

Kaspersky Cybersecurity Services 2017

www.kaspersky.com
#truecybersecurity



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 Lab

Introduction

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

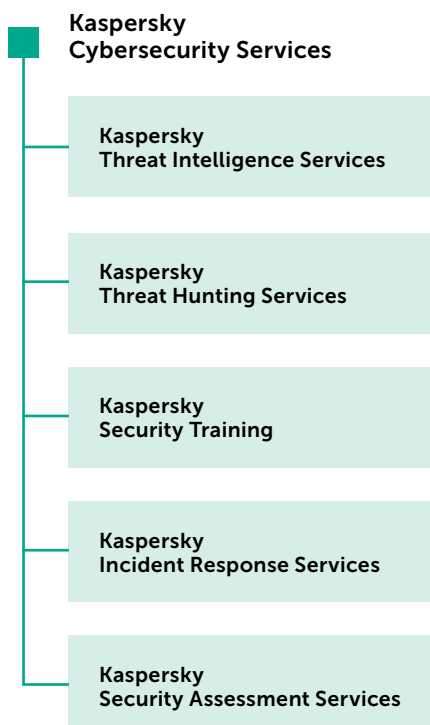
There is no single solution that offers comprehensive protection. However, even in our bigdata world, knowing where to look for danger is a large part of being able to combat the latest threats.

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

Kaspersky Lab 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 Lab products, you can still benefit from Kaspersky Lab Cybersecurity Services.



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, Europol, CERT, City of London Police – have actively sought our assistance.

Kaspersky Lab 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 Services

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

Kaspersky Cybersecurity Services

Kaspersky Threat Intelligence Services

Threat Data Feeds
APT Intelligence Reporting
Tailored Threat Reporting
Kaspersky Threat Lookup
Kaspersky Phishing Tracking
Kaspersky Botnet Tracking

Kaspersky Threat Hunting Services

Kaspersky Security Training

Kaspersky Incident Response Services

Kaspersky Security Assessment Services

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

Kaspersky Lab'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 Lab Threat Intelligence Services include:

- Threat Data Feeds
- APT Intelligence Reporting
- Tailored Threat Reporting
- Kaspersky Threat Lookup
- Kaspersky Phishing Tracking
- Kaspersky Botnet Tracking

Threat Data Feeds

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**.

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**.

Kaspersky Lab offers **continuously updated** Threat Data Feeds to **inform your business or clients about risks** and implications associated with cyber threats, helping you to **mitigate threats more effectively** and **defend against attacks** even before they are launched.

Intelligence Cycle



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;
- Malicious Hash Feed – covering the most dangerous, prevalent and emerging malware;
- 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.
- **NEW!!! Kaspersky Transforms for Maltego** – providing Maltego users with a set of transforms that give access to Kaspersky Lab Threat Data Feeds. Kaspersky Transforms for Maltego allows you to check URLs, hashes, and IP addresses against the feeds from Kaspersky Lab. The transforms can determine the category of an object as well as provide actionable context about it.

