Threat Intelligence Platform



Kaspersky[®] CyberTrace

Release Notes

About

Kaspersky CyberTrace is a Threat Intelligence Platform that helps analysts make timely and better-informed decisions. Kaspersky CyberTrace uses continuously updated threat data feeds to timely detect cyber threats, prioritize security alerts and effectively respond to information security incidents.

Kaspersky CyberTrace integrates threat intelligence (such as threat intelligence feeds from Kaspersky, other vendors, OSINT, internal Threat Intelligence, or even custom sources) with SIEM solutions and log sources so that users can immediately leverage threat intelligence for security monitoring and IR activities in their existing security operations workflow. If Indicators of Compromise (IoC) from the threat intelligence feeds are found in your environment, Kaspersky CyberTrace automatically sends alerts to your SIEM solutions for monitoring, validation, and uncovering of additional contextual evidence of ongoing security incidents.

Kaspersky CyberTrace provides analysts with a set of instruments for managing Threat Intelligence, conducting alert triage and response, and preventing future attacks.

RELEASE 4.1 FP2

RELEASE DATE: 31.03.2022

OPERATING SYSTEM: WINDOWS AND LINUX

HARDWARE PLATFORM: X86_64

New features:

• Adding CyberTrace indicators and External indicators (observables) to an existing graph from a file.

Deshboard	Search 👸 Retroscan 🙀 Indicators 🛆 Detections	N Graph 📑 Tasks 98 🔘 Settings		11) <u>Heir</u>
🖾 🕹 < 🌣 🕅 🔍 Search in grap				
	Add indica	tors to the graph		
	Manually From files			
		3		
		Drag & drop to upload		
		Browse		
	You can ac up to 128	d indicators of compromise (IoCs) by uploading text files IB in total. Each IoC in the file must be on a separate line.		
		Learn more		
		Create node(s) Cano	el	

Kaspersky CyberTrace displays a message when a certificate is added and there is no Internet connection
or the proxy settings are incorrect.

Import certificate	×	Import certificate	\times
Unable to verify certificate, please check y connection	our internet	Some failure with proxy connection occurred	
	Close	Close	

Change log

- Vulnerability Data Feed is not available for Kaspersky CyberTrace, by default. When Kaspersky CyberTrace is upgraded from 4.1.0 to 4.1.1, Vulnerability Data Feed is removed from the Kaspersky CyberTrace feeds list.
- Changing the path to the log files is removed from the user interface.

Dashboard	ि Retroscan 📓 Indicators	${ \ \ \ \ \ \ \ \ \ \ \ \ \ $	₰ ⁰ Graph	🚰 Tasks 98	දිටු Settings
📑 Service 📰 Feeds 🔗 Ta	ags 🖞 Indicators export []] Matching	ିର୍ Retroscan 🖉	Detections 📡	Events format	段 Users 骨
Logging settings	Specify the log directory in the configuration file kl_feed_service_log.conf.				
Log directory	Learn more				
	0				
Log level					
 None 					
 Error 					
🔿 Info					
-					

- The GET method is used to export indicators; the POST method is no longer available.
- Licensing policy changed: MSSP TIP licenses are now recognized as Enterprise TIP licenses with EPS limit.

Enterprise TIP Expiration date	EPS rate		Number	of indicators	Search	Custom feeds	Multi-user mode	Multitenancy	Indicators export	Graph	Key file
2022-10-01 (227 days left)	Now:	0	Now:	32 528	Yes	Yes	Yes	Yes	Yes	Yes	MSSP_TIP_100000eps.key
	Max:	100 000	Max:	Unlimited							

RELEASE 4.1 FP1

RELEASE DATE: 15.10.2021 OPERATING SYSTEM: WINDOWS AND LINUX

HARDWARE PLATFORM: X86_64

New features:

• Research Graph is introduced. The Graph (also known as Link Analysis) is designed to explore data and detections stored in Kaspersky CyberTrace visually, discover threat commonalities. It allows to graphically visualize relationships between URLs, domains, IPs, files, and other context encountered during investigations. Export of IoCs is also supported to ease importing into security controls. The Graph includes the following features: transformations, group nodes, adding links manually, adding indicators, and searching for nodes in the graph.



