kaspersky

Kaspersky®
Threat Intelligence

Kaspersky Threat Intelligence Services

Table of Contents

Kaspersky Value Proposition....4
Digital Footprint Intelligence....5
Executive Summary....5
Service Benefits....6
Service Description....6
Country-Specific Threat Intelligence Reporting....9
Executive Summary....9
Service Benefits....9
Service Description....10
APT Intelligence Reporting....11
Executive Summary....11
Service Benefits....11
Service Description....11
Delivery....12
Ask the Analyst....13
Executive Summary....13
Service Benefits....13
Service Description....13
Service Delivery....14
APT C&C Tracking....15
Executive Summary....15
Service Benefits....15
Service Description....15
Delivery....16
Financial Intelligence Reporting....17
Executive Summary....17
Service Benefits....17
Service Description....18
Delivery....18
ICS Threat Intelligence Reporting....19
Executive Summary....19
Service Benefits....19
Exclusive....19
Actionable....19
Complete....19
Easy to use....20
Service Description....20

Delivery 21
Kaspersky Threat Lookup 22
Executive Summary 22
Service Benefits 22
Service Description 23
Kaspersky Cloud Sandbox 24
Executive Summary 24
Service Benefits 24
Service Description 24
Kaspersky Research Sandbox 25
Executive Summary 25
Service Benefits 25
Service Description 26
Kaspersky Threat Attribution Engine 26
Executive Summary 26
Service Benefits 26
Service Description 27
Kaspersky Threat Data Feeds 28
Executive Summary 28
Service Benefits 28
Service Description 29
Delivery 29
Integration with Third-party Solutions 29
CyberTrace 30
Kaspersky Security Trainings 33
Executive Summary 33
Service Benefits 33
Service Description 33
Malware Analysis & Reverse Engineering 33
Advanced Malware Analysis & Reverse Engineering 34
Digital Forensics 35
Advanced Digital Forensics 36
Incident response 37
Efficient Threat Detection with Yara 38
Requirements for the room 38

Kaspersky Value Proposition

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them.

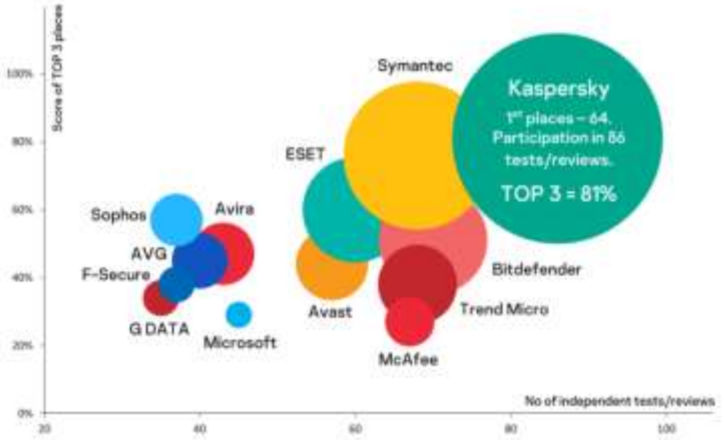
We are one of the world's fastest-growing cybersecurity companies and the largest one that is privately-owned. With a holding registered in the United Kingdom, we operate in 200 countries and territories and have 35 offices in 31 countries. Over 4,000 highly-qualified specialists work for Kaspersky.

Kaspersky utilizes advanced threats analysis, vulnerability research, forensics and investigations to help customers to protect their online services and reputation. It works together with the global IT security community, international organizations, national and regional law enforcement agencies (e.g. INTERPOL, Europol, Microsoft Digital Crimes Unit, The National High-Tech Crime Unit (NHTCU) of the Netherlands' Police Agency and The City of London Police), as well as Computer Emergency Response Teams (CERTs) worldwide. During investigations, Kaspersky's security experts provide technical expertise and focus their research on analysing malware.

Kaspersky has supported INTERPOL's launch of a new Digital Forensics Laboratory as part of the Digital Crime Centre at the Global Complex for Innovation (IGCI) in Singapore. The Digital Forensics Laboratory is responsible for carrying out the technical part of INTERPOL's investigations into cyber-incidents. It uses cutting-edge techniques and software to analyse malware, identifying and presenting evidence of illegal actions to help prosecute criminals.

Kaspersky also takes part in joint cyber threat investigations with companies and organizations including Adobe, AlienVault Labs, Dell SecureWorks, CrowdStrike, OpenDNS Security Research Team, GoDaddy Network Abuse Department, Seculert, SurfNET, Kyrus Tech Inc. and Honeynet Project.

Most Tested. Most Awarded. Kaspersky Protection.*



In 2019 Kaspersky products participated in 86 independent tests and reviews. Our products were awarded 64 firsts and achieved 70 top-three finishes.

MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION
*kaspersky.com/top3

* Notes:
- According to summary results of independent tests in 2019 for corporate, consumer and mobile products.
- Summary includes independent tests conducted by: AV-Comparatives, AV-TEST, SE Labs, ICSA Labs, NSS Labs, MRG Effitas, Virus Bulletin, PCSL.
- Tests performed in these programs assess all protection technologies against known, unknown and advanced threats.
- The size of the bubble reflects the number of 1st places achieved.

www.kaspersky.com/top3

Digital Footprint Intelligence

Executive Summary

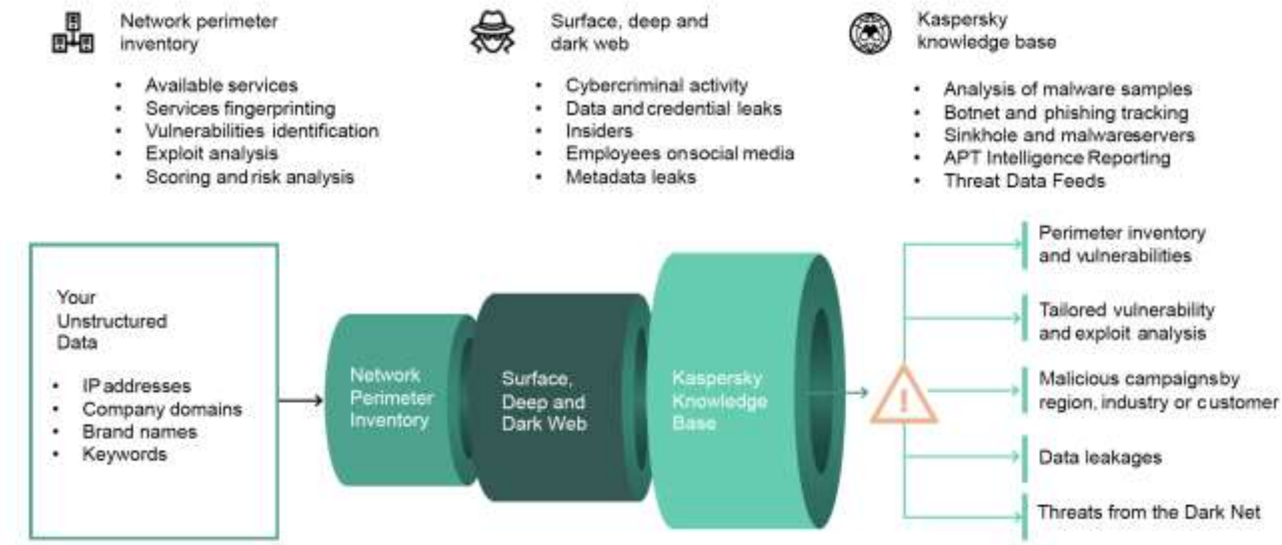
Kaspersky proposes **Digital Footprint Intelligence** service for the Customer, including the following works:

Network Reconnaissance and Vulnerability Analysis – open-source intelligence (OSINT) semi-passive methods are used at this stage; that is only methods that appear like normal Internet traffic and behavior: WHOIS, inactive analysis of public Internet sites, requests to search engines, DNS requests, etc. Among others, centralized resources to detect available network services and their versions based on port scanning periodically performed by these services (such as Shodan, censys.io, scans.io) are used. The experts also will use specialized tools for massive information gathering (like Maltego), and provide identification of services versions and analysis of potential vulnerabilities based on publicly available information.

Malware and Cyber-Attack Tracking Analysis – multiple Kaspersky internal resources are used for monitoring and tracking of actions of various malware (including ones used by cyber-criminals for sophisticated fraud), cyber-criminal and cyber-espionage campaigns. The following resources will be analyzed: Kaspersky Security Network (KSN) containing about a petabyte of malicious and potentially malicious samples, a botnet tracking system used to monitor botnet activities, Passive DNS records, as well as C&C sinkholes for certain malware. Records on IP addresses and domain names of victims of advance persistent threat (APT) sophisticated malware will be analyzed separately to detect the Customer's resources if any.

Data Leakage and Underground Activities Analysis – the Service Provider analyzes dumps of compromised accounts that became publicly available as a result of various breaches, as well as compromised data available on various hacker forums of limited access. Information on deals on underground forums will be checked for presence of the Customer's resources, clients or employees. In particular, we can reveal attempts to hire insiders, as well as malicious insiders trying to sell access or data, discussions about attack plans, or opened bounties (rewards) for compromising your company.

Threat analysis and report preparation. At this stage the Service Provider analyze threats actual for the Customer, and prepares a report containing description of threat intelligence results and recommendations on further remediation actions.