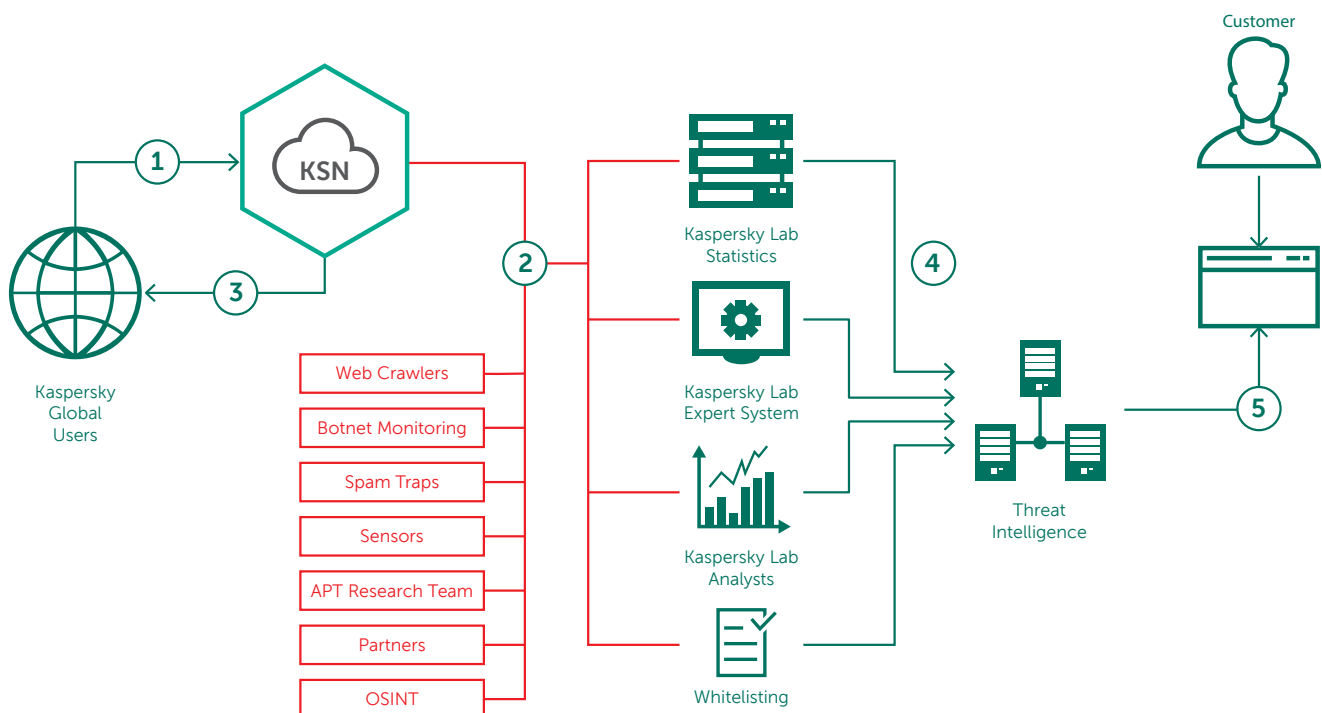
Contextual Data

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**.

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, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, multi-scanners, similarity tools, behavior profiling etc.), analysts validation and [whitelisting](#) verification:



Kaspersky Threat Data Feeds contain thoroughly vetted threat indicator data sourced from the real world in real time.

Service 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 Lab all combine to enable straightforward integration.

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 APT Intelligence Reporting provides:

- **Exclusive access** to technical descriptions of cutting edge threats during the ongoing investigation, before public release.
- **Insight into non-public APTs.** Not all high profile threats are subject to public notification. Some, due to the victims who are impacted, the sensitivity of the data, the nature of the vulnerability fixing process or associated law enforcement activity, are never made public. But all are reported to our customers.
- **Detailed supporting** technical data including an extended list of Indicators of Compromise (IOCs), available in standard formats including OpenIOC or STIX, and access to our Yara Rules.
- **Continuous APT campaign monitoring.** Access to actionable intelligence during the investigation (information on APT distribution, IOCs, C&C infrastructure).
- **Contents for different audience.** Each of the report contains executive summary offering C-level oriented and easy to understand information describing the related APT. 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 an actionable advice for superior protection from the related threat.
- **Retrospective analysis.** Access to all previously issued private reports is provided throughout the period of your subscription.
- **APT Intelligence Portal.** All of the reports including most recent IoC's are available via our APT Intelligence Portal creating seamless user experience for our customers. API is also available.

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 Lab.

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 Lab 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. During 2016 we have created more than 100 reports!

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 Lab's complete APT reports database – a further powerful research and analysis component of your corporate security armory.

Tailored Threat Reporting

Customer-specific Threat 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 Lab 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 using this Kaspersky Lab 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 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.

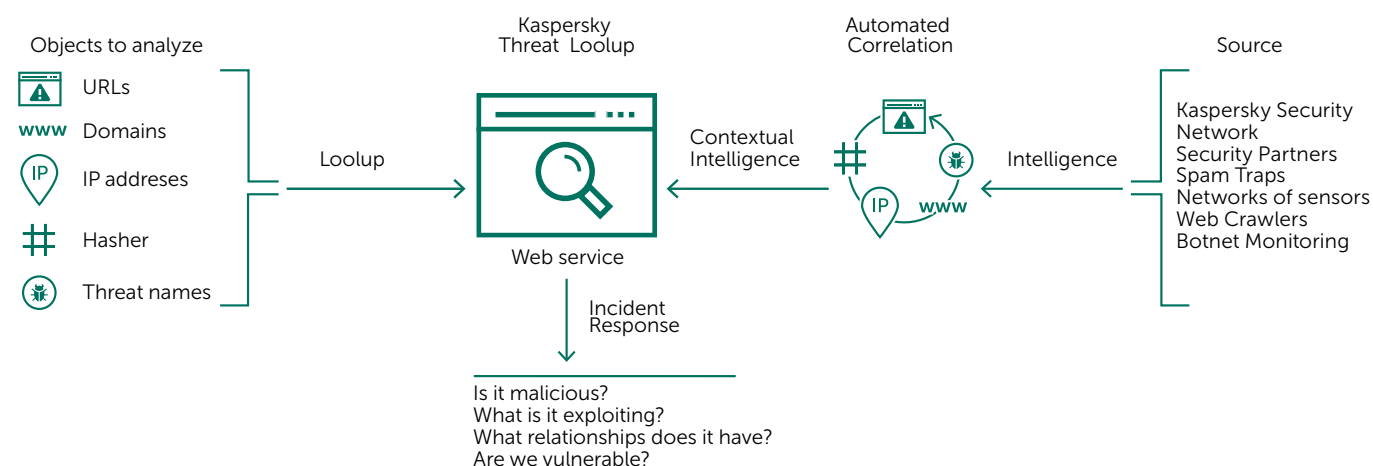
Created using approaches ranging from Open Source Intelligence (OSINT) to deep analysis of Kaspersky Lab expert systems and databases, and our knowledge of the underground cybercriminal networks, Country-specific Threat reports cover areas including:

- **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 Threat Lookup is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky Lab products lead the field in anti-malware tests¹, 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:**² 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 Lab 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.