- Working with Data Feeds in STIX 2.0/2.1 formats over TAXII 2.0/2.1, respectively, is now supported. Previously, only Data Feeds in JSON, STIX 1.0/1,1, XML, and CSV formats could be added to Kaspersky CyberTrace.
- Ability to tag IoCs is added. Now you can create tags, specify their weight (importance), and use them to tag IoCs manually. You can also sort and filter IoCs based on these tags and their weights. It simplifies management of IoCs groups and their importance.

	Ta	gs Add	tags Crea	ate new tag	Mar	lage all tags				
	То	tal tags weigh	it: 13							
		BFSI 🛿	RUSSIA 😣	KASPERSKY		usa 🛿	IMPO	RTANT AREA		
= (Dashboard	👼 Indicators	∠ _I Detections	∠o Search 🔅	Settings	🖓 Tasks				🖽 Help
In	dicato	rs Add indicator	Mark as false positive	Delete		indicato	r value			Q
	Type ↓	Value 4	Added 4	Changed ↓	Tag			Total tag weight ↓	Suppliers	
	MD5	127E6FBFE24A750E	2019-11-10 20:35	2020-04-01 09:01	BFSI		RSKY +15	13	Kaspersky Malicious H 3.more	
	IP address	93.159.228.40	2019-11-10 20:35	2020-02-29 17:31	No tags			5	Abusech_SSL_Certificate_Bloc	
	IP address	8.8.8.8	2019-11-10 20:35	2020-02-29 17:31	USA			-	Whitelist, Abusech_SSL_Certifi	
	SHA256	127E6FBFE24A750E	2019-11-10 20:35	2020-04-01 09:01	USA		+5	5	Kaspersky Malicious Hash Data	
	IP address	93.159.228.40	2019-11-10 20:35	2020-02-29 17:31	USA		+5	5	Abusech_SSL_Certificate_Bloc	
	SHA1	127E6FBFE24A750E	2019-11-10 20:35	2020-02-29 17:31	USA		+5	5	Kaspersky Malicious Hash Data	
	IP address	93.159.228.40	2019-11-10 20:35	2020-02-29 17:31	USA		+5	5	Abusech_SSL_Certificate_Bloc	
	IP address	8.8.8	2019-11-10 20:35	2020-02-29 17:31	USA		+5	5	Abusech_SSL_Certificate_Bloc	
	MD5	127E6FBFE24A750E	2019-11-10 20:35	2020-04-01 09:01	USA		+5	5	Kaspersky Malicious H 3 more	
	IP address	93.159.228.40	2019-11-10 20:35	2020-02-29 17:31	USA		+5	5	Abusech_SSL_Certificate_Bloc	
	SHA256	127E6FBFE24A750E	2019-11-10 20:35	2020-02-29 17:31	USA		+5	5	Kaspersky Malicious Hash Data	
	IP address	93.159.228.40	2019-11-10 20:35	2020-04-01 09:01	USA		+5	5	Abusech_SSL_Certificate_Bloc	
	IP address	93.159.228.40	2019-11-10 20:35	2020-02-29 17:31	USA		+5	5	Abusech_SSL_Certificate_Bloc	
< P	revious 1	. 234N	ext >						Selected indicators: 0	from 57788

Change log

• Support for Custom Data Feeds located on external URL resources that are more than 255 characters in length is added.

RELEASE 4.0.1.319

RELEASE DATE: 1.06.2021

OPERATING SYSTEM: WINDOWS AND LINUX

HARDWARE PLATFORM: X86_64

New features:

- Ability to load diff versions of Kaspersky Threat Data Feeds was added to speed up the update process and reduce network traffic;
- Ability to configure the settings of detection events storage was added to reduce HDD requirements;

■ Dashboard 20	Search 🕤 Retro	oscan 🔄 Indicators	∠ Detections	🖏 Settings 🔄	Tasks 370		
Service En Feeds	1 Indicators export	[]] Matching 👸 Retrosca	n 🛆 Detections	>>> Events format	හි Users 🔒 🔒	Tenants 🗐 Logging	Licensi
Detections s	torage						
Detections	lorage						
Size of saved detections	less than 1Gb	Delete saved detections					
General settings							
Save detections							

- High Availability mode (HA) for the following CyberTrace features was added to increase fault tolerance:
 - $\circ~$ HA for matching incoming events against feeds and suppliers.
 - HA for several methods if REST API:
 - POST lookup;
 - GET suppliers;
 - GET suppliers/{supplier};
 - POST ioc_exports/{ioc_export}.