Network perimeter inventory
Available services
Services fingerprinting
Vulnerabilities identification
Exploit analysis
Scoring and risk analysis
Surface, deep and dark web
Cybercriminal activity
Data and credential leaks
Insiders
Employees onsocial media
Metadata leaks
Kaspersky knowledge base
Analysis of malware samples
Botnet and phishing tracking
Sinkhole and malwareservers
APT Intelligence Reporting
Threat Data Feeds
Your Unstructured Data
IP addresses
Company domains
Brand names
Keywords
Network Perimeter Inventory
Surface, Deep and Dark Web
Kaspersky Knowledge Base
Perimeter inventory and vulnerabilities
Tailored vulnerability and exploit analysis
Malicious campaignsby region, industry or customer
Data leakages
Threats from the Dark Net

Knowing about the weakest spots and having recommendations from Kaspersky will allow you to fix the vulnerabilities and avoid possible negative impact on system from cybercriminal attacks or insiders.

Digital Footprint Intelligence service 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.

Service Benefits

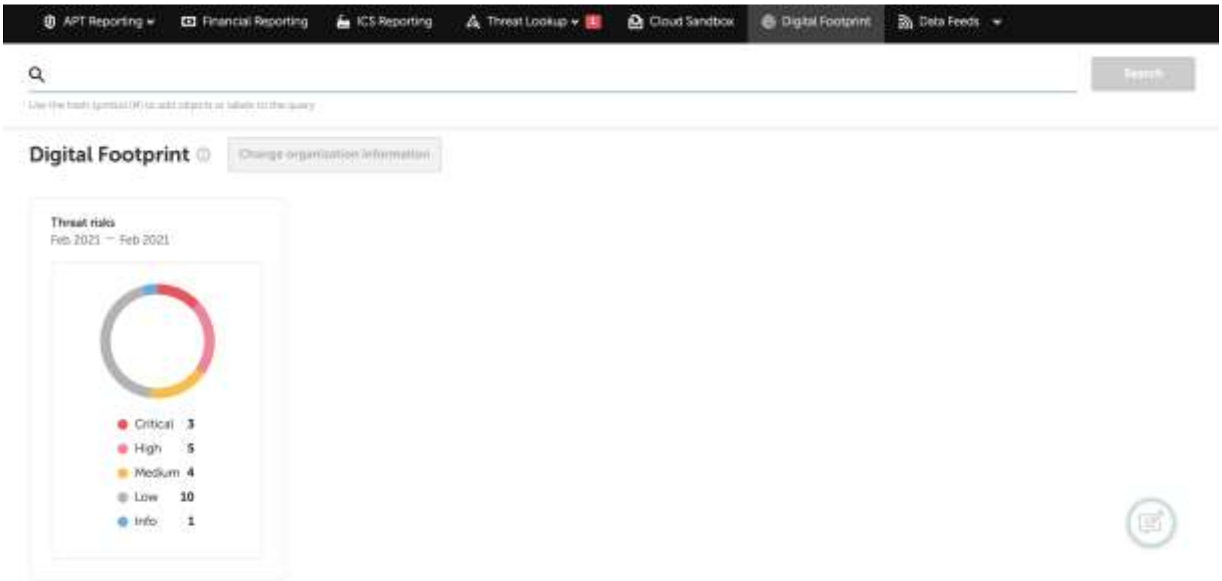
Digital Footprint Intelligence helps to recognize the best way to mount an attack against the organization, identify routes and information, which is available to an attacker specifically targeting the Customer and more. Our experts piece together a comprehensive picture of your current attack status, identifying weak-spots ripe for exploitation, and revealing evidence of past, present and planned attacks.

Service Description

Service is available in Threat Intelligence Portal and provides notifications about detected vulnerabilities that may reduce the level of protection of your organization.

Threat notifications may include information about compromised credentials, data leakages, vulnerable services on the network perimeter, insider threats, and many more.

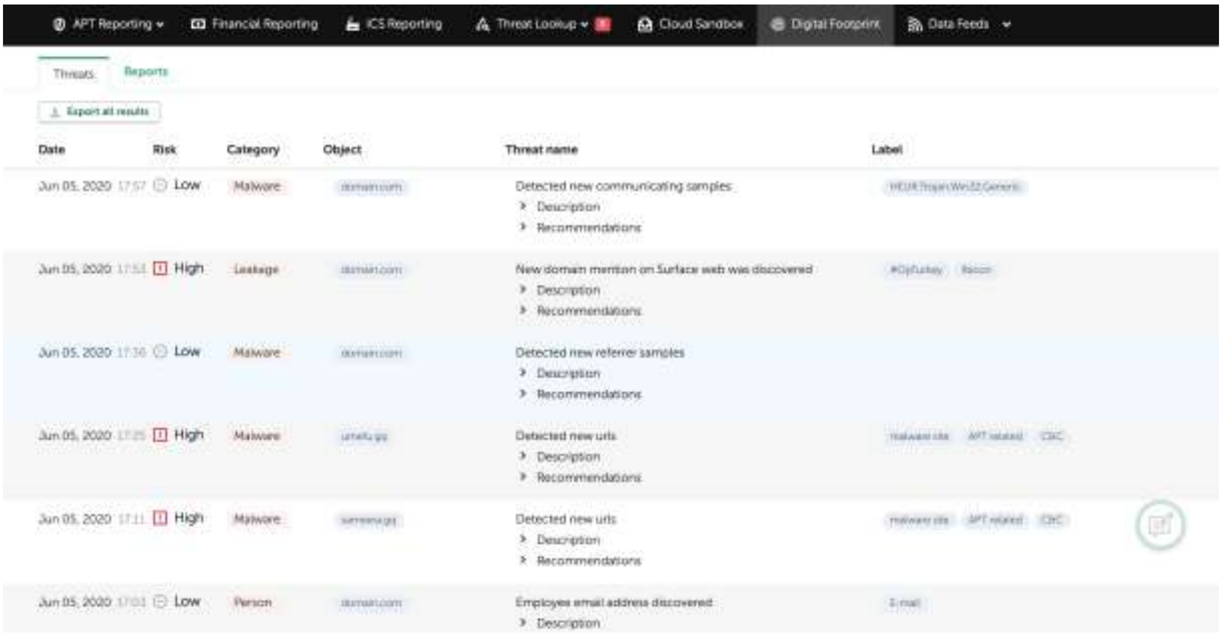
Threat notifications are displayed on the **Threats** tab of the **Digital Footprint page**. The **Threat risks circle** chart represents the total number of the detected vulnerabilities and their danger level (*Critical, High, Medium, Low, Info*).



For each notification, the following data is displayed:

- **Date**. Date and time when the threat was detected.
- **Risk**. Danger level of the detected threat (Critical, High, Medium, Low, Info).
- **Category**. Category of the threat, for example *vulnerability, malware, person, leakage, darknet.* Other threat categories may also appear.
- **Object**. Object associated with the detected threat (domain, IP address, keyword).
- **Threat name.** Description of the threat and recommendations on how to mitigate risks associated with this threat. You can expand or collapse the description and recommendations for better viewing.
- **Label**. Labels associated with the threat (for example, threat name according to the Kaspersky classification, Common Vulnerabilities and Exposures (CVE), or keywords).

You can export notifications on **Threat tab** into CSV format.



Date	Risk	Category	Object	Threat name	Label
Jun 05, 2020 17:57	Low	Malware	domain.com	Detected new communicating samples Description Recommendations	HEUR:Trojan.Win32.Generic
Jun 05, 2020 17:53	High	Leakage	domain.com	New domain mention on Surface web was discovered Description Recommendations	#OpTurkey #anon
Jun 05, 2020 17:36	Low	Malware	domain.com	Detected new referrer samples Description Recommendations	
Jun 05, 2020 17:25	High	Malware	[illegible]	Detected new urls Description Recommendations	malware site APT related C&C
Jun 05, 2020 17:11	High	Malware	[illegible]	Detected new urls Description Recommendations	malware site APT related C&C
Jun 05, 2020 17:03	Low	Person	domain.com	Employee email address discovered Description	E-mail

In addition to notifications, each quarter the Customer will obtain a report containing description of actual notable threats related to the Customer, as well as additional information on detailed technical analysis results. Reports are delivered via threat intelligence portal. Each report includes the following information:

- **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, which are potential targets for attack.
- **Malware and cyberattack 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 your organization.
- **Information leakage.** Through discreet monitoring of underground online forums and communities, Kaspersky experts discover whether hackers are discussing attack plans with your organization in mind or, for example, if an unscrupulous employee is trading information.
- **Current attack status.** APT attacks can continue undetected for many years. If a current attack affecting your organization's infrastructure is detected, Kaspersky experts provide advice on effective remediation.

For each Digital Footprint Intelligence report, Kaspersky Threat Intelligence Portal displays the following information:

- **Date.** Date when the Digital Footprint Intelligence report was added.
- **Report name.** Digital Footprint Intelligence report name. For each Digital Footprint Intelligence report, a brief description is available.
- **Time interval.** Time interval for which the Digital Footprint Intelligence report was generated (quarter, by default).

Any user of the group that has access to the **Digital Footprint Intelligence service** can view current information about the organization. To update information about the organization, additional rights must be granted to the user. Kaspersky experts can also view and, if necessary, edit information. The information about the organization is updated in Kaspersky Threat Intelligence Portal only after a Kaspersky expert's approval. Before the approval, the user that updated organization information can view both the current and edited versions. Right after the Kaspersky expert approves the changes, only updated information is available for all users.

Kaspersky experts use the following information in the research:

- Domains and subdomains
- Network (CIDR or range)
- IP addresses
- Keywords related to the organization brand or product name
- Names of subsidiaries

You can also provide any additional information that can help to improve research.

Make sure the information you provide does not include personal data.

If you receive information on resources that are not relevant to your organization, you can specify these resources in the **The following data is explicitly excluded from the research** field (see the procedure below). Before adding a resource to the list of excluded ones, check the information about the organization that was provided earlier and make sure that other users in your organization did not request information about this resource.

Country-Specific Threat Intelligence Reporting

Executive Summary

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. Kaspersky Enterprise Cybersecurity 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.