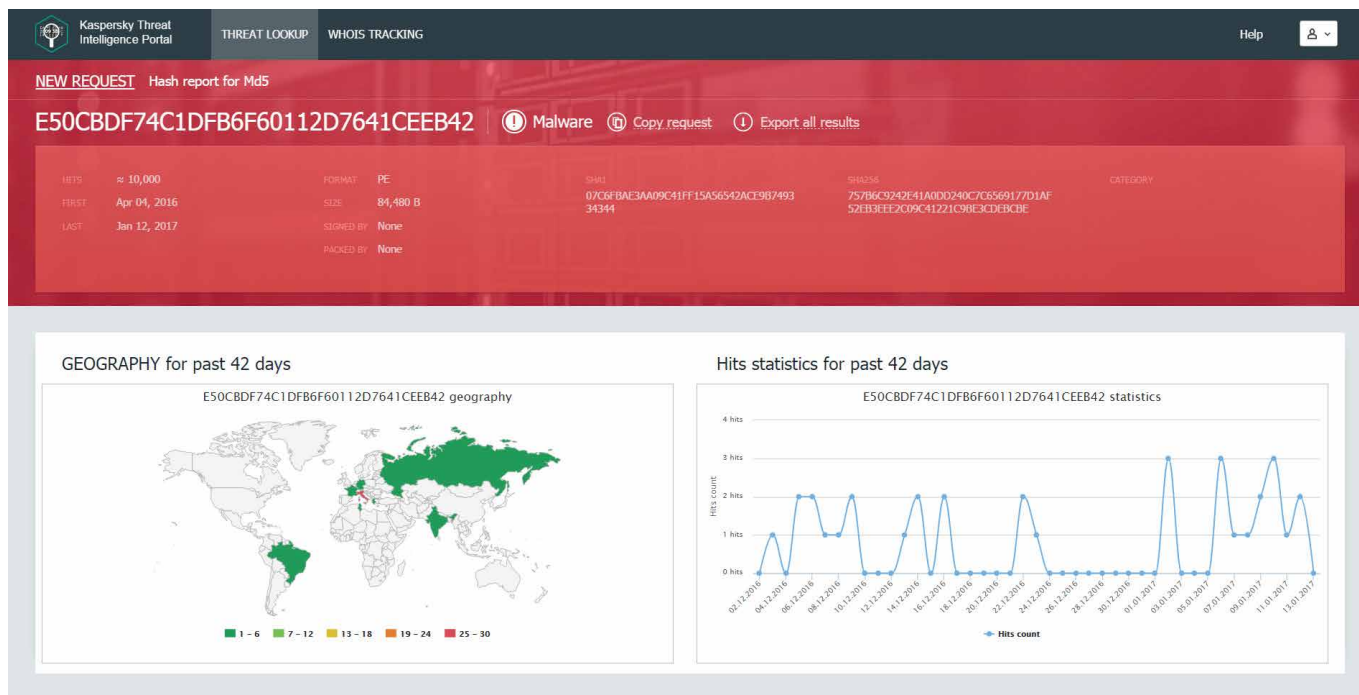
Threat intelligence delivered by Kaspersky Threat Lookup is generated and monitored in real time by a highly fault-tolerant infrastructure ensuring continuous availability and consistent performance. Hundreds of experts, including security analysts from across the globe, world-famous security experts 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>

² The feature is planned to be released in H1' 2017.



Now You Can

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

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

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

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

Every Kaspersky Phishing Tracking notification is delivered via HTTPS and includes:

- Screenshot of the phishing URL;
- HTML-code of the phishing URL;
- JSON file that includes the following fields:
 - the phishing URL;
 - brand name the phishing URL is targeted at;
 - first seen timestamp;
 - last seen timestamp;
 - popularity of the phishing URL;
 - geolocation of users that are affected by the phishing URL;
 - type of stolen data (credit cards info, credentials for bank, email or social network, personal info, and etc.);
 - attack type (a menace to block an account, an offer to download a file, a request to update personal info, and etc.);
 - resolved IP addresses of this phishing URL;
 - WHOIS data;
 - and much more.

Phishing Tracking

Phishing, and particularly targeted spear-phishing, is one of today's most dangerous and effective online fraud methodologies. Fake websites capture logins and passwords to hijack users' online identities, then steal money or spread spam and malware through compromised email accounts and social networking platforms. It's a powerful weapon in the cybercrime armory, and the frequency and diversity of attacks continues to accelerate.

And it's not just financial institutions being hit. Everyone, from online retailers to ISPs and government institutions, now risks coming under active attack from spear-phishing. Picture perfect copies of your website complete with full corporate branding, or messages appearing to come directly from your own named executives, can easily convince users to hand over confidential data – damaging themselves, and causing massive potential damage to your enterprise.

A single successful phishing attack can have a huge impact on its corporate victim. Aside from direct losses, there are all the indirect costs, like cleaning up compromised websites and accounts. And then, of course, there's the reputational damage, which can be worst of all – an erosion of user trust in your online services that can see you hemorrhaging customers and facing credibility challenges for years to come. 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.