Change log

- Kaspersky P-SMS Trojan Data Feed is no longer supported due it's End Of Life;
- IPv6 addresses are supported in settings.

RELEASE 4.0.0.6488 (TIP)

RELEASE DATE: 26.01.2021

OPERATING SYSTEM: WINDOWS AND LINUX

HARDWARE PLATFORM: X86_64

New features:

- Historical correlation feature (retroscan) was added to allow analyzing observables from previously checked events by using the latest feeds to find previously uncovered threats. All historical detections will be included to the report for future investigations.
- Database of indicators with full text search capability and ability to search by using advanced search queries was added to enable complex searches across all indicators fields, including the context fields. The ability to filter results by Intelligence supplier simplifies the process of analyzing threat intelligence.
- Pages with detailed information about each indicator were added for deeper analysis. Each page presents
 all information about an indicator from all threat intelligence suppliers (deduplication) and allows analysts to
 discuss threats in comments as well as add internal threat intelligence about the indicator. If the indicator
 was detected, the information about detection dates and links to the detections list will be available.

D. D. 11		Set 1 -		
[a] Dashboard ∠ _Q S	earch Cd Retroscan	∰ Indicators ∠i Detection	ns 💮 Settings 🕑 Tasks	III He
K Back Mark as	false positive Add to Inter	mal TI Delete		
Type IP	Added on 2021-01-22 22:51	First detected on 2021-01-28 11:18		
Value 123.253.110.198 Associated detections	Last updated on 2021-01-26 08:56	Last detected on 2021-01-28 11:18		
Browse in external resources KTIP				
Suppliers				
IP_Reputation_Data_Fee	ed			
Confidence Type 100 lp	Use for matchin true	ng Updated 2021-01-26 08:56	Send detection events	
 Indicator context 				
category botnet_cnc			ip_whois/descr: IJC.NET	
first_seen: 21.01.2021 16:12			ip_whois/riet_name: JP-Colt	
ip: 123 253 110 198			ip_whois/net_range: 123.253.110.0 - 123.253.110.255	
ip_geo.jp	nul nacific net		1851_54907. 21.01.2021 10.50	
ip_whois/conusci_owner_e	man, moctalic net		thread tensor 100	
ip_whois/created: 10.09.202	o			
Comments				
Add comment here				

Storage for detections was added to simplify security monitoring and alerts triage processes. The raw event
from the source and full information about the detection are saved to the database for future analysis. The
detection list supports searching over the saved data to find all detections by threat, source IP address, user
name, or any other field.

	Kaspersk CyberTra	y ce			admin Timezone: UTC+3			
	Dashboard	Search	🗟 Retroscan 🛛 🎘 Indic	≫s Detections Settings Tasks	III Het			
	EvalTestUserName				Q Search also in detection events 🚺 Auto-update table 🗍			
	Detection date	Source	Category	Details (1) ×				
~	2021-01-22 01:43:19	default	KL_IP_Reputation	IP <u>192.0.2.0</u>				
	Source event RE_USERNAME EvalTer	tUserName	RE_IP 127.0.0.0 RE_IP 192.0.2.0	RE_IP 192.168.0.0 SRC_IP 192.168.0.0				
Window example events CEFC (Pitogenetry)ChewFrace Verification Kell 200Verification_test(2) suser-EvaTestUserName src=192.168.0.0 dvc=1270.0.0 dtrs192.0.2.0 exts/VerificationTest eventds110								
	Detection event category test first_see id A99D335A24C4675i	n 01.01.201 06B433D225	7 00:00 ip <u>192.0.2.0</u> ip_geo ru 3B9CEE	st_seen 21.01.2021 20:55 popularity 1 threat_score 75				
	Whole detection event - category=KL_IP_Repu last_seen=21.01.2021 20	tation match):55 popularit	edIndicator=192.0.2.0 url=- src=19 y=1 threat_score=75	68.0.0 ip=192.0.2.0 md5=- sha1=- sha256=- usrName=EvalTestUserName confiden	nce=100 category=test first_seen=01.01.2017 00:00 ip=192.0.2.0 ip_geo=ru			
	2021-01-22 01:43:17	default	KL_IP_Reputation	IP <u>192.0.2.0</u>				
1								

• Filter for sending detection events to SIEM solutions was added to reduce the load on the solutions and on the Analyst (fighting with alerts fatigue). It allows to send to SIEM solutions only the most dangerous and

confident detections that must be treated as incidents. All other detections will be saved to the internal database and can be used during root cause analysis or in threat hunting.