Created using approaches ranging from Open Source Intelligence (OSINT) to deep analysis of Kaspersky 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 – multiple Kaspersky internal resources are used for monitoring and tracking of actions of various malware (including ones used by cyber-criminals for sophisticated fraud), cyber-criminal and cyber-espionage campaigns. The following resources will be analyzed: Kaspersky Security Network (KSN) containing about a petabyte of malicious and potentially malicious samples, a botnet tracking system used to monitor botnet activities, Passive DNS records, as well as C&C sinkholes for certain malware. Records on IP addresses and domain names of victims of advance persistent threat (APT) sophisticated malware will be analyzed separately to detect the Customer's resources if any.

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.

Service Benefits

Country-Specific Threat Intelligence Reporting helps to recognize the best way to mount an attack against the organization, identify routes and information, which is available to an attacker specifically targeting the Customer and more. 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.

Service Description

Under **Country-Specific Threat Intelligence Reporting Service**, each quarter the Customer will obtain a report containing description of actual notable threats related to the Customers Country and industry, as well as additional information on detailed technical analysis results. Reports are delivered via encrypted email messages. Each report includes the following information:

- **Executive summary –** brief description of the revealed vulnerabilities, threats, traces of compromise, as well as current cybercriminal and cyberespionage activity against the Customer's assets.
- **Detailed description** – in-depth analysis of the threat intelligence data, description of potential vulnerabilities, possible attack sources, information on malware targeting your organization (if any), leaked confidential documents, underground forums data analysis, etc.
- **Remediation recommendations** – the report will suggest steps to mitigate consequences of the critical vulnerabilities or ongoing cyber-attacks and protect your resources from actual security threats

If Kaspersky will find any critical information the Customer will be notified immediately.

APT Intelligence Reporting

Executive Summary

APT Intelligence Reporting will swift up Information and Intelligence. As a matter of fact, intelligence cannot be produced without a deep knowledge of all parts involved, including the receiver of the information. However, the industry might be going too far when sharing terabytes of information without any context is considered intelligence.

Our vision is different. Our deep knowledge in the field of APT research can be proven by our research during the last years, which includes Duqu, Carbanak, The Flame, Careto or Equation Group. All of them belong to the selected group of **World´s class APT research**.

Based on this continuous research of more than **100** different APT groups operating at this moment, we share context and **actionable** information **immediately**. Our focus is to provide actionable information using Indicators of Compromise in different open standards and Yara rules, and we serve it while it's hot. That´s why we will share every time we see any new relevant activity.

We also believe that human analysts are still the most valuable asset in any APT investigation, and that´s why we always include context information about the investigation, as well as C-level executive summary for abridged dissemination of the report.

Service Benefits

Benefits associated with the use of our actionable intelligence:

Exclusive access to technical description of cutting-edge threats during the ongoing investigation before public release.

Quick start: no additional infrastructure is required to start using the service

Technical support of investigation: subscription includes access to technical artifacts supporting the investigations such as Indicators of compromise (IOC's).

Support of industrial standards: IOCs provided in industrial-grade formats, such as OpenIOC, STIX, YARA rules.

Retrospective analysis: access to all previously issued private reports is provided during subscription.

Continuous monitoring of APT campaign: access to actionable intelligence during the investigation (information on APT distribution, IOC, C&C infrastructure).

Insight of non-public APT: not all high-profile threats are subject to public notification. Some of them due victim's impact, vulnerability fixing process or law enforcement activity are not public. Not every single investigation gets public – but they are available to our customers[1].

Early response to APT: information and tools provided in reports makes it possible to quickly respond to new threats and vulnerabilities, to block the attacks via known vectors and to reduce the damage caused by advanced attacks.

Service Description

APT intelligence reporting will provide early notification reports on new APT campaigns as well as updates on active threats. Reports include the following information:

[1] Except of sensitive information on the victims

Executive summary – brief description of threat, timeline, geographic distribution and generic features.

Detailed description – in-depth analysis of the threat intelligence data: kill chain overview, attack methods, exploits used, malware description, C&C infrastructure and protocols description, victims' analysis, data exfiltration analysis.

Conclusions and recommendations.

Appendix - Technical analysis, IOC, C&C, hashes, and any other available information.

Delivery

Repository of reports available as web-portal with filtering via industry, geolocation and actor's information. Information available for customer to access: reports themselves, indicators of compromise, YARA-Rules, Appendixes.

Ask the Analyst

Executive Summary

To further enhance cybersecurity posture, we are pleased to offer Kaspersky Ask the Analyst service tailored to offer heightened intelligence and awareness in high profile cyberespionage campaigns on top of aforementioned APT intelligence reporting service.

Threat intelligence sharing is in the root of the security strategy of any entity. Indeed, there is a common consensus of the importance of sharing as one of the few effective ways in effectively combating against advanced actors, allowing to gain deep knowledge of the modus operandi of their operations.

Common use cases for Ask the Analyst service:

- The Customer needs further clarification on an APT report
- The Customer needs additional intelligence on top of already provided IoC's
- The Customer detected unusual activity and need assistance in identifying if it is related to an APT actor

This service allows access to a core group of researches within Kaspersky and is offered on a case-by-case basis to customers who have mature cybersecurity environment in place.

Service Benefits

Benefits associated with the use of our actionable intelligence:

- **Exclusive access** to technical experts that will help to understand and answer to all question related to APT reports or ongoing research.
- **Additional intelligence:** clarification regarding published reports, threat intelligence support or additional information about certain indicators
- **Early response**: information and tools provided by our experts make it possible to timely respond to new threats and vulnerabilities, to block the attacks via known vectors and to reduce the damage caused by advanced attacks.

PLEASE NOTE **Ask the Analyst service** is an additional tool to support requests from customers who need to obtain more information on published reports and ongoing research. It provides direct access to our research analysts and is not to be used for incident response/forensic analysis. The service does handle urgent requests and does not provide customized reports.

Service Description

Scope of Work:

- The scope of work includes 5 requests from the customer side during a period of 12 months since the activation of the service (engagement is limited to a total of 10 hours which can be extended by Kaspersky)
- If the customer does not use all 5 requests for a period of 12 months since the beginning of the service agreement, they expire
- Kaspersky to provide clarification on published reports, threat intelligence support or additional information about certain indicators, analysis of customer submitted malware/suspected Sample(s) or other indicators via secure medium (pgp/rar+pw), enabling the launch of an inquiry

- If needed, Kaspersky can request additional information (such as but not limited to, timeframe, targets, hashes, IOCs, additional filenames and details related to the attack) from customer to support the investigation
- In situations when Kaspersky don't have enough information to fulfill the request, or Kaspersky don´t have an internal ongoing investigation relevant to your request, or if the customer cannot provide necessary background information in order to conduct an inquiry, we will communicate to you that request cannot be completed and will not account this request against the number of requests you purchased in scope of this service
- The name of the Customer shall never be used in any potential APT reports where data from the Customer might be used

Service Delivery

- To submit a request, you need to send email to the following address intelreports@kaspersky.com. Email subject should be in the following format: [Company name] Ask the Analyst request #: {Subject}. Example: [Company name] Ask the Analyst request 1: Clarification about APT report *{Report name}.* If possible please attach you public PGP key to secure further communication.
- For each request, Kaspersky commits on providing a complete answer by email. If necessary and agreed, a conference call and/or screen sharing can be established
- Upon acceptance of enquiry by us, we will inform you of the hours (including delivery of the request) that it will take to handle the request
- Our aim is to provide you with responses in a timely manner, we do not provide strict SLAs for the service due to the nature of the team handling this service. We reserve the right to provide the service is on 8 hours a day, 5 business days per week basis with response from Kaspersky within 48 hours
- The service is provided in English through a dedicated email address
- Updates on the progress will be shared with the customer on demand
- Once the answer is delivered and all related questions are answered, investigation case is closed.

APT C&C Tracking

Executive Summary

APT C&C Tracking Service delivers IP addresses of infrastructure connected to advanced threats. This helps security analysts working in CERTs, National SOCs, and National Security Agencies monitoring the deployment of new malware, so that they can take the required measures to mitigate ongoing and upcoming attacks.

The service is updated daily with recent findings of Kaspersky Global Research and Analysis Team who have a proven track record in discovering APT campaigns across the world. For each IP address, there is a name of an APT group, operation, or malware it is associated with, Internet service provider, and autonomous system, collection of associated IP addresses hosting information, and dates when this was first and last seen.

The IP addresses can be downloaded in a machine-readable format, so customers can upload it to existing security solutions to automate detection.

Service Benefits

APT C&C Tracking tracks active APT-related C&C worldwide and provides daily feeds (dumps of active C&C's) for a particular country or for countries throughout the world.

This service is designed to:

- Identify active APT-related C&C in a particular country
- Get information about country's security posture related to APT C&C pervasion
- Enable accelerating Incident Response and Threat Hunting activities in regions
- Enable accelerating Incident Response and Threat Hunting activities related to ISPs services
- Enable attributing attacks to known APT actors

Service Description

Service is available on **Threat Intelligence Portal.**

For each IP address, the following information is displayed on the **Active feed tab**:

IP address. Detected IP address. The items are clickable and take you to the **Threat Lookup**[2] page, where you can search for information about the IP address.

First seen. Date when the IP address was first detected by the Kaspersky experts.

Last seen. Date when the IP address was last detected by the Kaspersky experts.

Domain. Domain that resolves to the detected IP address. Items are clickable and take you to the Threat Lookup page, where you can search for information about the domain.

