulnerabilities in client-server communications
- Insecure data storage or transferring, for instance lack of PAN masking in payment systems
- Configuration flaws, including ones leading to session attacks
- Sensitive information disclosure
- Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.

Service scope and options

Applications assessed can include official web sites and business applications, standard or cloud based, including embedded and mobile applications.

The services are tailored to your needs and application specifics, and may involve:

- **Black-box testing** – emulating an external attacker
- **Grey-box testing** – emulating legitimate users with a range of profiles
- **White-box testing** – analysis with full access to the application, including source codes; this approach is the most effective in terms of revealing numbers of vulnerabilities
- **Application firewall effectiveness assessment** – applications are tested with and without firewall protection enabled, to find vulnerabilities and verify whether potential exploits are blocked

Results

Results are given in a final report including detailed technical information on the assessment processes, results, vulnerabilities revealed and recommendations for remediation, together with an executive summary outlining management implications. Videos and presentations for your technical team or top management can also be provided if required.

About Kaspersky's Approach To Application Security Assessment

Security assessments of applications are performed by Kaspersky security experts both manually and through applying automated tools, with full regard to your systems' confidentiality, integrity and availability and in strict adherence to international standards and best practices, such as:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide
- Other standards, depending on your organization's business and location

Project team members are experienced professionals with a deep, current practical knowledge of the field, including different platforms, programming languages, frameworks, vulnerabilities and attack methods. They speak at leading international conferences, and provide security advisory services to major vendors of applications and cloud services, including Oracle, Google, Apple, Facebook and PayPal.

Delivery options

Depending on a type of security assessment service, specifics of systems in the scope, and your requirements to work conditions, security assessment services can be provided remotely or onsite. Most of these services can be performed remotely.

ATM/POS Security Assessment

ATMs and POS devices are no longer vulnerable only to physical attacks like ATM burglary or card skimming. As protection measures applied by banks and ATM/POS vendors evolve, so attacks against these devices also shift up a gear, becoming ever more sophisticated. Hackers are exploiting vulnerabilities in ATM/POS infrastructure architecture and applications, and are creating malware specifically tailored to ATM/POS. ATM/POS Security Assessment services from Kaspersky help you to recognize the security flaws in your ATM/POS devices, and to mitigate the risk of being compromised.

There is no single solution that offers comprehensive protection. As a business manager, it`s your responsibility to protect your organization against today's threats, and to anticipate the dangers that lie ahead in the coming years. This needs more than just smart operational protection against known threats; it demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

Security Assessment Services from Kaspersky – the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

ATM/POS
Security Assessment
Comprehensive analysis of ATMs and POS devices, designed to identify vulnerabilities that can be used by attackers:

- unauthorized cash withdrawal
- performing unauthorized transactions
- obtaining your clients' payment card data
- initiating denial of service

What happens when fraudsters goes in?
Each ATM machine consist of 4 cassettes with up to 3000 banknotes in each cassette. In worst case scenario criminals can obtain up to 255000$. ATM cash-out scheme happened in May, 2016 showed, that criminals are ready to coordinate their actions to access 1400 ATM machines in couple hours frame. Taiwan incident in July, 2016 with malicious software installed on multiple ATMs given criminals possibility to withdraw 2 million $ from twenty ATMs. Criminals are ready to attack ATMs. Don't be a victim.

Who we are
Project team members are professionals highly experienced in practical security, who have a deep knowledge in the field and are constantly improving their skills; they regularly provide security consultancy to ATM/POS vendors and present the results of our ATM/POS security researches at leading information security conferences, including Black Hat, Hack in Paris, Positive Hack Days, Security Analyst Summit, Nuit Du Hack, HITB GSEC, DefCamp, ATMIA events, Chaos Communication Congress and many others.

Follow our experts at
www.securelist.com

Call us for help 1337@kaspersky.com

Why you should do this

ATM/POS Security Assessment by Kaspersky helps vendors and financial organizations to:

- Understand the vulnerabilities in their ATM/POS devices and improve your corresponding security processes
- Avoid the financial, operational and reputational losses that can result from an attack, through proactively detecting and fixing the vulnerabilities whichattackers could exploit.
- Comply with government, industry or internal corporate standards, which include the carrying out of security assessments, e.g. PCI DSS (Payment Card Industry Data Security Standard).

What we are testing

The service includes comprehensive ATM/POS analysis including assessment of software components, hardware devices and network communications. Service can be conducted on a single ATM/POS device or on a network of devices. We recommend you to choose for assessment the type of ATMs/POS device in most common use within your organization, or those that are most critical (which have, for instance, already suffered from incidents) in their typical configurations.

How we do this

During analysis, our experts will not just seek out and identify configuration flaws and vulnerabilities in obsolete software versions, but will deeply analyze the logic behind the processes performed by your ATMs/POS devices, undertaking security research aimed at identifying any new (0-day) vulnerabilities at component level. If we uncover vulnerabilities which could profit an attacker (resulting, for example, in unauthorized cash withdrawal), our experts can provide demonstrations of possible attack scenarios using specially crafted automation tools or devices.

Though an ATM/POS Security Assessment involves emulating the attack behavior of a genuine hacker in order to practically assess the effectiveness of your defenses, it is entirely safe and non-invasive.

Threats for Financial Industry

As banks, stock markets, and other financial institutions are under persistent interest of cybercriminals due to the very nature of the financial business, to avoid financial and reputational losses they have to stay ahead of the curve in the field of cybersecurity. Kaspersky offers a set of proactive threat intelligence services for financial institutions that are looking to enhance their security operations and take a proactive approach against advanced threats:

- Security Assessment Services (Penetration Testing, Application Security Assessment, ATM and POS Security Assessment)
- Threat Intelligence Reports (APT Intelligence Reports, Customer-Specific Threat Intelligence Reports)
- Cyber-Attack Readiness Testing
- Botnet Threat Tracking
- Threat Data Feeds
- Malware Analysis and Digital Forensic
- Training: Threat Analysis, Forensic and Investigation

See more at www.kaspersky.com/enterprise

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.