- HTTP RestAPI for looking up and managing threat intelligence was added. By using the Rest API, Kaspersky CyberTrace can be easily integrated into complex environments for automation and orchestration. The API supports observables lookup as well as TI indicators and TI suppliers managing scenarios (for example, creating and configuring TI supplier).
- Indicators export feature was added to support exporting indicator sets in CSV format to security controls such as policies lists (block lists) and to support sharing of threat data between Kaspersky CyberTrace instances or with other TI Platforms.

Task properties		Maximum records	Export every	Delimiter			
to_FW		50000	24 hours 🗸				
Limit access to speci	fied credentials						
Use authorization to dov	vnload indicators export						
User name	Password						
user							
Fields to export							
Field name	Condition		Value		Inclu	de Output name	<i>—</i>
loc_value	value is non-emp	ty	~			ioc_value	<u> </u>
AND supplier_confidence	e value is more that	n (inclusive)	~ 70				Ĩ
AND ioc_first_detected_	date v date is more than	(inclusive)	✓ %NOW% - 7				Û
Add new filter							
Sort conditions							
Condition name	Direction						
ioc_value	✓ Descending		~ 🗇				
Add sort conditions							

 Multitenancy feature was added to support MSSP or Large Enterprise use cases when a service provider (central office) needs to handle events from different branches (tenants) separately. The feature allows to connect a single Kaspersky CyberTrace instance with different SIEM solutions from different tenants and configure what feeds must be used for each tenant.

🗈 Dashboard 🕰 Search 🏹 Retroscan 🏾 🎘 Indicators	∠ Detections	Settings 🕑 Tasks	III He
🕅 Service 🔝 Feeds 🖞 Indicators export 🔲 Matching 🏹 Re	trosc New tenant	×	
	Tenant *	SPB	
Tenants Add new tenant	Description	saint petersburg office	
Tenant: General	Select a SIEM *	LogRhythm	
Description: General settings applied to all tenants by default	Service listens on:	IP and port UNIX socket	
	IP address *	0.0.0.0	
	Port *	9978	
	Service sends events to:		
	IP address *	10.65.97.17	
	Port *	514	
	* Page irad fields	Add	

- Task manager was added to keep user informed about the current status and usage of Kaspersky CyberTrace. Task manager provides information about running and finished tasks.
- Integration with SIEM Kaspersky Unified Monitoring and Analysis Platform (KUMA) was supported, including Web UI integration (single UI).

Change log

- New components were added to the Dashboard:
 - o Table with last feed update statuses was added to inform the user about feeds updating statistics.
 - Graph with checked events count was added to inform the user about the current and historical load on the system (in Event Per Second – EPS).
 - Feeds intersection matrix was added to help choosing the most valuable threat intelligence suppliers.
- Scenario for auto-updatable dashboard on TV was supported to allow displaying key metrics on a TV screen in the user's office.



- Custom feeds in MISP format was supported to allow integrating feeds from MISP to CyberTrace
- Authentication with LDAP (MS Active Directory) was supported.
- Ability to load feeds from Kaspersky as custom feeds was added to simplify the process of adding new Kaspersky feeds to Kaspersky CyberTrace.
- Process of creating format strings for events that will be sent to SIEM solutions was simplified. A wizard that automatically composes event format strings based on the selected set of event fields has been added.
- URL normalization for 3rd party intelligence sources was added to simplify the process of integrating 3rd party intelligence into Kaspersky CyberTrace.
- An ability to specify confidence for all used Data Feeds was added to improve alerts triage process.
- New X-KF-SaveStatistic flag was added to support saving detection statistics when X-KF-ReplyBack mode is used.