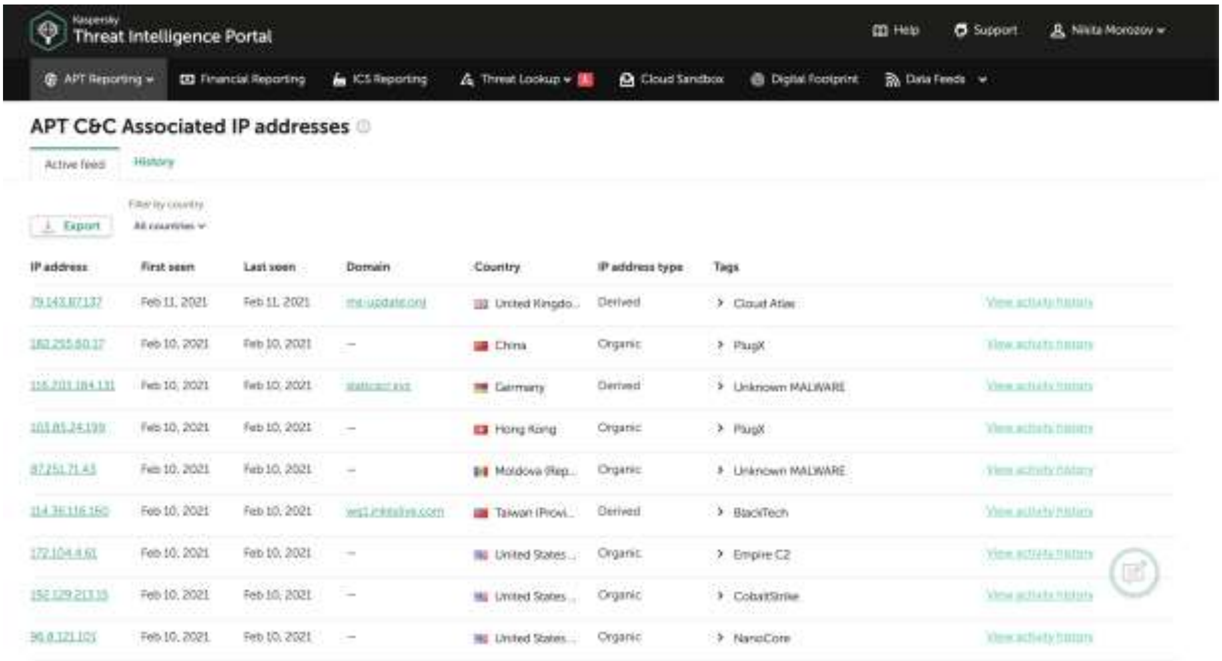
Country. Country that the detected IP address belongs to.

IP address type. Type of the detected IP address (for example, Derived or Organic).

[2] Threat Lookup license should be purchased separately.

Tags. Tags associated with the detected IP address. For certain IP addresses, a brief description is available.

On the **History** tab, the activity periods for the IP addresses are displayed. You can filter IP addresses by country, or specify the time period of the activity by using predefined filters (**Day, Week, Month, All)** or the **Custom** filter (calendar).



APT C&C Associated IP addresses

Filter by country
All countries

IP address	First seen	Last seen	Domain	Country	IP address type	Tags	
79.143.87.137	Feb 11, 2021	Feb 11, 2021	ms-update.org	United Kingdo...	Derived	Cloud Atlas	View activity history
182.255.60.17	Feb 10, 2021	Feb 10, 2021	–	China	Organic	PlugX	View activity history
116.203.184.131	Feb 10, 2021	Feb 10, 2021	statcast.xyz	Germany	Derived	Unknown MALWARE	View activity history
103.85.24.159	Feb 10, 2021	Feb 10, 2021	–	Hong Kong	Organic	PlugX	View activity history
87.251.71.43	Feb 10, 2021	Feb 10, 2021	–	Moldova (Rep...	Organic	Unknown MALWARE	View activity history
114.36.116.160	Feb 10, 2021	Feb 10, 2021	wg1.inkeslive.com	Taiwan (Provi...	Derived	BlackTech	View activity history
172.104.4.61	Feb 10, 2021	Feb 10, 2021	–	United States ...	Organic	Empire C2	View activity history
152.129.213.15	Feb 10, 2021	Feb 10, 2021	–	United States ...	Organic	CobaltStrike	View activity history
96.8.121.101	Feb 10, 2021	Feb 10, 2021	–	United States ...	Organic	NanoCore	View activity history

Delivery

Service is available as separate tab on Threat Intelligence Portal. Information From the portal can be obtained via web-interface or using RESTful API.

Information from the portal can be downloaded in the following formats:

- CSV archive (.zip)
- JSON archive (.zip)

Financial Intelligence Reporting

Executive Summary

Financial Threat Intelligence Reporting will provide the Customer heightened intelligence and awareness in high profile cyberespionage campaigns. In addition to using the reports to learn, detect and mitigate risks posed by new attack techniques, big campaigns or recently-developed malware, many organizations leverage them for private research purposes, to detect the described threats or to further enhance their security strategy.

Threat intelligence sharing is in the root of the security strategy of any entity. Indeed, there is a common consensus of the importance of sharing as one of the few effective ways in effectively combating against advanced actors, allowing to gain deep knowledge of the modus operandi of their operations.

The current problem many companies are facing is mixing up Information and Intelligence. As a matter of fact, intelligence in essence cannot be produced without a deep knowledge of all parts involved, including the receiver of the information. However, the industry might be going too far when sharing terabytes of information without any context is considered intelligence.

Our vision is different. We have a deep knowledge in the field of APT and Financial Institution related attacks research as can be stated by our research during the last years, which includes Duqu, Carbanak, The Flame, Careto or Equation Group. All of them belong to the selected group of World´s class APT research.

We also believe that human analysts are still the most valuable asset in any investigation, and that´s why we always include context information about the investigation, as well as C-level executive summary for quick dissemination of the report.

Service Benefits

Benefits associated with the use of our actionable intelligence:

Exclusive access to technical description of cutting edge threats during the ongoing investigation before public release.

Quick start: no additional infrastructure is required to start using the service

Technical support of investigation: subscription includes access to technical artifacts supporting the investigations such as Indicators of compromise (IOC's).

Support of industrial standards: IOCs provided in industrial-grade formats, such as OpenIOC, STIX, YARA rules.

Retrospective analysis: access to all previously issued private reports is provided during subscription.

Continuous monitoring of cybercriminals campaigns: access to actionable intelligence during the investigation (information on attacks distribution, IOC, C&C infrastructure).

Insight of non-public attacks: not all high profile threats are subject to public notification. Some of them due victim's impact, vulnerability fixing process or law enforcement activity are not public. Not every single investigation gets public – but they are available to our customers[3].

Early response to attacks: information and tools provided in reports makes it possible to quickly respond to new threats and vulnerabilities, to block the attacks via known vectors and to reduce the damage caused by advanced attacks.

[3] Except of sensitive information on the victims

Service Description

Financial Intelligence reporting will provide early notification reports on new fraud campaigns as well as updates on active threats. Reports include the following information:

Executive summary – brief description of threat, timeline, geographic distribution and generic features.

Detailed description – in-depth analysis of the threat intelligence data: kill chain overview, attack methods, exploits used, malware description, C&C infrastructure and protocols description, victim's analysis, data exfiltration analysis.

Conclusions and recommendations.

Appendix - Technical analysis, IOC, C&C, hashes, and any other available information.

Delivery

Repository of reports available as web-portal with filtering via industry, geolocation and actor's information. Information available for downloading: reports itself, indicators of compromise, YARA-Rules, Appendixes.

ICS Threat Intelligence Reporting

Executive Summary

The **Kaspersky ICS Threat Intelligence Reporting** Service provides the customer with in-depth intelligence and greater awareness of malicious campaigns targeting industrial organizations, as well as information on vulnerabilities found in the most popular industrial control systems and underlying technologies. Reports are delivered via a web-based portal, which means you can start using the service immediately.

Within the subscription you will get access to the following report types:

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

Threat landscape. Reports on significant changes to the threat landscape for industrial control systems, newly discovered critical factors affecting ICS security levels and ICS exposure to threats, including regional, country- and industry-specific information.

Vulnerabilities found. Reports on vulnerabilities identified by Kaspersky in the most popular products used in industrial control systems, the industrial internet of things, and infrastructures in various industries.

Vulnerability analysis and mitigation. Our advisories provide well-thought actionable recommendations from Kaspersky experts to identify and mitigate vulnerabilities in your infrastructure.

Service Benefits

Exclusive

Insight into non-public information: as a cybersecurity professional you get information that might be essential for planning and performing cybersecurity activities, but which is not publicly available due to responsible disclosure policies.

Early access to technical information on threats while research and investigation is still ongoing, and before information is made public.

Exclusive access to information that may never be released into the public domain due to the risk of malicious actors abusing it (does not include software sent exclusively to vendors to demonstrate vulnerabilities).

Actionable

Early response to emerging threats: the information and tools provided allow you to quickly respond to new threats and vulnerabilities, to mitigate risks associated with advanced attacks and those that use known vectors.

Technical support for ICS operations: the subscription includes access to technical artifacts, such as indicators of compromise (IOCs) that can be integrated into a customer's automated tools and used to support vulnerability assessment, incident detection, response and investigation activities.

Complete

Retrospective analysis: access to all previously released private reports during the subscription period.

Continuous malicious campaign monitoring: access to actionable intelligence during an investigation and updates on new findings, including TTP changes and IOCs of newly detected toolsets.

Easy to use

Automation: report information can be automatically parsed and integrated into automated cybersecurity processes.

Support for multiple industrial standards: IOCs are provided in industrial-grade formats, such as OpenIOC, STIX, YARA and SNORT rules.

Service Description

You can use **ICS Threat Intelligence reports** to:

Detect and prevent reported threats to safeguard critical assets, including software and hardware components and to ensure safety and continuity of technological process.