Our Solution – Kaspersky Phishing Tracking Service

This service actively tracks and alerts you in real time to the appearance of phishing sites targeting your brand, and provides you with relevant, accurate and detailed ongoing reporting about phishing or fraudulent activity directly relevant to your business, including injected malware and phishing URLs that steal credentials, sensitive information, financial information and personal data from your users. The service also monitors specific Top Level Domains (TLDs) or even whole regions for the appearance of phishing sites

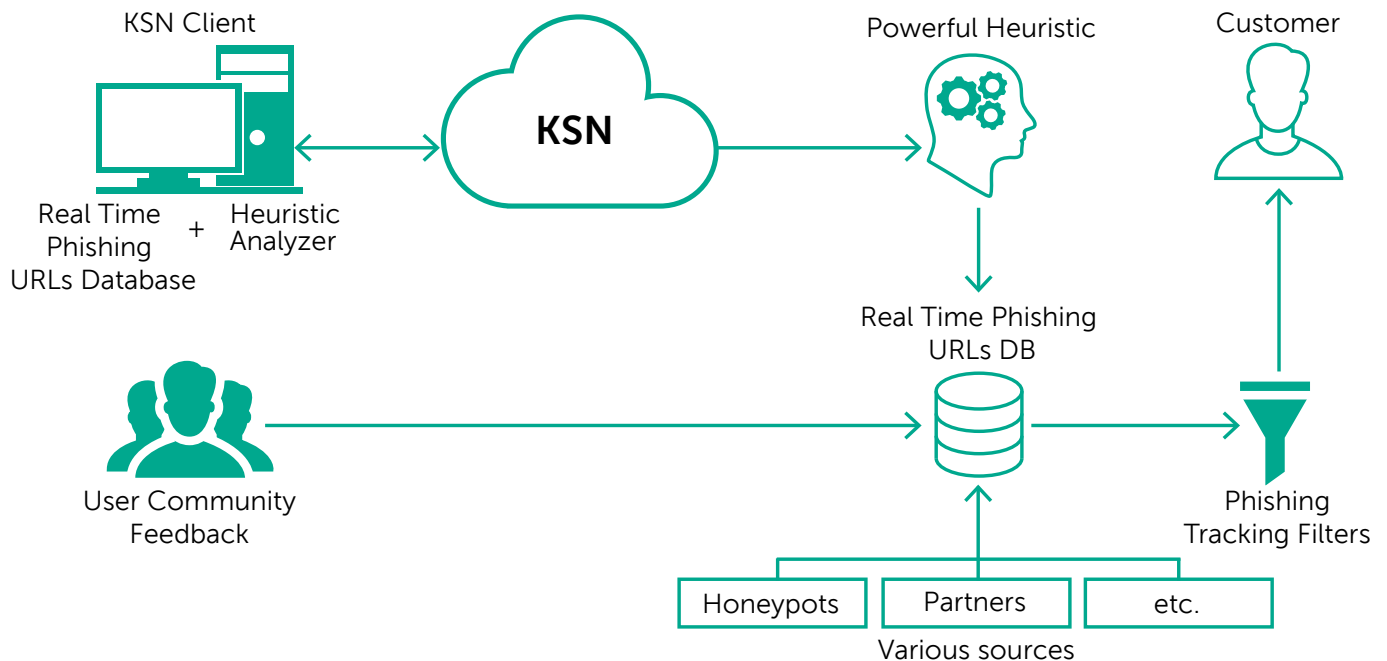
Email notifications confirmed phishing threats against your brands, company name or trademarks are continuously. Every notification provides deep coverage, high accuracy and reliable information about increasingly sophisticated phishing attacks, enabling you to react fast to dynamically generated phishing domains and URLs as well as to phishing outbreaks. Together with a list of phishing sites, you will receive additional intelligence so you can immediately take specific measures against any phishing attack.

Empowered with this timely, professionally validated intelligence, you can act swiftly and with precision to mitigate the impact of phishing activity on your organization and your users, taking a proactive stance against fraud.

Sources of intelligence

Kaspersky Phishing Tracking synthesizes data from heterogeneous, highly reliable intelligence sources, including the Kaspersky Security Network (KSN), powerful heuristic engines, email honeypots, web crawlers, spam traps, research teams, partners and historical data about malicious objects we've been collecting for almost 2 decades. Aggregated data is then fully inspected in real time, and refined using multiple preprocessing techniques including statistical criteria, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, similarity tools, behavior profiling etc.), content analyst validation and whitelisting verification tools.

The worldwide coverage of Kaspersky Security Network, combined with Kaspersky Lab detection technologies and a barrage of tests and filters ensures the maximum detection of any kind of phishing attack and threat with no false positives, as is continuously confirmed through independent tests*.



Your Early Warning of Phishing Attacks

Subscribing to the Kaspersky Phishing Tracking Service gives you a critical edge against your attackers. Armed with early warning of phishing attacks, in progress or still in planning, that are targeting your brands, online services and customers, enables you to protect resources and mitigate risk more pragmatically, more accurately and more cost-effectively.

Getting Ahead

Critical information is provided in real time, as well as through regular reporting on malicious activities that indicate that advanced attacks are being planned, as well as those in progress. Now it's you, not the cybercriminals who have you in their sights, that's one step ahead.

Improving Your Users' Experience

Once you know and understand your spear-phishing adversaries, you can plan appropriate protection, from banning outdated software to introducing SMS-based authorization, all helping your online customers feel better protected and reassured.

Minimizing Impact

Knowing the URLs of phishing websites means ISPs hosting the sites can be notified, preventing the further leakage of any personal data acquired by the site and stopping the attack in its tracks.