- Installers for Windows and Linux were updated:
 - Kaspersky CyberTrace will be delivered as a single package for all SIEM solutions.
 - Initial configuration was moved from installers to CyberTrace Web and must be performed after the first launch in Web UI with configuration wizard.
- LogRhythm SIEM solution is supported out-of-the-box.
- In Linux packages, init.d management scripts were replaced with system.d scripts.
- Integration with RSA SIEM was updated (":rfc3164" mode for forwarding from SIEM solutions is recommended instead of using EventDelimiter on the Kaspersky CyberTrace side).
- Windows Server 2019 was supported, support for Windows Server 2008 and Desktop versions of Windows (Windows 7, Windows 8, Windows 8.1) was limited.
- OSINT feed Abuse.ch Ransomware and Abuse.ch Feodo MalwareHash was removed due to its discontinuing.
- New versions of the following Kaspersky Data Feeds supported:
 - Vulnerability feed (with CPE field)
 - APT Hash feed (with SHA hashes)
- New Kaspersky ICS Hash Data Feed supported out-of-the box. ICS Hash Data Feed set of file hashes with corresponding context covering the malicious objects that are used to attack Industrial Control Systems infrastructure (ICS).
- Default filter for IP Reputation feed added to detect only dangerous IP Addresses excluding Suspicious ones.

RELEASE 3.1.0.1204

OPERATING SYSTEM: WINDOWS AND LINUX

HARDWARE PLATFORM: X86_64

Change log

• Multiuser mode was added. Now you can use role-based access features to control the operations that different users manage. For example, only users with the Administrator role can manage Kaspersky CyberTrace configuration and browse the search results of all analysts.



Support for downloadable reports was added. The reports contain Kaspersky CyberTrace statistics that are
valuable for measuring the effectiveness of Threat Intelligence to inform the management team about the
value brought by each TI source.



• Search history was added to improve the user experience during Incident Response activities. Analysts now have immediate access to full historical results of searched observables and log file checks.

Kasp Cyb	Kaspersky CyberTrace							
Dashboard & Search Settings								
() Indicator Log file E File								
		Hash, IP address, domain, or URL http://fakess123bn.nu Read about the available resulest types			Search			
Statistics period Day Week I	Statistics period Day Week Month 3 months All time Custom range							
Recent re	quests							
Detected	Date	Query	User					
Detected	Dec 13 2019 21:31	http://fakess123bn.nu	admin					
✓ No	Dec 13 2019 21:08	http://example.com	admin					

- Event Sources management was improved:
 - Normalization for each source was added to support events from a broad range of sources in a single Kaspersky CyberTrace instance. For example, from different SIEMs like McAfee and QRadar.
 - Determining the source based on regular expressions was added to support sources with events in the non-syslog format. The previous methods of determining event sources based on IP or syslog hostname are supported as well.

Kaspersky CyberTrace		<u>admin</u> ~
🔟 Dashboard 🖉 Search 😧 Settings		🛄 Help
Event sources	Add new event source O × Source ID Palo Alto	
Source ID CISCO_ASA Type: IP address V Value	Type Value RegExp V [^]+pa_fw]	/ 1
Save Cancel	Next Cancel	

- New Kaspersky Data Feeds were added:
 - IoT URL Data Feed. A set of URLs with context that cover malicious links used to download malware that targets Internet of Things-enabled devices.
 - Vulnerability Data Feed. A set of file hashes of applications with vulnerabilities, supplemented with hashes of exploits that use those vulnerabilities, and related cyber threat intelligence context.
 - New version of Mobile Botnet CnC URL Data Feed with extra context. The feed contains URLs and masks for detecting C&C servers and web resources that are related to mobile botnets.
- Updated OSINT feed list:
 - o ZeuS Tracker was removed due to its discontinuing.
 - o Abuse.ch SSL Certificate Blacklist, BlockList.de, Cyber Crime Tracker OSINT feeds were added.
 - Several OSINT categories were renamed:
 - AbuseSh_Ransomware_Common_URL was renamed to AbuseCh_Ransomware_Common_URL.
 - AbuseSh_Ransomware_BlockURL was renamed to AbuseCh_Ransomware_Block_URL.
 - AbuseSh_Ransomware_BlockDomain was renamed to
 - AbuseCh_Ransomware_Block_Domain.
 - AbuseSh_Ransomware_BlockIP was renamed to AbuseCh_Ransomware_Block_IP.
 - AbuseSh_Feodo_BlockIP was renamed to AbuseCh_Feodo_Block_IP.
 - EmergingThreats_Block_IP was renamed to EmergingThreats_BlockIP.
 - EmergingThreats_Compromised_IP was renamed to EmergingThreats_CompromisedIP.