Correlate malicious and suspicious activity you detect in industrial environments with Kaspersky's research results to attribute your detection to the reported malicious campaigns, identify threats and promptly respond to incidents.

Perform a vulnerability assessment of your industrial environments and assets based on accurate assessments of vulnerability scope and severity and make informed decisions on patch management or the implementation of the other preventative measures we recommend.

Leverage information on attack technologies, tactics and procedures, recently discovered vulnerabilities and other important threat landscape changes we report to:

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

Reports contains the following information:

- **Executive summary:**
  - {Threat urgency} / {vulnerability severity} assessment
  - Threat / vulnerability description
  - Timeline
  - Distribution across regions, countries and industries
  - Recommendations on risk mitigation
- **Detailed description of analysis results**
- **For reports on threats:**
  - Attack methods
  - Exploits used (if any)
  - Malware description(s)
  - C&C infrastructure and protocol descriptions
  - Victim analysis
  - Data exfiltration analysis

  - Attribution
- **For reports on vulnerabilities:**
  - Public availability of exploits
  - Signs of exploitation in real-world attacks
  - Methodology used to identify the vulnerability
  - Technical analysis of security issues that made it possible to exploit the vulnerability
  - Possible attack vectors (possibly in conjunction with other vulnerabilities and security flaws)
  - Evaluation of products / product versions affected
  - Estimates of vulnerable product distribution across regions / countries / industries
- **Conclusions**
- **Appendix**
  - Technical analysis, important IOCs and any additional relevant information.

Delivery

Repository of reports available as web-portal with filtering via industry, geolocation and actor's information. Information available for customer to access: reports themselves, indicators of compromise, YARA-Rules, Appendixes.

Kaspersky Threat Lookup

Executive Summary

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 affect 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, etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.

Trusted Intelligence: A key attribute of Kaspersky Threat Lookup is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky 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.

High levels of Real Time Coverage: Threat intelligence is automatically generated in Real Time, based on findings across the globe (thanks to Kaspersky Security Network providing visibility to a significant percentage of all internet traffic and all types of data, covering tens of millions of end-users in more than 213 countries) providing high coverage and accuracy.

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.

Rich Data: Threat intelligence delivered by Kaspersky Threat Lookup covers a huge range of different data types including hashes, URLs, IPs, whois, pDNS, GeoIP, file attributes, statistical and behavior data, download chains, timestamps and much more. Empowered with this data, you can survey the diverse landscape of security threats you are facing.

Continuous Availability: Threat intelligence is generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability and consistent performance.

Continuous Review by Security Experts: 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.

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. Sandbox functionality will be available in November 2017.

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.

Service 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 the specific threats your organization faces.

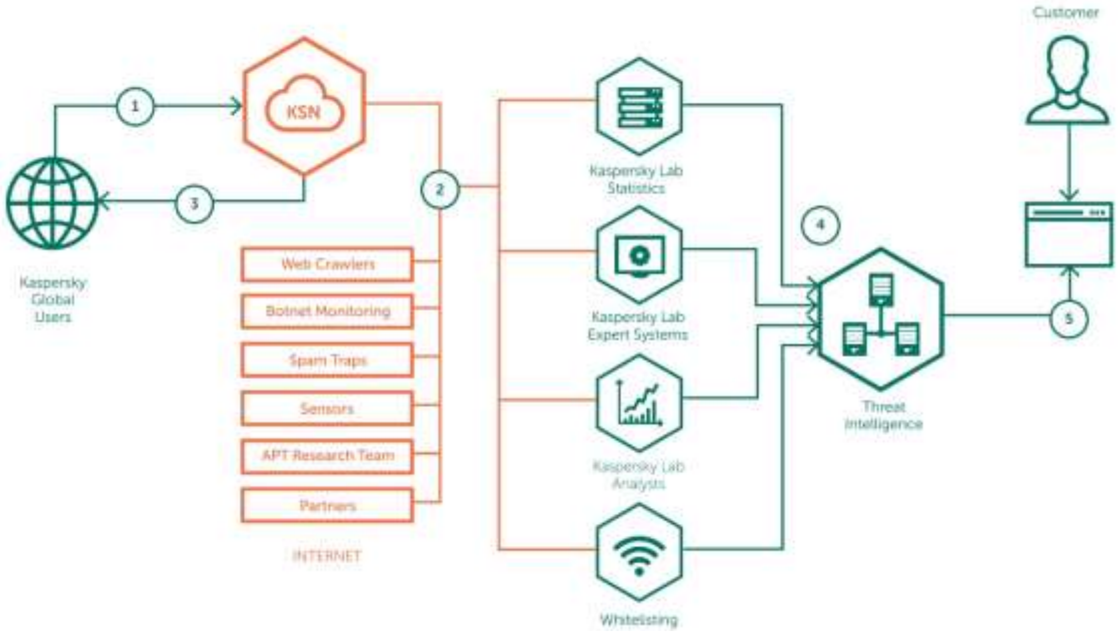
Service Description

With access to **Kaspersky Threat Lookup** service, 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.

Threat Intelligence Sources:

Threat intelligence is aggregated from a fusion of heterogeneous and highly reliable sources, including the Kaspersky Security Network (KSN) and our own web crawlers, our Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams, partners and other historical data about malicious objects collected by Kaspersky over almost 2 decades. Then, in Real Time, all aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky Expert Systems (sandboxes, heuristics engines, similarity tools, behavior profiling etc.), analyst validation and whitelisting verification.



Kaspersky Cloud Sandbox

Executive Summary

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.

Service Benefits

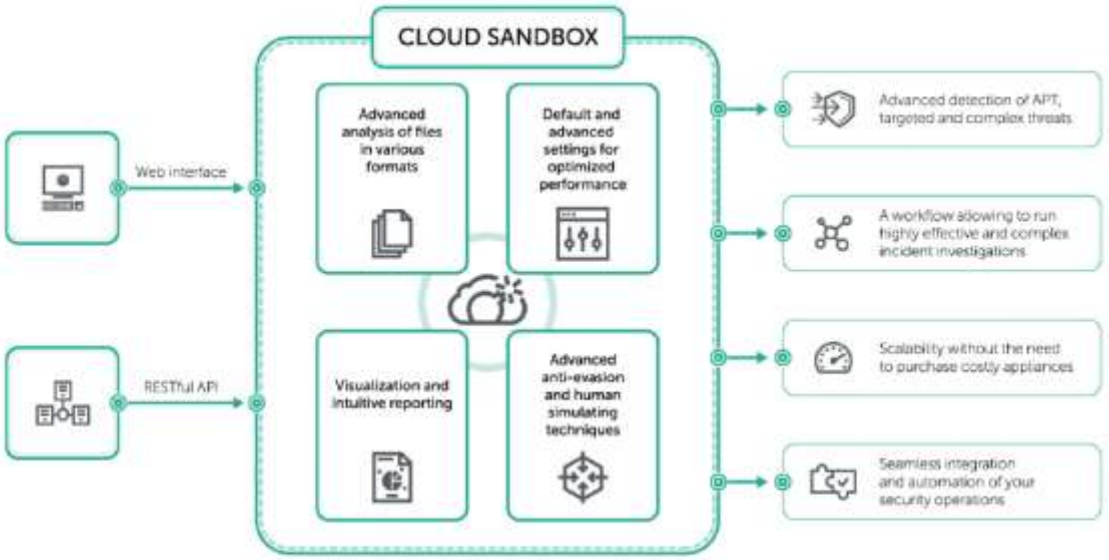
- Advanced detection of APTs, targeted and complex threats
- A workflow allowing the running of highly effective and complex incident investigations
- Scalability without the need to purchase costly appliances or worry about system resources
- Seamless integration and automation of your security operations

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

Service Description

As part of our Threat intelligence Portal, Kaspersky Cloud Sandbox is the final component that completes your threat intelligence workflow. While the portal 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.


CLOUD SANDBOX
Web interface
RESTful API
Advanced analysis of files in various formats
Default and advanced settings for optimized performance
Visualization and intuitive reporting
Advanced anti-evasion and human simulating techniques
Advanced detection of APT, targeted and complex threats
A workflow allowing to run highly effective and complex incident investigations
Scalability without the need to purchase costly appliances
Seamless integration and automation of your security operations

Delivery

Service is accessible via web-based portal and RESTful API.

Kaspersky Research Sandbox

Executive Summary

Kaspersky Research Sandbox has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over a decade. It incorporates all the knowledge about malware behaviors acquired by Kaspersky throughout our continuous threat research, allowing us to detect 350 000+ new malicious objects every day. Deployed on-premises, this powerful technology also prevents exposure of data outside the organization.