Staying Better Informed

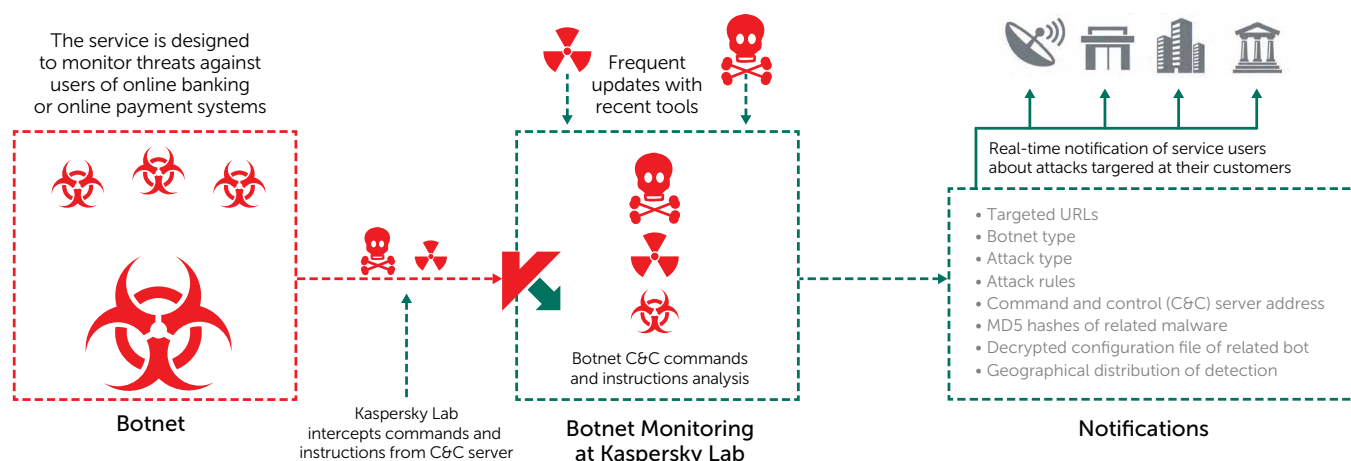
This flow of relevant, accurate and detailed information, with no 'false positives' or time-wasting, provides new insights to help inform and enhance your current and future security strategy. Now, you and your business can take a proactive, informed stance against online fraud.



* AV-comparatives test reports are available upon request.

Botnet Tracking

Expert monitoring and notification services to identify botnets threatening your customers and your reputation.



Use Cases / Service Benefits

- Proactive alerts about threats coming from botnets that target your online users allow you to always remain one step ahead of the attack
- Identifying a list of Botnet Command & Control server URLs that are targeting your online users allows you to block them by sending requests to CERTs or law enforcement agencies
- Improve your online banking / payment cabinets by understanding the nature of attack
- Train your online users to recognize and avoid falling foul of the social engineering used in attacks

Take action with real-time deliverables:

The service provides a subscription to personalized notifications containing intelligence about matching brand names by tracking keywords in the botnets monitored by Kaspersky Lab. Notifications can be delivered via email or RSS in either HTML or JSON format. Notifications include:

- **Targeted URL(s)** — Bot malware is designed to wait until the user accesses the URL(s) of the targeted organization and then starts the attack.
- **Botnet type** — Understand exactly what malware threat is being employed by the cybercriminal to jeopardize your customers' transactions. Examples include Zeus, SpyEye, and Citadel, etc.
- **Attack type** — Identify what the cybercriminals are using the malware to do; for example, web data injection, screen wipes, video capture or forwarding to phishing URL.
- **Attack rules** — Know what different rules of web code injection are being used such as HTML requests (GET / POST), data of web page before injection, data of web page after injection.
- **Command and Control (C&C) server address** — Enables you to notify the Internet service provider of the offending server to dismantle of the threat faster.
- **MD5 hashes of related malware** — Kaspersky Lab provides the hash sum that is used for malware verification.
- **Decrypted configuration file of related bot** — identifying the full list of targeted URLs.
- **Geographical distribution of detection (top 10 countries)** — Statistical data of related malware samples from around the world.

Kaspersky Threat Hunting Services

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 Services

Kaspersky Threat Hunting Services

Kaspersky Managed Protection
Targeted Attack Discovery

Kaspersky Security Training

Kaspersky Incident Response Services

Kaspersky Security Assessment Services

Kaspersky Managed Protection

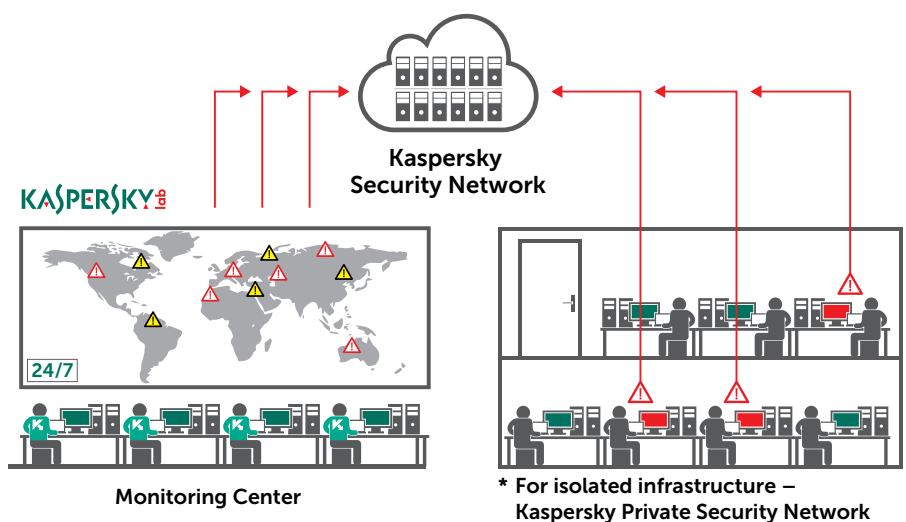
The Kaspersky Managed Protection service offers Kaspersky Endpoint Security and Kaspersky Anti Targeted Attack Platform users a fully managed service, deploying a unique range of advanced technical measures to detect and prevent targeted attacks on your organization. The service includes round-the-clock monitoring by Kaspersky Lab 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 Lab 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 Lab 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:

Threat intelligence gathering and analysis. The goal is to obtain a snapshot in time of your attack surface – the cybercriminal and cyber-espionage threats and attacks potentially or actively targeting your assets. We'll be tapping into internal and external intelligence sources, including underground fraudster communities, as well as internal Kaspersky Lab monitoring systems. Analyzing this intelligence allows us to identify, for example, weaknesses in your infrastructure of current interest to cybercriminals, or compromised accounts.

Onsite data collection and early incident response. Alongside threat intelligence activity conducted in our own labs, Kaspersky Lab experts will be on site collecting network and system artefacts, together with any SIEM information available. We may also conduct a brief vulnerability assessment to reveal the most critical security flaws for immediate action. If an incident has already taken place, we'll be collecting evidence for investigation. At this stage, we'll provide you with our interim recommendations for short-term remediation steps.

Data analysis. The network and system artefacts collected will be analyzed back at the lab, using the Kaspersky Lab knowledge base of IoCs, C&C blacklists, sandboxing technology etc. to understand exactly what's been happening in your system. If, for example, new malware is identified at this stage, we'll give you advice and the tools (i.e. YARA rules) to detect it right away. We'll be keeping in close touch with you throughout, working remotely with your systems if appropriate.

Report preparation. Finally, we'll prepare our formal report with targeted attack discovery results and our recommendations for further remediation activity.

Targeted Attack Discovery

Kaspersky Lab 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:

Our overall discoveries – confirmation of the presence or absence of compromise signs in your network

In-depth analysis – of threat intelligence data gathered and of the Indicators of Compromise (IoCs) revealed.

Detailed descriptions – of vulnerabilities exploited, possible attack sources, and the network components affected.

Remediation recommendations – suggested steps to mitigate consequences of the incident revealed and to protect your resources from similar attacks in future.

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 detect and respond promptly to targeted attacks, counteracting the attack at all stages of its lifecycle in your system.

Kaspersky Security 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 Services

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 Lab office, if applicable.

Kaspersky Threat Hunting Services

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.

Kaspersky Security Training

Digital Forensics
Malware Analysis and Reverse Engineering
Advanced Digital Forensics
Advanced Malware Analysis and Reverse Engineering
Incident Response
Yara
KATA Administration
KATA Security Analyst

Kaspersky Incident Response Services

Kaspersky Security Assessment Services

Service Benefits

Digital Forensics and Advanced 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

Reverse engineering training is designed to help incident responding groups in the investigation of malicious attacks. This course is intended for IT department employees and system administrators. Students will learn to analyze malicious software, to collect IoCs (Indicators of Compromise), to write signatures for detecting malware on infected machines, and to restore infected/encrypted files and documents.

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.

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.

KATA Administration

KATA Administration Training provides all the know-how required to plan, install and configure the solution in order to optimize its threat detection efficiency.

KATA Security Analyst

The training course includes a number of practical exercises based on the real threat detection scenarios providing the knowledge needed to confidently monitor, interpret and respond to KATA alerts.

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
Digital Forensics		
<ul style="list-style-type: none">• Introduction to Digital Forensics• Live response and evidence acquisition• Windows registry internals• Windows artifacts analysis• Browsers forensics• Email analysis	5 days	<ul style="list-style-type: none">• Build a Digital Forensics lab• Collect digital evidence and deal with it properly• Reconstruct an incident and use time stamps• Find traces of intrusion based on artifacts in Windows OS• Find and analyze browser and email history• Be able to apply with the tools and instruments of digital forensics
Malware Analysis & Reverse Engineering		
<ul style="list-style-type: none">• Malware Analysis & Reverse Engineering goals and techniques• Windows internals, executable files, x86 assembler• Basic static analysis techniques (strings extracting, import analysis,• PE entry points at a glance, automatic unpacking, etc.)• Basic dynamic analysis techniques (debugging, monitoring tools, traffic interception, etc.)• .NET, Visual Basic, Win64 files analysis• Script and non-PE analysis techniques (Batch files; Autoit; Python; Jscript; JavaScript; VBS)	5 days	<ul style="list-style-type: none">• Build a secure environment for malware analysis: deploy sandbox and all necessary tools• Understand principles of Windows program execution• Unpack, debug and analyze malicious object, identify its functions• Detect malicious sites through script malware analysis• Conduct express malware analysis
Advanced Digital Forensics		
<ul style="list-style-type: none">• Deep Windows Forensics• Data recovery• Network and cloud forensics• Memory forensics• Timeline analysis• Real world targeted attack forensics practice	5 days	<ul style="list-style-type: none">• Be able to perform deep file system analysis• Be able to recover deleted files• Be able to analyze network traffic• Reveal malicious activities from dumps• Reconstruct the incident timeline
Advanced Malware Analysis & Reverse Engineering		
<ul style="list-style-type: none">• Malware Analysis & Reverse Engineering goals and techniques• Advanced static analysis techniques (Analysing shellcode statically, parsing PE header, TEb, PEB, loading functions by different hash algorithms)• Advanced dynamic analysis techniques (PE structure, manual and advanced unpacking, unpacking malicious packers that store the full executable in an encrypted form)• APT reverse engineering (cover an APT attack scenario, starting from phishing email and going as in-depth as possible)• Protocol analysis (analyse encrypted C2 communication protocol, how to decrypt traffic)• Rootkits and Bootkits analysis (debugging the boot sector using Ida and VMWare, Kernel debugging using 2 virtual machines, analysing Rootkit samples)	5 days	<ul style="list-style-type: none">• Be able to follow best practices in reverse engineering while recognizing anti-reverse engineering tricks (obfuscation, antidebugging)• Be able to apply advanced malware analysis for Rootkits/Bootkits dissection• Be able to analyze exploit shellcode embedded in the different file types and non-Windows malware

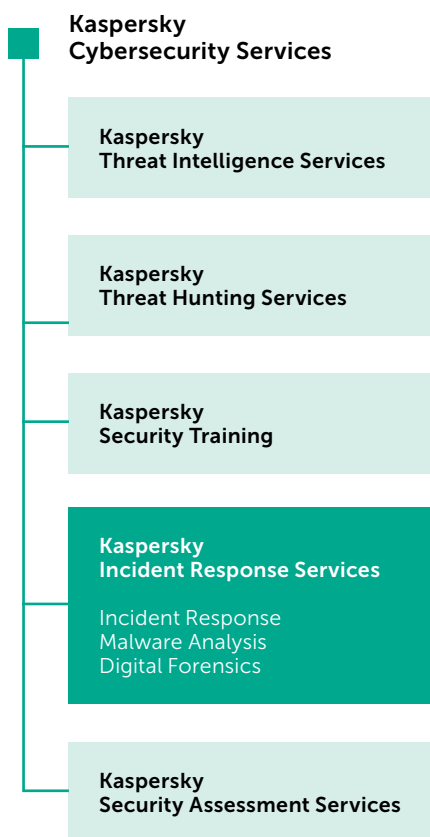
Program Description

Topics	Duration	Skills gained
Incident Response		
<ul style="list-style-type: none"> • Introduction to Incident Response • Detection and primary analysis • Digital analysis • Creating of detection rules (YARA, Snort, Bro) 	5 days	<ul style="list-style-type: none"> • Differentiate APTs from other threats • Understand various attackers' techniques and targeted attack anatomy • Apply specific methods of monitoring and detection • Follow incident response workflow • Reconstruct incident chronology and logic • Create detection rules and reporting
Yara		
<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Create effective Yara rules • Test Yara rules • Improve them to the point where they find threats that nobody else does
KATA Administration		
<ul style="list-style-type: none"> • Common Solution Deployment Scenarios and Server Locations • Sizing Considerations • Licensing Model • Sandbox Server • Central Node • Sensor • Integration with Infrastructure • Installation of Endpoint Sensor • Adding a License and Updating Databases • Solution Operation Algorithm 	1 day	<ul style="list-style-type: none"> • Design the implementation plan fitted to a customer's environment • Install and setup all the KATA components • Maintain and monitor the solution
KATA Security Analyst		
<ul style="list-style-type: none"> • KATA alerts interpretation • Detection and analysis technologies explanation • Scoring and risk engines explanation 	1 day	<ul style="list-style-type: none"> • Understand how scoring works and how it's used by risk engines • Be able to confidently monitor, interpret and respond to KATA alerts

Kaspersky Incident Response Services

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.



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 Lab'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 Lab'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 Lab 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 Lab 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 Lab'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 Services

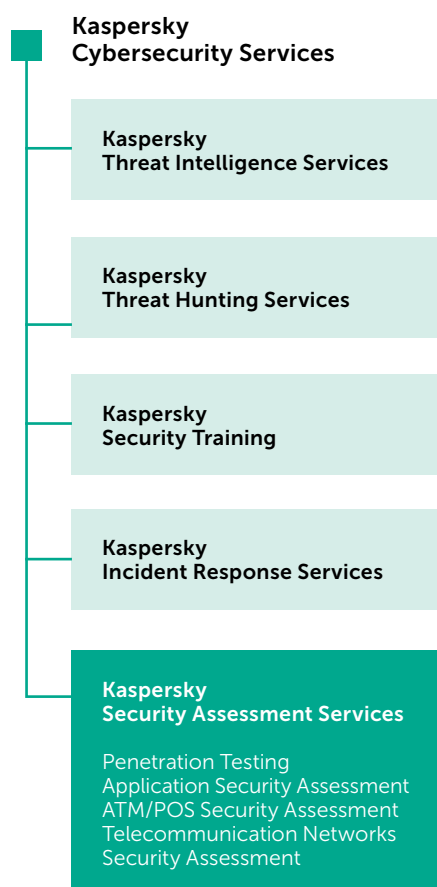
Security Assessment Services from Kaspersky Lab are the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

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
- Application security Assessment
- ATM/POS Security Assessment
- Telecommunication Networks 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 Lab'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 Lab 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 Lab's approach to penetration testing

While penetration testing emulates genuine hacker attacks, these tests are tightly controlled; performed by Kaspersky Lab 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.

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 Lab'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 Lab 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

Results

Vulnerabilities which may be identified by Kaspersky Lab Application Security Assessment services include:

- 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.

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.

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

About Kaspersky Lab's Approach To Application Security Assessment

Security assessments of applications are performed by Kaspersky Lab 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 Lab help you to recognize the security flaws in your ATM/POS devices, and to mitigate the risk of being compromised.

ATM/POS Security Assessment is comprehensive analysis of your ATMs and/or POS devices, designed to identify vulnerabilities that can be used by attackers for activities like unauthorized cash withdrawal, performing unauthorized transactions, obtaining your clients' payment card data, or initiating denial of service. This service will uncover any vulnerabilities in your ATM/POS infrastructure that are exploitable by different forms of attack, outline the possible consequences of exploitation, evaluate the effectiveness of your existing security measures, and help you plan further actions to fix detected flaws and improve your security.

Service benefits

ATM/POS Security Assessment by Kaspersky Lab 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 which attackers could exploit.
- **Comply with government, industry or internal corporate standards**, which stipulate the carrying out of security assessments, e.g. PCI DSS (Payment Card Industry Data Security Standard).

Service scope

The service includes comprehensive ATM/POS analysis, including fuzzing and attack demonstrations in a test environment. This can be provided 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.

ATM/POS Security Assessment Results

The ATM/POS Security Assessment service may be expected to identify a range of vulnerabilities, including:

- Vulnerabilities in network architecture and insufficient network protection.
- Vulnerabilities which enable an attacker to escape kiosk-mode and obtain unauthorized access to the OS.
- Vulnerabilities in third-party security software, allowing potential attackers to bypass security controls.
- Insufficient input and output device protection (card reader, dispenser unit, etc.) including vulnerabilities in device communications, which can allow the interception and modification of transferred data.
- Vulnerabilities caused by errors in application code or resulting from using outdated hardware and software versions (buffer overflows, code injections, etc.)
- Information disclosure.

Once the assessment is concluded, you will receive a report containing both detailed technical information on the testing process, results, vulnerabilities and recommendations, and a straightforward executive summary outlining our conclusions based on the testing results and illustrating the various attack vectors. Additionally, videos of attack demonstrations and presentations for your technical team or top management can be provided if required.

Kaspersky Lab's Approach To ATM/POS Security Assessment

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. The service is performed by experienced Kaspersky Lab security experts who will pay particular attention to the confidentiality, integrity and availability of your systems, in strict adherence with international law and best practices. If we discover a new vulnerability in a customer ATM/POS, we are committed to following a responsible disclosure policy, notifying the vendor and providing consultative help to prepare a fix.

Kaspersky Lab provides ATM/POS Security Assessments in accordance with the following international standards and best practices:

- Payment Card Industry standards
 - Data Security Standard
 - Payment Application Data Security Standard
 - PIN Transaction Security
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Common Vulnerability Scoring System (CVSS)
- Other standards applicable to specific business models and geographical locations, as required.

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 (like Black Hat).

Telecommunication Networks Security Assessment

Services Overview

IT infrastructure of a telecommunication company comprises a number of interconnected networks based on various functions and technologies. These typically include a corporate network including management elements, a core radio network (GSM/UMTS/LTE), providing broadband Internet Access to subscribers, dedicated high-speed trunk channels, hosting and cloud services. Each part of this infrastructure is critical to the business, and should be well protected from hacker attacks if financial, operational and reputational risk is to be minimized. Kaspersky Lab's services for telecommunication networks allow you reduce these risks by recognizing the vulnerabilities in your systems and either removing them or remediating their effects through introducing controls.

Kaspersky Lab offers the following security assessment services for telecommunication networks:

- IT Infrastructure Penetration Testing
- IT Infrastructure Configuration Security Assessment
- Security Assessment for GSM/UMTS/LTE Networks
- Application Security Assessment (for applications providing various services: IP-TV, client self-service portals etc.)

- VoIP Security Assessment
- Telecommunications Equipment Security Assessment

Services Outcome

As a result of each security assessment, you will receive both technical and high-level views of security flaws in your telecommunication networks, as well as conclusions on the effectiveness of your security controls. These results can be used to enhance the security of the network, and this mitigate the financial, operational and reputational risks associated with information security threats.

The report will contain the following information:

- High-level conclusions on the current security levels of your telecommunication networks
- Descriptions of the service methodology and process.
- Detailed descriptions of detected vulnerabilities, including the severity level, exploitation complexity, possible impact on the vulnerable system, and evidence of the vulnerability existence (where possible).
- Recommendations on vulnerability elimination, including changes in configuration, updates, changing source codes, or implementing compensatory controls where elimination of the vulnerability is impossible

Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.com

© 2017 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