Filtering rules for feeds Add custom feed Manage lists ~		
Kaspersky feeds OSINT feeds Custom feeds		
> Abuse.ch_Feodo_BlockIPjson		Feed is off
> Abuse.ch_Feodo_MalwareHash.json		Feed is on
> Abuse.ch_Ransomware_BlockDomain.json		Feed is off
> Abuse.ch_Ransomware_BlockIP.json		Feed is off
> Abuse.ch_Ransomware_BlockUrl.json		Feed is off
> Abuse.ch_Ransomware_Common.json		Feed is on
 Abuse.ch_SSL_Certificate_BlockHash.json 		Feed is on
Path is https://sslbl.abuse.ch/blacklist/sslblacklist.csv		
Truncate feed Maximum records 0		
Available fields:		
SHA1		
✓ first_seen		
✓ threat		
Filtering rules	Actionable fields	
Field name Value	Field name Output	
Add new rule	Add new field	

- TAXII 1 protocol support was improved.
- Licensing was added. The license limits the number of available indicators of compromise (IoCs) from Data Feeds, the number of incoming Events per second (EPS) for matching, and available features (multiuser mode, threat search, third-party feeds).

Licensing Add new I	icense key						
Active license key							
Expiration date 2020-11-09 (332 days left)	EPS rate Now: 0 Max: Unlimited	Indicators count Now: 710 375 Max: Unlimited	Search Yes	Custom feeds Yes	Multi-user mode Yes	Key file Owner 5751180E key	Ū
Inactive license key							
Community Edition							
Expiration date	EPS rate	Indicators count	Search	Custom feeds	Multi-user mode	Key file	
Unlimited	Now: 0	Now: 710 375					
	Max: 250	Max: 1 000 000					

- Deprecated features were removed:
 - The mode without GUI was disabled.
 - The steps for specifying feed parameters were removed from the installers (DEB, RPM, MSI). This function is now performed from the Web UI.
 - The ability to run Kaspersky CyberTrace in the foreground on Linux was disabled. Kaspersky CyberTrace now always runs as a Linux-daemon.
- HTML documentation was improved.

RELEASE 3.0.0.382

OPERATING SYSTEM: WINDOWS AND LINUX

HARDWARE PLATFORM: X86_64

Features

- Kaspersky CyberTrace Web, a web user interface for Kaspersky CyberTrace, provides data visualization, on-demand IoC lookup functionality and access to Kaspersky CyberTrace configuration. Kaspersky CyberTrace Web also supports the management of feeds, log parsing rules, blacklists and whitelists and event sources.
- 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) available through HTTP(S), FTP or TAXII. Demo data feeds from Kaspersky and OSINT are available out of the box.

Kaspersky CyberTrace				admin ~
🗈 Dashboard 💪 Lookup 😳 Settings				CD Help
Service Feeds Matching Levents format Lo Feeds update period Import certificate Update frequency 30 min Launch update now Lest update 15 26 00 28 01 2019 Filtering rules for feeds + Add custom feed	Custom feed Feed name * Path to the feed * Certificate Feed type * * Required fields	json Next	Erowse Cancel	
> Kaspersky APT Hash Data Feed				
> Kaspersky APT IP Data Feed				
> Kaspersky APT URL Data Feed				No certificate
> Kaspersky Botnet CnC URL Data Feed				No certificate
> Kaspersky Demo Botnet CnC URL Data Feed				Feed is on
> Kaspersky Demo IP Reputation Data Feed				Feed is on
> Kaspersky Demo Malicious Hash Data Feed				Feed is on

 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.

🗈 Dashboard 🛆 Lookup 🔅 Settings		III <u>Help</u>
🕈 Service 📰 Feeds []] Matching 🛄 Events format 🗐 Logging		
Event parsing rules + Add new event source		
Device ID default		Set event parsing rules
Device ID Source1		Set event parsing rules
Event normalizing rules		
Event normalizing rules Replacing rules Substring to replace Replace with	Ignoring rules Ignore events that contain this substring	
Event normalizing rules Peplacing rules Subarring to replace Add new rule	Ignoring rules Ignore events that contain this substring The substring Add new rule	
Event normalizing rules Replacing rules Substring to replace Add new rule Suve Cancel	Ignoring rules Ignore events that contain this substring	

• Generates feed usage statistics for measuring the effectiveness of feeds.