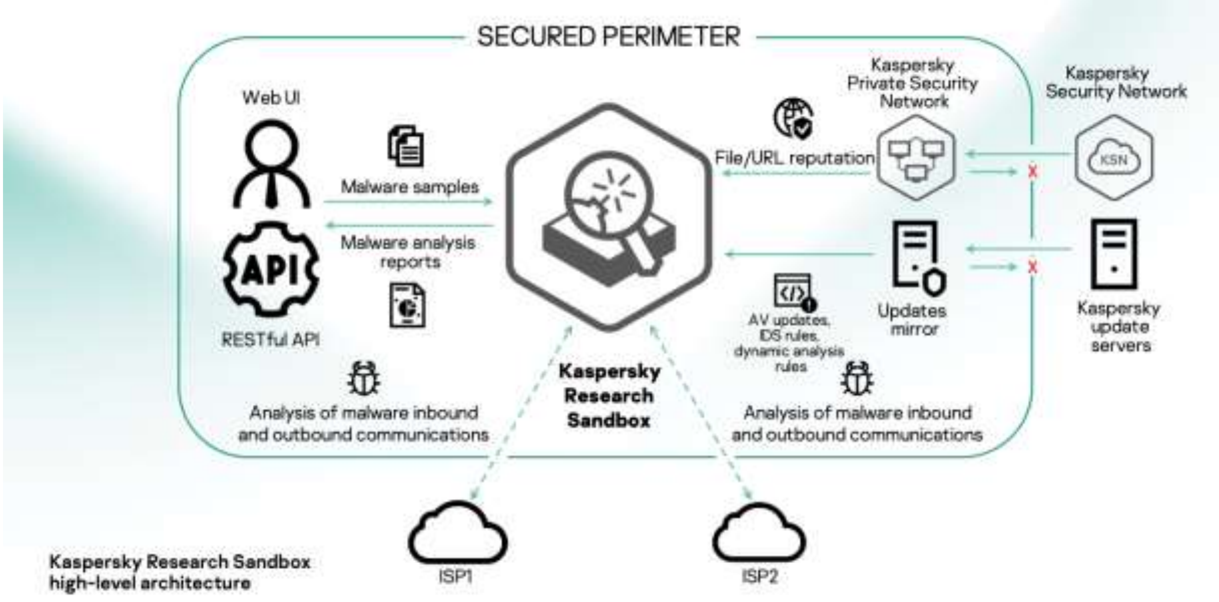
It offers a hybrid approach, combining behavioral analysis, and rock-solid anti-evasion, with human-simulating technologies. Kaspersky Research Sandbox also allows to customize images of the systems for analysis tailoring them to real environments, which increases the accuracy of threat detection and the speed of investigation.

Service Benefits

- On-premises deployment makes sure no data is exposed outside the organization
- Supports the analysis of more than a hundred file types
- Advanced anti-evasion techniques
- User activity emulation
- Custom images allowing to analyze threats across a range of operating systems and applications and only those that apply to real environments
- Separate analysis of each process to detect suspicious activities with associated network connections
- Detailed analysis reports, including all system activities, extracted files, network activities (PCAP) and visual graphs
- Supports integration with Kaspersky Private Security Network
- Manual file submission and RESTful API for seamless integration and automation of your security operations

Service Description

The diagram below describes the high-level architecture of Kaspersky Research Sandbox.


SECURED PERIMETER
Web UI
Malware samples
Malware analysis reports
API
RESTful API
Analysis of malware inbound and outbound communications
Kaspersky Research Sandbox
Kaspersky Private Security Network
File/URL reputation
Updates mirror
AV updates, IDS rules, dynamic analysis rules
Analysis of malware inbound and outbound communications
Kaspersky Security Network
KSN
Kaspersky update servers
ISP1
ISP2

Kaspersky Research Sandbox high-level architecture

Delivery

On-premises deployment

Kaspersky Threat Attribution Engine

Executive Summary

Kaspersky Threat Attribution Engine incorporates the database of APT malware samples and clean files gathered by Kaspersky experts for the last 22 years. We track 600+ threat actors and campaigns with 120+ APT Intelligence Reports released every year. Our ongoing research supports the actuality of the large APT collection which contains 60K+ files. It improves the false flags detection and make the attribution as much accurate as possible using the automated tools.

The product enables the unique approach for comparing samples for their similarity while ensuring zero false positive rates. It can quickly link a new attack to known APT malware, previous targeted attacks and hacker groups, helping to see the high-risk threat among less serious incidents and take timely protective measures to prevent an attacker from gaining a foothold in the system.

Service Benefits

- Provides instant access to a repository of curated data about hundreds of APT actors and samples
- Allows efficient automated or manual threat prioritization and alert triage
- Functionality to add private actors and samples, educating the product to detect samples that are similar to files in your private collection
- Manual sample upload and open API for integration with automated workflows
- Can be deployed in a secure, air-gapped environment to protect your systems and data as well as meeting any compliance requirements

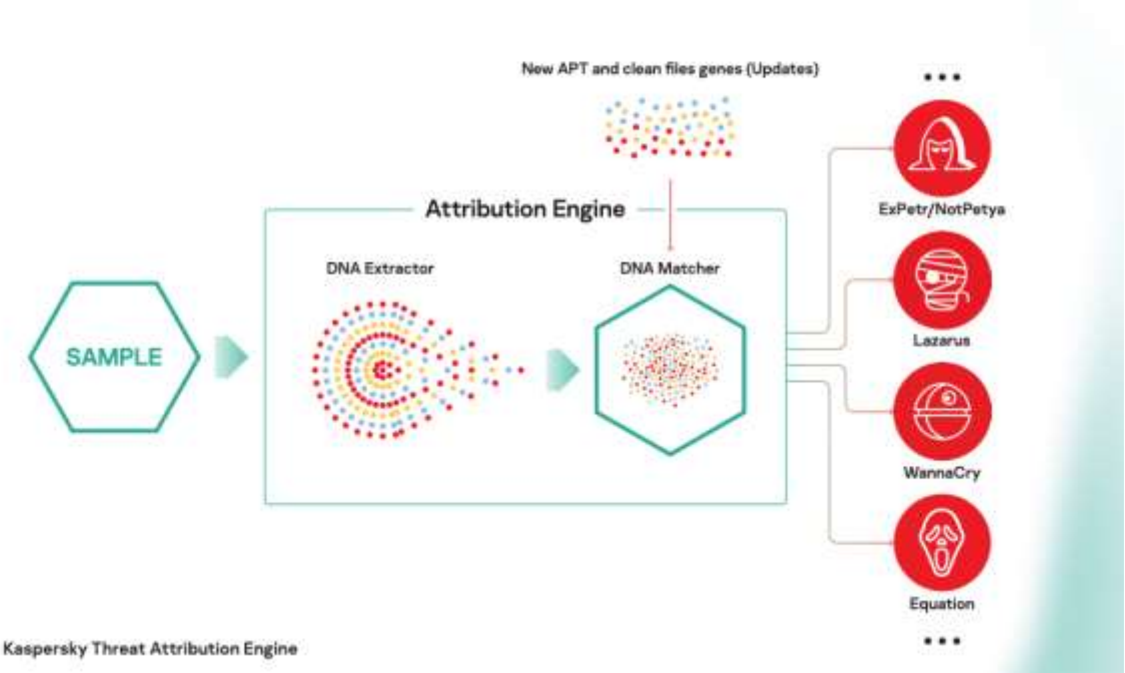
- Maintains absolute privacy and confidentiality of all submissions to avoid exposing sensitive information

Service Description

Kaspersky Threat Attribution Engine analyzes the “genetics” of malware looking for code similarity with previously investigated APT samples and linked actors in an automated way. It compares the “genes”, i.e. small binary pieces of the decomposed files, with the APT malware samples database and provides a report on malware origin, threat actors and file similarity with known APT samples. Moreover, the product allows security teams to add private actors and objects to its database and educate the product to detect samples that are similar to files in your private collection. With the Threat Attribution Engine the attribution process only takes seconds comparing to the years it was required in the past.

Kaspersky Threat Attribution Engine extracts relevant “genes” that meet certain criteria and calculates the sample’s reputation score. It reveals the sample’s genotype and code attribution, providing you with insights into the malware’s origin and its possible authors.

The product can be deployed in a secure, air-gapped environment restricting any 3rd party from accessing the processed information and submitted objects. There is an API interface to connect the Engine to other tools and frameworks in order to implement attribution into existing infrastructure and automated processes.



Delivery

On-premises deployment.

Detailed information about the related APT actor can be found in Kaspersky APT Intelligence reports. 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. A subscription to Kaspersky APT Intelligence Reporting needs to be purchased separately.

Kaspersky Threat Data Feeds

Executive Summary

Malware families and variations have grown exponentially in recent years. Kaspersky currently detects about 325,000 unique malware samples daily, and these malicious samples are growing in complexity as well as in volume.

To protect their IT-infrastructure from all these new threats, most enterprises already deploy protection measures including anti-malware solutions, intrusion prevention and threat detection systems. Kaspersky Intelligence Data Feeds have a crucial role in a comprehensive multi-layered defense strategy, continuously providing essential security information to in-house SIEM (Security Information and Event Management) systems.

This service is designed for use by any enterprise organization planning to control the presence of malware at infrastructure level leveraging existing SIEM solution via integration with KL Threat Data Feeds. Using superior global intelligence, security operation centers are armed to combat the latest cybercrime techniques, which are designed to bypass even the most sophisticated protection. Combined with local intelligence data, this global information can help protect the enterprise IT-infrastructure.

Kaspersky Intelligence Data Feeds are highly flexible and can be provided in different formats, allowing easy integration into different third-party cybersecurity solutions, including HP ArcSight, IBM QRadar, Splunk, RSA and LogRhythm SIEMs or popular Threat Intelligence Platforms – Anomali, EclecticIQ, Threat Connect, Threat Quotient.

Service Benefits

Intelligence Feed databases are updated regularly with the latest findings from the Kaspersky Security Network. In its turn, this global cloud database is fed in real time by data from over 100 million participating Kaspersky software users worldwide, as well as the organization's own experts.

Kaspersky Intelligence Data Feeds give customers an additional level of malware defense. The distribution of malicious objects can be controlled at infrastructure level by comparing data from the log files coming from the SIEM systems with the data from KL Threat Data Feeds. In case of detection the SIEM admin can receive notifications about this incident that helps additionally prevent malware infection within the organization.

Key values:

- Deep 20+ year expertise, one of the most advanced and recognized AV vendor with the highest DR in the industry
- Huge coverage – 100M+ KSN users
- Diversified sources to collect, analyze and refine TI (KSN, botfarm, whitelists, deep/dark web, GREAT team, actor's tracking,…)
- Not only IP addresses, but
- URLs – best for matching against web proxies
- Hashes – best for matching against DLP and AV logs
- Only fresh and actual data

- One of the industry's lowest FPR
- We store more data than our competitors (over 30B of files or over 20PB of data) to analyze and build relationships. More than 10B of our observables (files (20B+), URLs and domains (10B+), IPs (500M+)) have relationship data.
- Rich context
- Ready-made integration package for SIEMs/TIPs
- Premium feeds based on APT/Financial Reports
- We cover all worldwide cyber threats, do not hide even Russian based
- Dedicated Technical Account Manager to assist with the integration

Service Description

Threat Data Feeds provide comprehensive information about Threats that the organization should block:

- **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; • Mobile Malicious Hash Feed – supporting the detection of malicious objects that infect mobile Android and iPhone platforms;
- **Whitelisting Data Feed** – providing third-party solutions and services with a systematic knowledge of legitimate software.
- **Kaspersky Transforms for Maltego** – providing Maltego users with a set of transforms that give access to Kaspersky Threat Data Feeds. Kaspersky Transforms for Maltego allows you to check URLs, hashes, and IP addresses against the feeds from Kaspersky. The transforms can determine the category of an object as well as provide actionable context about it.

Delivery

Threat Intelligence Feeds can be delivered via HTTPs protocol in JSON format. Convertors to STIX, Open IoC and CSV are available.

Integration with Third-party Solutions

Kaspersky Threat Intelligence Data Feeds are designed to integrate with third-party SIEM systems including HP ArcSight, IBM QRadar, Splunk, RSA and LogRhythm SIEMs and many others.

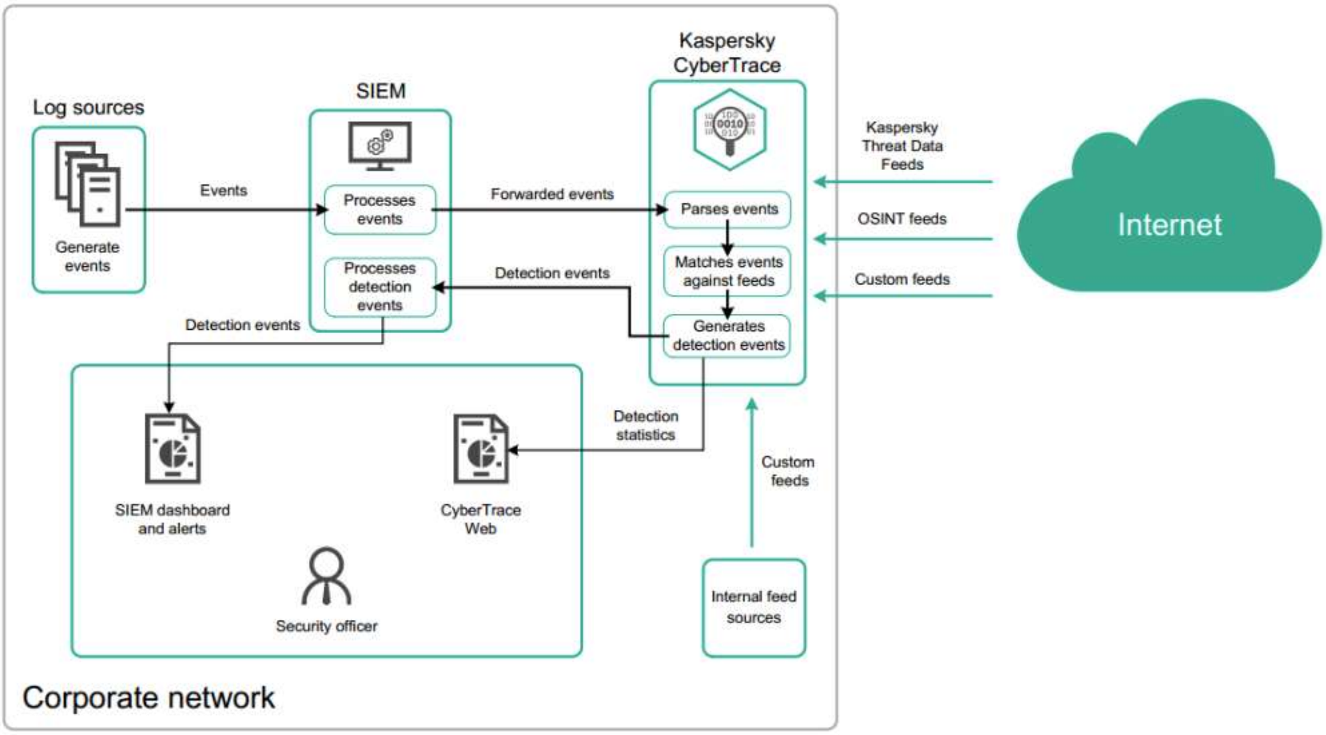
Integration with popular Threat Intelligence Platforms (Anomali, EclecticIQ Threat Connect, Threat Quotient) also available.

CyberTrace

Kaspersky CyberTrace is a threat intelligence fusion and analysis tool that integrates threat data feeds with SIEM solutions so that users can immediately leverage threat intelligence for security monitoring and IR activities in their existing security operations workflow.

Kaspersky CyberTrace uses continuously updated threat data feeds to identify existing breaches or newly launched attacks, and to inform your business or clients about the risks and implications associated with the threat.

Kaspersky CyberTrace integrates with threat intelligence sources (threat intelligence feeds from Kaspersky, other vendors, OSINT, or even custom sources), SIEM solutions, and log sources. As indicators of compromise (IoC) from the threat intelligence feeds are found in your environment, Kaspersky CyberTrace automatically sends alerts to SIEM solutions for ongoing monitoring, validation, and discovery of additional contextual evidence for ongoing security incidents. Kaspersky CyberTrace provides analysts with a set of instruments for conducting alert triage and response through categorization and assessment of identified matches.



Features of Kaspersky CyberTrace:

- Automatic high-performance matching of incoming logs and events with Kaspersky Threat Data Feeds, OSINT feeds, or any other custom feeds in the most popular formats (JSON, STIX, XML, CSV). Demo feeds from Kaspersky and OSINT are available out of the box.
- Internalized process of parsing and matching incoming data significantly reduces SIEM solution load. Kaspersky CyberTrace parses incoming logs and events, matches the resulting data to feeds, and generates its own alerts on threat detection. Consequently, a SIEM solution has to process less data.
- Generates feed usage statistics for measuring the effectiveness of feeds.

- In-depth threat investigation by means of on-demand search of indicators (hashes, IP addresses, domains, URLs). Bulk scanning of logs and files is also supported.

- Universal approach to integration of threat matching capabilities with SIEM solutions and other security controls. SIEM connectors for a wide range of SIEM solutions can be used to visualize and manage data about threat detections.

- IoC and related context are efficiently stored in RAM for rapid access and filtering.

- Kaspersky CyberTrace Web, a web user interface for Kaspersky CyberTrace, provides data visualization, on-demand IoC search functionality, and access to Kaspersky CyberTrace configuration. Kaspersky CyberTrace Web also supports the management of feeds, log parsing rules, black lists and white lists, and event sources.

- Command-line interface for Windows and Linux platforms.

- Advanced filtering for feeds and log events. Feeds can be converted and filtered based on a broad set of criteria such as time, popularity, geographical location, and threat type. Log events can be filtered based on custom conditions.

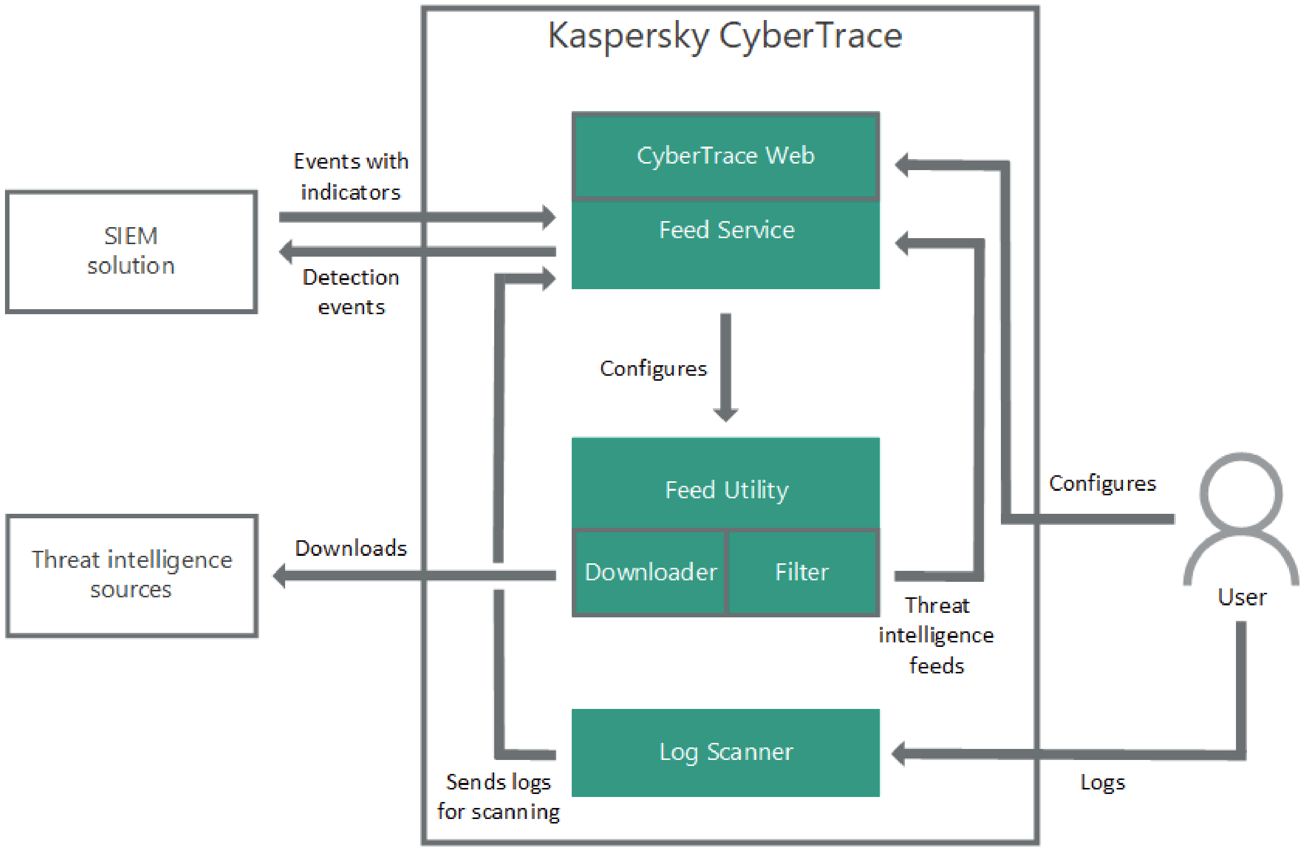
- DMZ integration support. The computer on which event data is matched against feeds can be located in DMZ and isolated from the Internet.

- In standalone mode, where Kaspersky CyberTrace is not integrated with a SIEM solution, Kaspersky CyberTrace receives logs from various sources such as networking devices, processes these logs according to the defined normalizing rules, and parses the logs according to the defined regular expressions.

- Export lookup results that match feeds to CSV format for integration with other systems (firewalls, network and host IDS, custom tools).

- Exposes obfuscation techniques used by some threats to hide malicious activities in logs.

The main parts of Kaspersky CyberTrace are Feed Service, Feed Utility, Log Scanner, and Kaspersky CyberTrace Web.


Kaspersky CyberTrace
CyberTrace Web
Feed Service
Configures
Feed Utility
Downloader
Filter
Log Scanner
SIEM solution
Events with indicators
Detection events
Threat intelligence sources
Downloads
Sends logs for scanning
Threat intelligence feeds
Configures
User
Logs

Kaspersky Security Trainings

Executive Summary

Cybersecurity awareness and education are now critical requirements for enterprises faced with an increasing volume of constantly evolving threats. Security employees need to be skilled in the advanced security techniques that form a key component of effective enterprise threat management and mitigation strategies.

Kaspersky Cybersecurity Education program has been developed specifically for any organization looking to promote the role of cybersecurity in order to better protect its infrastructure and intellectual property. The program offers a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert.

Service Benefits

Different customers may find themselves benefiting in different ways:

- Enterprises (banks, Telco's, airlines, hotel chains, etc.) By raising level, the expertise amongst their own IT security employees, costs associated with outsourcing incident response, digital forensics and malware analysis services can be avoided, and reaction times to security incidents shortened.
- MSSPs can leverage the knowledge and experience gained from the courses, adding additional value to their own IT security services.

Law enforcement agencies can also leverage knowledge and experience gained from the courses to prepare their own security staff to fight cybercrime more effectively.

Service Description

Kaspersky Cybersecurity Education Program covers everything from security fundamentals to advanced digital forensics and malware analysis, helping customers and their employees to improve their cybersecurity knowledge in five main areas:

- Cybersecurity Fundamentals
- Digital Forensics and Incident Response
- Malware Analysis & Reverse Engineering
- Incident Response
- YARA Training

Malware Analysis & Reverse Engineering

This five-day training is dedicated to the basics of reverse engineering. Some previous programming experience is crucial for the students. They don't have to be professional programmers, but our experience shows that for students with system administration or penetration testing expertise assembly language part of the training is hard due to lack of analogies in their previous experience.

Through the course they would face PE files, compiled with Microsoft Visual Studio, .NET samples, standalone and embedded shellcodes. Students would get the experience of IDA Pro: reading disassembler listing, recognize common algorithms, library functions and malware tricks inside it, adding standard and custom data structures, correlate static analysis and dynamic one in debugger. As a result of these five days students get the initial real-life experience of malware analysis and recommendations how organize their further grow as reverse engineers.

Topics covered

- 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

Class requirements

Level: medium

Prerequisites for students:

- Basic understanding of x86 and x86_64 assembly, Python
- Basic knowledge of C/C++
- Basic experience with analyzing code in IDA Pro

Some previous programming experience is crucial for the students. They don’t have to be professional programmers, but our experience shows that for students with system administration or penetration testing expertise assembly language part of the training is hard due to lack of analogies in their previous experience

Room: limited to max 15 participants

Hardware & Software requirements:

- Laptop with VMWare / VirtualBox virtualization solution (x64 machine with virtualization support, 8 GB Ram, 60 GB free space on disk)
- Internet connection
- Free or full version of IDA Pro

Duration: 5 days

Advanced Malware Analysis & Reverse Engineering

This 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. The course material is based on many years of experience analyzing the most complex threats ever discovered in-the-wild, including: Equation, Red October, Sofacy, Turla, Duqu, Carbanak, ShadowPad, and many more. It’s time to set your static analysis game to God-Mode.

Topics covered

- 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)

Class requirements

Level: advanced

Prerequisites for students:

- Solid understanding of x86 and x86_64 assembly, Python
- Basic knowledge of C/C++
- Experience with analyzing code in IDA Pro

Hardware & Software requirements:

- Laptop with VMWare / VirtualBox virtualization solution
- Legitimate copy of IDA Pro (latest version preferred)
- Working C/C++ compiler toolset: clang, g++, mingw

Duration: 5 days

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.

Topics covered

- Introduction to Digital Forensics
- Live response and evidence acquisition
- Windows registry internals
- Windows artifacts analysis
- Browsers forensics
- Email analysis

Class requirements

Level: medium

Prerequisites for students:

- Be familiar with using Windows and Linux operating environments and be able to troubleshoot general OS connectivity and setup issues.
- Be familiar with VMware and be able to import and configure virtual machines

Hardware & Software requirements:

- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory.
- 8 GB (Gigabytes) of RAM or higher is mandatory.
- USB 2.0 or higher Port(s)

- 100 Gigabytes of Free Space on your System Hard Drive - Free Space on Hard Drive is critical.
- Attendees should have the capability to have Local Administrator Access within their host operating system.
- Internet access in the training location.
- 7Zip, http://www.7-zip.org/
- VMware Workstation version 10 at least, http://www.vmware.com/products/workstation/ If they do not own a licensed copy of VMware Workstation, they can download a free 30-day trial copy from VMware.com.

Duration: 5 days

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.

Topics covered

- 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

Class requirements

Level: advanced

Prerequisites for students:

- Solid experience of using Windows and Linux operating environments and be able to troubleshoot general OS connectivity and setup issues
- Be familiar with VMware and be able to import and configure virtual machines

Hardware & Software requirements:

- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory
- 8 GB (Gigabytes) of RAM or higher is mandatory
- USB 2.0 or higher Port(s)
- 100 Gigabytes of Free Space on your System Hard Drive - Free Space on Hard Drive is critical
- Attendees should have the capability to have Local Administrator Access within their host operating system
- Internet access in the training location
- 7Zip, http://www.7-zip.org/

- VMware Workstation version 10 at least, http://www.vmware.com/products/workstation/ If they do not own a licensed copy of VMware Workstation, they can download a free 30-day trial copy from VMware.com

Duration: 5 days

Incident response

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.

Topics covered

- 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

Class requirements

Level: medium

Prerequisites for students:

- Be familiar with using Windows and Linux operating environments and be able to troubleshoot general OS connectivity and setup issues
- Be familiar with VMware and be able to import and configure virtual machines

Hardware & Software requirements:

- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory for this class
- 16 GB (Gigabytes) of RAM or higher is mandatory for this class
- USB 3.0 port
- 150 Gigabytes of Free Space on the System Hard Drive - Free Space on Hard Drive is critical
- Attendees should have the capability to have Local Administrator Access within their host operating system

- 7Zip, http://www.7-zip.org/
- VMware Workstation 10, http://www.vmware.com/products/workstation/ or higher

Duration: 5 days

Efficient Threat Detection with Yara

Have you ever wondered how Kaspersky discovered some of the world's most famous APT attacks? Now, the answer is within your reach. This training will lead you through one of the essential tools for the APT hunter: the Yara detection engine.

If you've wondered how to master Yara and how to achieve a new level of knowledge in APT detection, mitigation and response, it all breaks down to a couple of secret ingredients. One of them is our private stash of Yara rules for hunting advanced malware.

During this training you will learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats that nobody else does. During the training you will gain access to some of our internal tools and learn how to maximize your knowledge for building effective APT detection strategies with Yara.

Topics covered

- Brief intro into Yara syntax
- Tips & tricks to create fast and effective rules
- Using 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

Class requirements

Level: medium and advanced

Prerequisites for students:

- Knowledge of the Yara language and basic rules

Hardware & Software requirements:

- CPU: 64-bit Intel x64 2.0+ GHz processor or higher-based system is mandatory for this class
- 16 GB (Gigabytes) of RAM or higher is mandatory for this class
- USB 3.0 port

Duration: 2 days

Requirements for the room

- Limited to max 15 participants
- Enough space to come to every student if needed. How many students do we have this time?
- Marker board (preferred) or flip chart to write at, markers. Board big enough to leave comments from previous days as a reminder for the students

- Big screen or projector to show the materials to the students. If projecting on the writable surface is possible - it would be nice. Materials have to be visible to everyone in the room. HDMI interface from the screen/projector to trainer's laptop

SMB share or 3-4 USB sticks to spread the virtual machine among the students. It's about 10 GB.