Cyberfrace							
🖹 Dashboard 🛆 Lookup 🔅	Settings						III <u>He</u> l
Time range Day Week Month 3 months							
Statistics overview							
statistics over view							
Number of detections Number of detected in	ndicators					IP address	- Hash - URL
80							
60							
40	-/						
20	_/						
0		γ	1				
Jan 27 15:57:02 Jan 27 17:57:02 Jan 27 19:57:02	. Jan 27 21:57:02 Jan 2	27 23:57:02 Jan 28	01:57:02 Jan 28 03	i7:02 Jan 28 05:57:02	Jan 28 07:57:02 Jan 28 09:	:57:02 Jan 28 11:57:02	Jan 28 13:57:02 Jan 28 15:57:02
Food statistics							
reed statistics							
	Indicators	Whitelisted	Detected	Detected	Whitelisted		
Feed name							
Feed name IP_Reputation_Data_Feed.json	0	0	1 961		• IP.	_Reputation_Data_Feed	
Feed name IP_Reputation_Data_Feed.json Malicious_URL_Data_Feed.json	0	0	1 961 597		• IP.	_Reputation_Data_Feed alicious_URL_Data_Feed	

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

Kaspersky CyberTrace	admin ~					
Dashboard A Lookup ③ Sett	ings			III Hele		
	Indicato	r Log file File				
	Selec	t files				
Summary						
Number of processed file(s) Processed 1 file(s)	Number of detected indicator(s) Detected 12 indicator(s) in 1 file(s)	Number of processed lines Processed 24385 lines				
KL_IP_Reputation 7 matches KL_Melicious_Hesh_MD5 3 matches	KL_Malicious_Hash_SHA1	1 matches	KL_Malicious_Hash_SHA256 1 matches			
Top 100 matching indicators	Download resort					
Category: KL_Malicious_Hash_SHA256 Matcheolindicator: 68343D143DE4409D135013	RFE05849412F94F9C873542842F24751088874178F	popularity: 2 threat: HEUR Trojan Script Generic				
IP: 80.78.250.58, 87.236.19.88, 178.172.235.204	185.68.16.7 213.155.11.22 185.68.16.8 91.218.228.19	urls/0/url: <u>distant.gbou-bpt.ru/jgu</u>	ery/latest/eoo.is			
MD5: <u>8C2761F090F1F2F878DEF3AFD66E2F6E</u>		uris/1/uri: artiife1.com/jguery/lates				
SHA1: 8991F4646B1141FB4EB6BEC2B9EDDC76	34A9E7968	urls/3/url: zito.su/jguery/latest/duy	urls/2/url: <u>kdsk.com.ua/jquery/latest/ufgf37.js</u> urls/3/url: zito.su/jquery/latest/duvg14.js			
SHA256: 68343D143DEAA09D1350138EF05B4	9A12E9AE9CB73542842E247510BBB7A17BF	urls/4/url: teplomarket.kiev.ua/jgur	ery/latest/fny.js			
file size: 20.071	iujs, aedotujs, saekrizujs, tydyrg37.js, enegtuujs, pot29.js	urls/5/url: neman.lim.by/jguery/lat	<u>rest/skiuai.js</u>			
file type: Txt		urls/6/url: megaservis.kiev.ua/jque	ry/latest/augu.js			
first_seen: 15.11.2017 01:49		urls/7/url: <u>parkmetallurg.ru/iguery</u>	/latest/skh12.js			
geo: ru, ua, kz, uz, by		uns/s/un: maladost.lim.by/jguery/	latest/teogzb.)s			
1000 0000 0710 0010 1118		enterorente enterenter-dozite/jgpei	11.0000-000-00100-000-000			

- Export lookup results that match data feeds to CSV format for integration with other systems (firewalls, network and host IDS, custom tools).
- Universal approach to integration of threat matching capabilities with SIEMs 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.
- 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.

 Nasperský botnet ChC OKE t 	Jala Peeu			The definitioned
 Kaspersky Demo Botnet Cn0 	C URL Data Feed			Feed is on
This is a demo version of Botnet	t CnC URL Data Feed.			
Truncate feed Maximum r	records in feed 0			
Available fields:				
IP	🗹 id	urls/url	whois/country	whois/org
✓ files/MD5	last_seen	whois/MX	✓ whois/created	whois/registrar_email
✓ files/SHA1	🗹 mask	whois/MX_ips	vhois/domain	whois/registrar_name
✓ files/SHA256	popularity	whois/NS	vhois/email	whois/updated
first_seen	🗹 threat	whois/NS_ips	 whois/expires 	
🗹 geo	🗹 type	whois/city	vhois/name	
Filtering rules		Actionable fields		
Field name	Value	Field name	Output	
		Û		Ū.
Add new rule		Add new field		
> Kaspersky Demo IP Reputati	on Data Feed			Feed is on
> Kaspersky Demo Malicious H	Hash Data Feed			Feed is on
> Kaspersky IP Reputation Dat	a Feed			No certificate
> Kaspersky Malicious Hash Da	ata Feed			No certificate

- 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, Kaspersky CyberTrace receives logs from various sources such as networking devices and parses these logs according to defined regular expressions.

Kaspersky							_
CyberTrace	Rules for extracting d	ata from incoming ever	nts			\times	<u>admin</u> ∽
🖹 Dashboard 🛛 💪 Lookup	Start collecting events	Stop collecting events	Restart collecting events				III Help
👔 Service 🔛 Feeds [] Matchin							
Event parsing rules +							
Device ID default							Set event parsing rules
Device ID Source1							Set event parsing rules
	Indicator type	Rule name	Regular expression		Concatenation rule		
Event normalizing rules	CONTEXT 🗸	RE_DATE	(\w{3}\s+\d+\s+[\d\:]+)\s	Extract all		ŵ	
	IP 🗸	RE_IP	(((?:25[0-5]]2[0-4][0-9]][0	Z Extract all	#1	Û	
Replacing rules Substring to replace	MD5 ~	RE_MD5	([\da-fA-F]{32})	Z Extract all		Û	
	SHA1 ~	RE_SHA1	([\da-fA-F]{40})	Z Extract all		ŵ	
Add annuals	SHA256 V	RE_SHA256	([\da-fA-F]{64})	Z Extract all		Û	
Add new rule	URL ~	RE_URL	(?:\:\/\/)((?:\S+{?::\S*)?+@]	Z Extract all		Û	
Save Cancel	CONTEXT ~	RE_USERNAME	usrName=([0-9a-zA-Z]+)	Extract all		Û	
	IP v	SRC_IP	src\={\d{1,3}.\d{1,3}.1,.	Extract all	#1	Û	
© 2019 AO Kaspersky Lab. All Rights Reserved.							KASPERSKY

- Exposures obfuscation techniques used by some threats to hide malicious activities in logs.
- TAXII protocol support.
- Out of the box supported Kaspersky Threat Data Feeds:
 - o Demo Botnet CnC URL
 - o Demo IP Reputation
 - o Demo Malicious Hash
 - o APT Hash
 - o APT IP
 - o APT URL
 - o Botnet CnC URL
 - Malicious URL
 - o Phishing URL
 - o IP Reputation
 - Malicious Hash
 - o Mobile Botnet
 - o Mobile Malicious Hash
 - o P-SMS Trojan
 - o Ransomware URL
- Out of the box supported OSINT Data Feeds:
 - Abuse.sh_Zeus_Hosts
 - Abuse.sh_Zeus_Configs
 - o Abuse.sh_Zeus_Binaries
 - o Abuse.sh_Zeus_Dropzones
 - o Abuse.sh_Zeus_BadIP
 - o Abuse.sh_Zeus_BadDomain
 - Abuse.sh_Zeus_BlockIP
 - Abuse.sh_Zeus_BlockDomain
 - Abuse.sh_Ransomware_Common
 - o Abuse.sh_Ransomware_BlockUrl
 - o Abuse.sh_Ransomware_BlockDomain
 - o Abuse.sh_Ransomware_BlockIP
 - Abuse.sh_Feodo_BlockIP
 - EmergingThreats_BlockIP
 - o EmergingThreats_CompromisedIP

- Out of the box supported SIEMs: Spunk, ArcSight, IBM QRadar and RSA NetWitness. Connectors for other SIEMs can be provided by request.
- Watchdog mode is supported.
- HTML documentation is available.



www.kaspersky.com/ www.securelist.com

© 2019 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners