Threat Intelligence Platform

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 4.0.0.6488 (TIP)

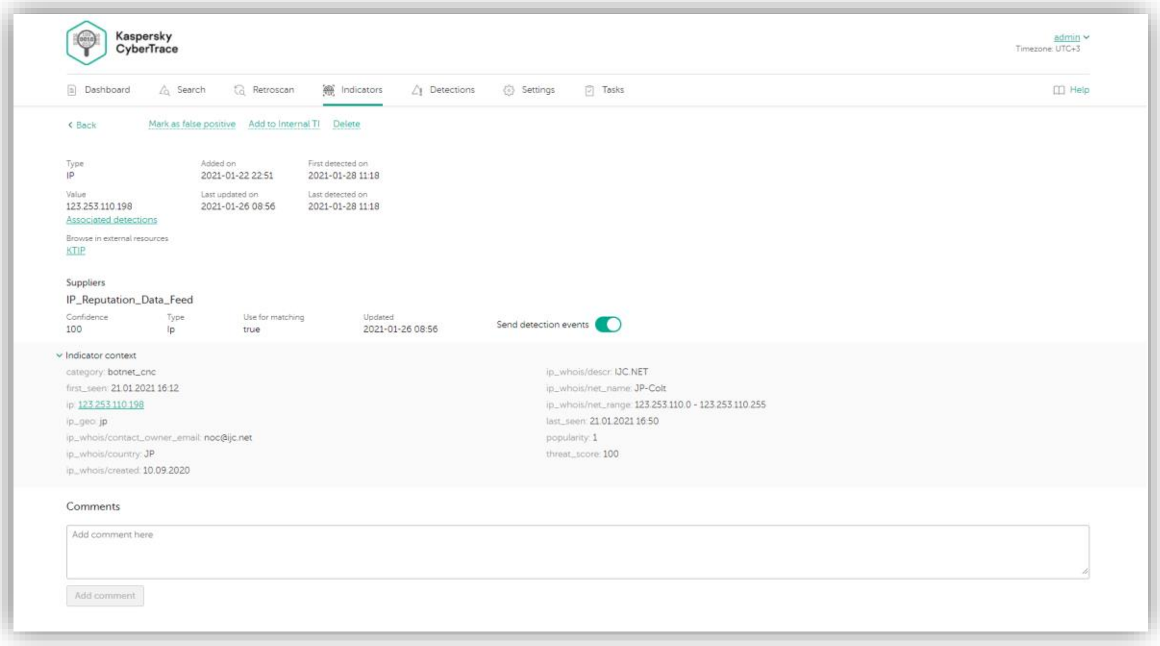
RELEASE DATE: 26.01.2021

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.



Timezone: UTC+3

Type: IP
Added on: 2021-01-22 22:51
First detected on: 2021-01-28 11:18
Value: 123.253.110.198
Last updated on: 2021-01-26 08:56
Last detected on: 2021-01-28 11:18
Associated detections
Browse in external resources: KTIP

Suppliers
IP_Reputation_Data_Feed

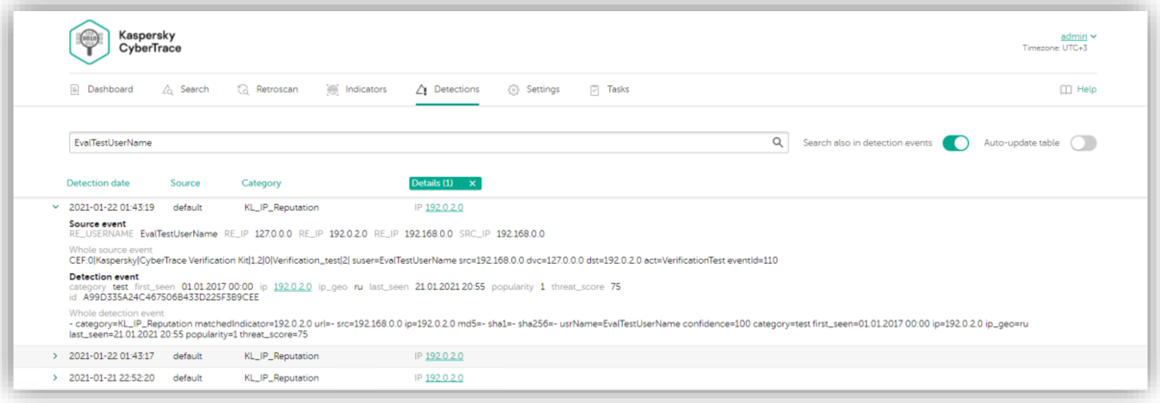
Confidence	Type	Use for matching	Updated
100	Ip	true	2021-01-26 08:56

Send detection events: ●

Indicator context
category: botnet_cnc
first_seen: 21.01.2021 16:12
ip: 123.253.110.198
ip_geo: jp
ip_whois/contact_owner_email: noc@ijc.net
ip_whois/country: JP
ip_whois/created: 10.09.2020
ip_whois/descr: IJC.NET
ip_whois/net_name: JP-Colt
ip_whois/net_range: 123.253.110.0 - 123.253.110.255
last_seen: 21.01.2021 16:50
popularity: 1
threat_score: 100

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.



Timezone: UTC+3

EvalTestUserName
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 192.0.2.0

Source event
RE_USERNAME EvalTestUserName RE_IP 127.0.0.0 RE_IP 192.0.2.0 RE_IP 192.168.0.0 SRC_IP 192.168.0.0

Whole source event

```
CEF:0|Kaspersky|CyberTrace Verification Kit|1.2|0|Verification_test|2| suser=EvalTestUserName src=192.168.0.0 dvc=127.0.0.0 dst=192.0.2.0 act=VerificationTest eventId=110
```

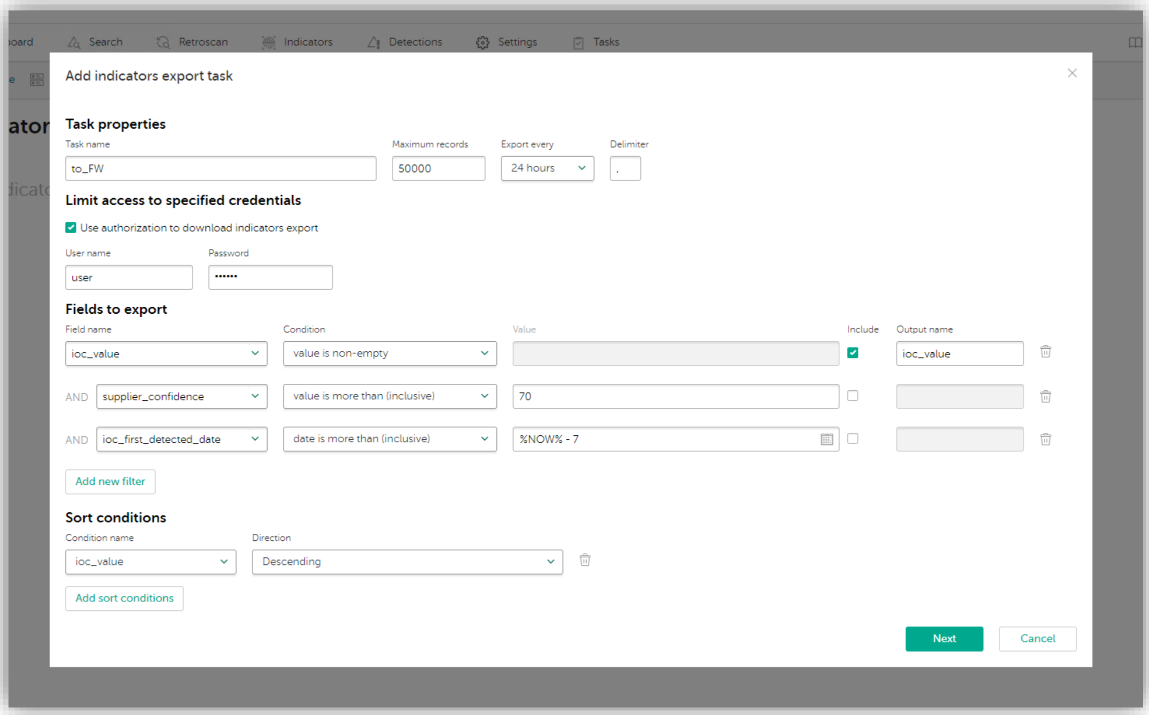
Detection event
category test first_seen 01.01.2017 00:00 ip 192.0.2.0 ip_geo ru last_seen 21.01.2021 20:55 popularity 1 threat_score 75
id A99D335A24C467506B433D225F3B9CEE

Whole detection event

```
- category=KL_IP_Reputation matchedIndicator=192.0.2.0 url=- src=192.168.0.0 ip=192.0.2.0 md5=- sha1=- sha256=- usrName=EvalTestUserName confidence=100 category=test first_seen=01.01.2017 00:00 ip=192.0.2.0 ip_geo=ru
last_seen=21.01.2021 20:55 popularity=1 threat_score=75
```

Detection date	Source	Category	Details (1)
2021-01-22 01:43:17	default	KL_IP_Reputation	IP 192.0.2.0
2021-01-21 22:52:20	default	KL_IP_Reputation	IP 192.0.2.0

- 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.



Add indicators export task

Task properties

Task name: to_FW
Maximum records: 50000
Export every: 24 hours
Delimiter: ,

Limit access to specified credentials

☑ Use authorization to download indicators export

User name: user
Password: ••••••

Fields to export

	Field name	Condition	Value	Include	Output name
	ioc_value	value is non-empty		☑	ioc_value
AND	supplier_confidence	value is more than (inclusive)	70	□	
AND	ioc_first_detected_date	date is more than (inclusive)	%NOW% - 7	□	

Add new filter

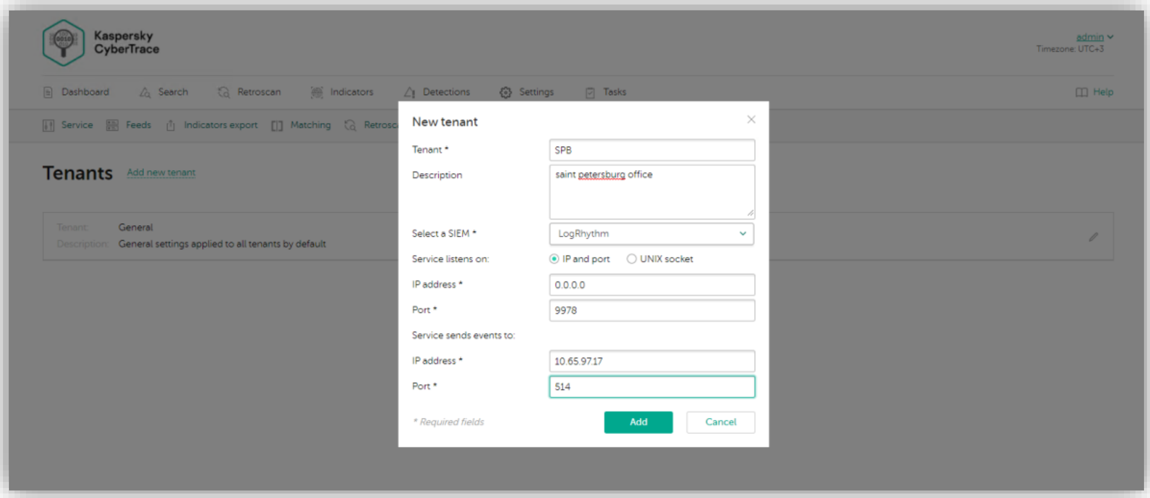
Sort conditions

Condition name	Direction
ioc_value	Descending

Add sort conditions

Next Cancel

- 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.



Tenants

Tenant: General
Description: General settings applied to all tenants by default

New tenant

Tenant *: SPB
Description: saint petersburg office
Select a SIEM *: LogRhythm
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

* Required fields

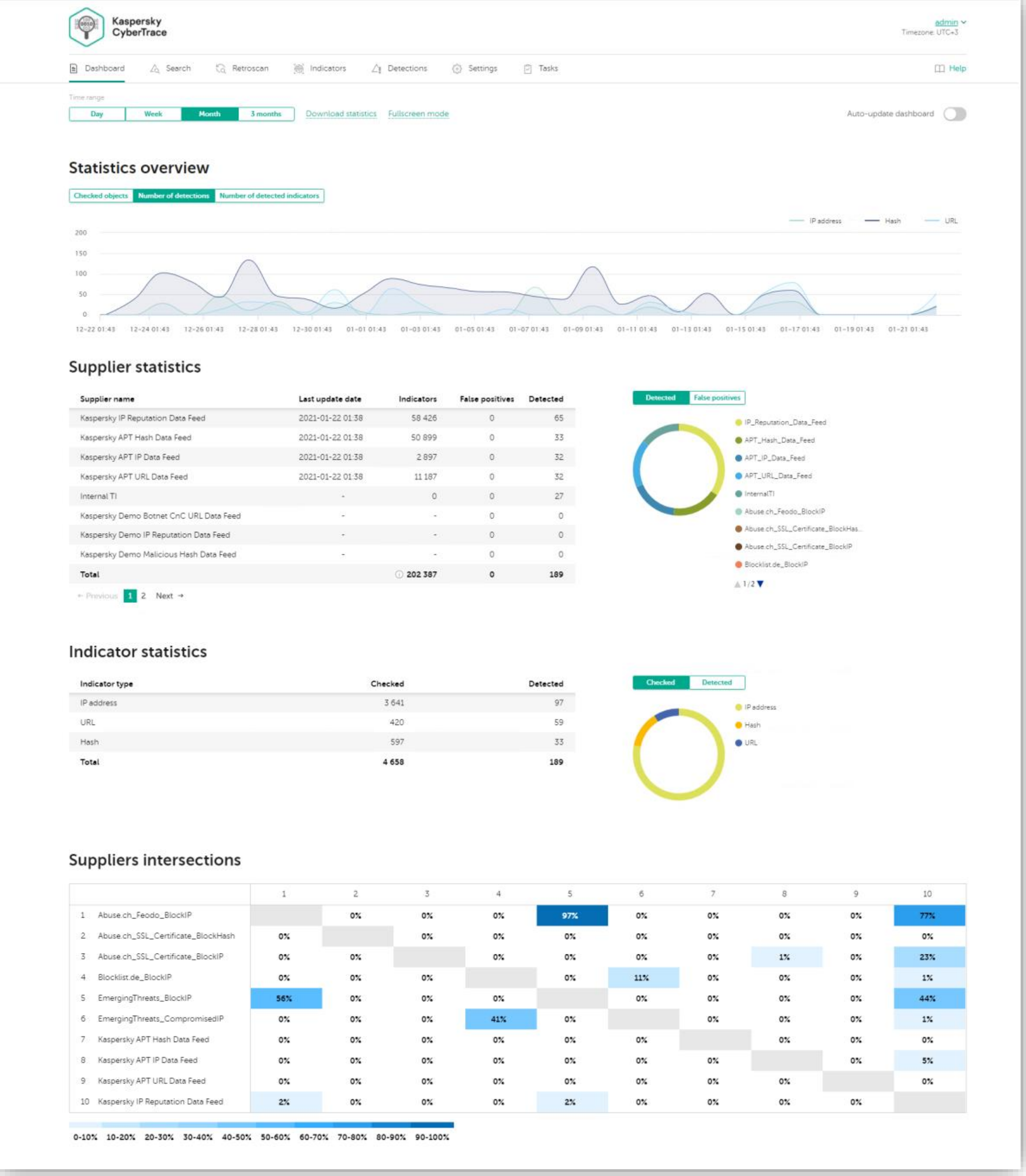
Add Cancel

- 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:
  - 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.



Statistics overview

Supplier statistics

Supplier name	Last update date	Indicators	False positives	Detected
Kaspersky IP Reputation Data Feed	2021-01-22 01:38	58 426	0	65
Kaspersky APT Hash Data Feed	2021-01-22 01:38	50 899	0	33
Kaspersky APT IP Data Feed	2021-01-22 01:38	2 897	0	32
Kaspersky APT URL Data Feed	2021-01-22 01:38	11 187	0	32
Internal TI	-	0	0	27
Kaspersky Demo Botnet CnC URL Data Feed	-	-	0	0
Kaspersky Demo IP Reputation Data Feed	-	-	0	0
Kaspersky Demo Malicious Hash Data Feed	-	-	0	0
Total		ⓘ **202 387**	**0**	**189**

Indicator statistics

Indicator type	Checked	Detected
IP address	3 641	97
URL	420	59
Hash	597	33
Total	**4 658**	**189**

Suppliers intersections

		1	2	3	4	5	6	7	8	9	10
1	Abuse.ch_Feodo_BlockIP		0%	0%	0%	97%	0%	0%	0%	0%	77%
2	Abuse.ch_SSL_Certificate_BlockHash	0%		0%	0%	0%	0%	0%	0%	0%	0%
3	Abuse.ch_SSL_Certificate_BlockIP	0%	0%		0%	0%	0%	0%	1%	0%	23%
4	Blocklist.de_BlockIP	0%	0%	0%		0%	11%	0%	0%	0%	1%
5	EmergingThreats_BlockIP	56%	0%	0%	0%		0%	0%	0%	0%	44%
6	EmergingThreats_CompromisedIP	0%	0%	0%	41%	0%		0%	0%	0%	1%
7	Kaspersky APT Hash Data Feed	0%	0%	0%	0%	0%	0%		0%	0%	0%
8	Kaspersky APT IP Data Feed	0%	0%	0%	0%	0%	0%	0%		0%	5%
9	Kaspersky APT URL Data Feed	0%	0%	0%	0%	0%	0%	0%	0%		0%
10	Kaspersky IP Reputation Data Feed	2%	0%	0%	0%	2%	0%	0%	0%	0%	

- 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 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.

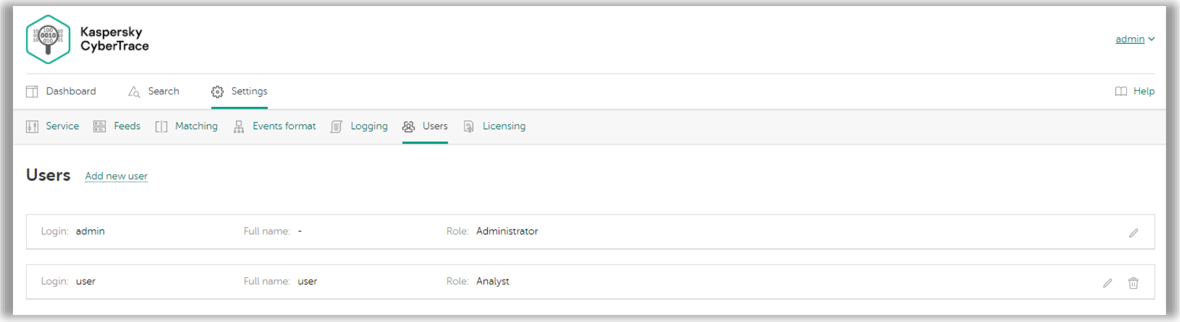
RELEASE 3.1.0.1204

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.

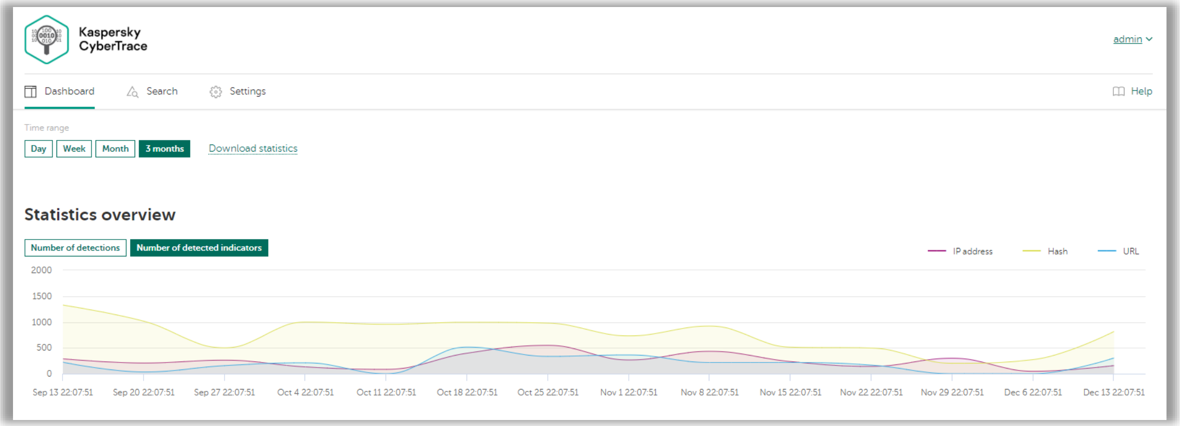


Users

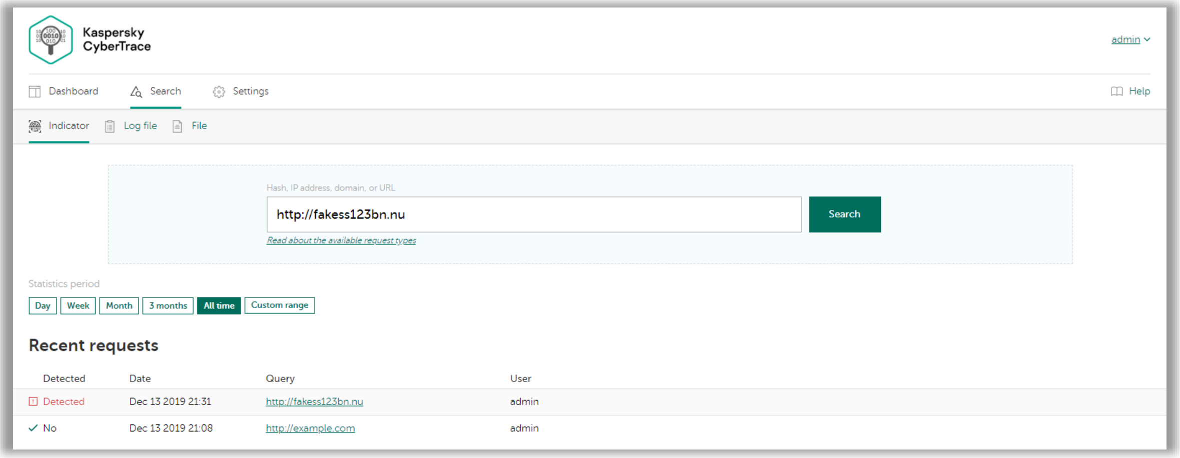
Login: admin Full name: - Role: Administrator

Login: user Full name: user Role: Analyst

- 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.

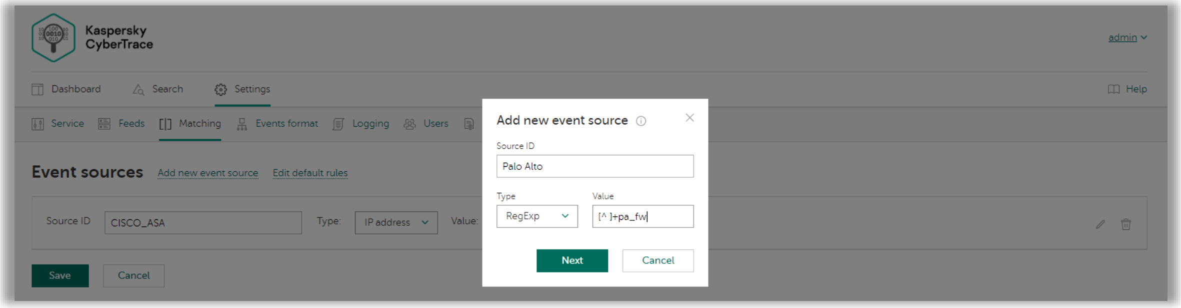


Hash, IP address, domain, or URL: http://fakess123bn.nu

Recent requests

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.



Event sources

Source ID: CISCO_ASA Type: IP address Value:

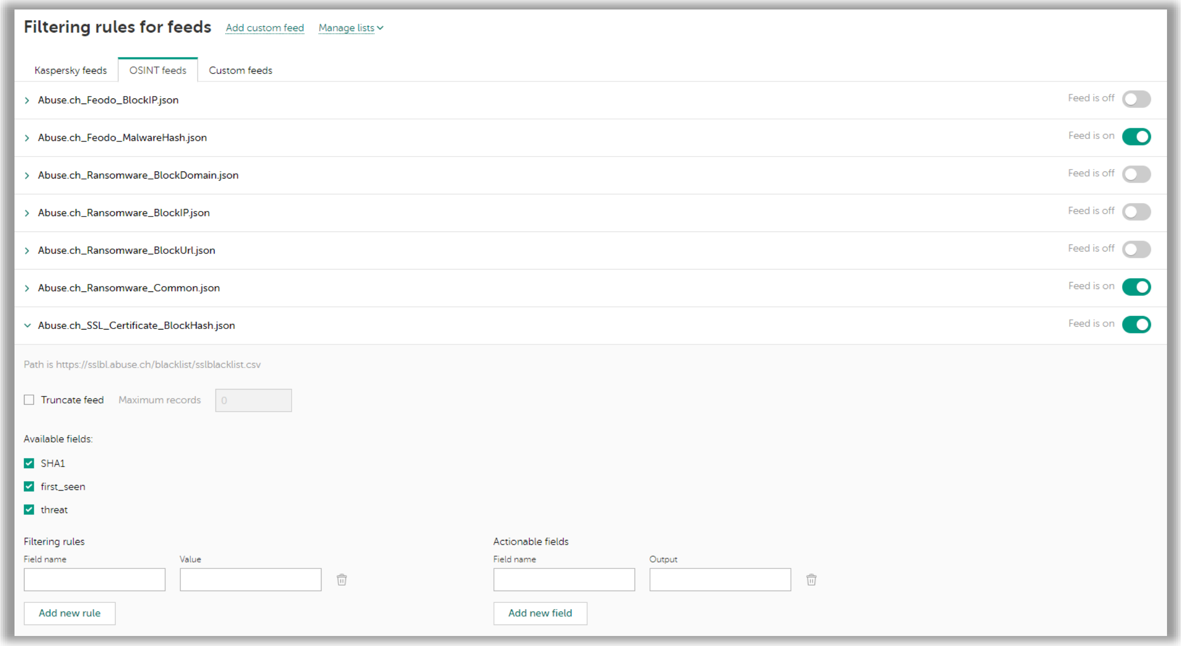
Add new event source

Source ID: Palo Alto

Type: RegExp

Value: [^]+pa_fw

- 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:
  - ZeuS Tracker was removed due to its discontinuing.
  - 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

Abuse.ch_Feodo_BlockIP.json	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

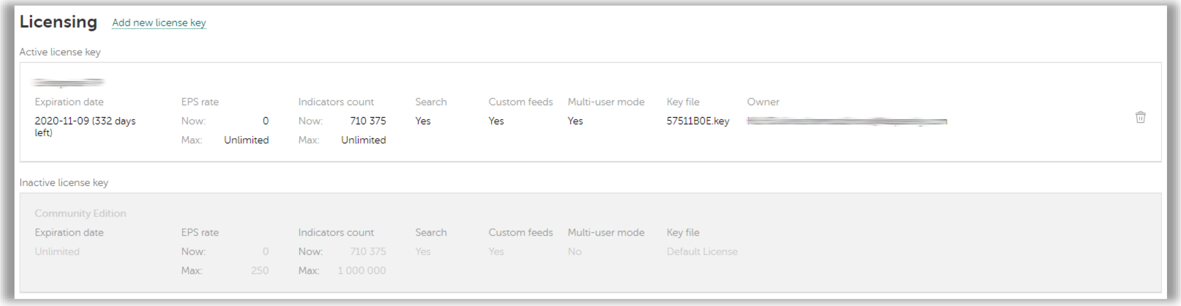
Filtering rules

Field name Value

Actionable fields

Field name Output

- 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

Active license key

[redacted]

Expiration date	EPS rate	Indicators count	Search	Custom feeds	Multi-user mode	Key file	Owner
2020-11-09 (332 days left)	Now: 0 Max: Unlimited	Now: 710 375 Max: Unlimited	Yes	Yes	Yes	57511B0E.key	[redacted]

Inactive license key

Community Edition

Expiration date	EPS rate	Indicators count	Search	Custom feeds	Multi-user mode	Key file
Unlimited	Now: 0 Max: 250	Now: 710 375 Max: 1 000 000	Yes	Yes	No	Default License

- 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.

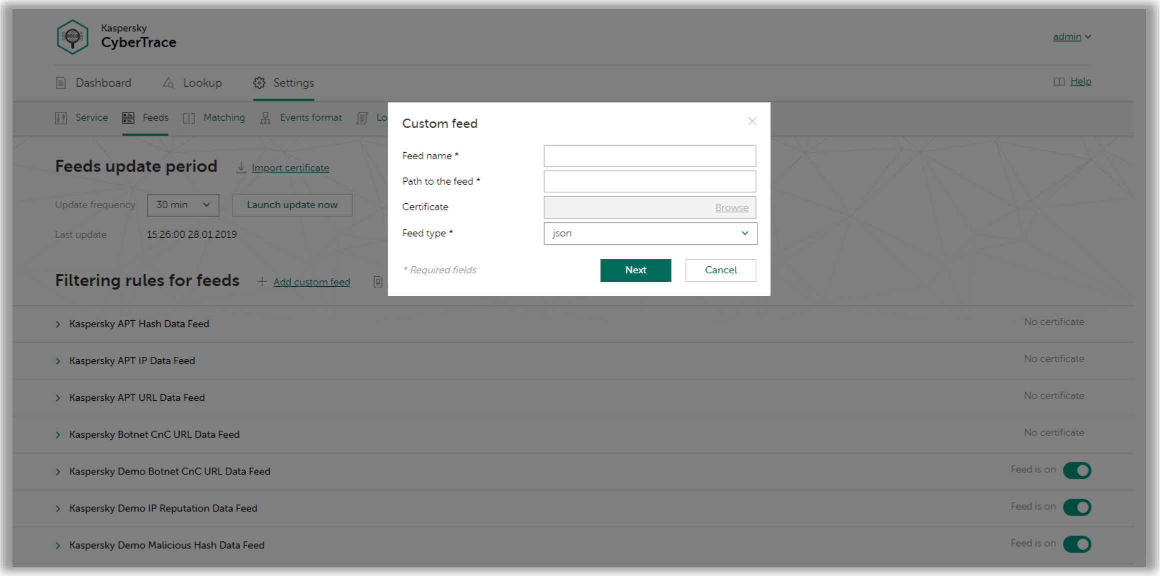
RELEASE 3.0.0.382

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.



Feeds update period

Update frequency 30 min

Last update 15:26:00 28.01.2019

Filtering rules for feeds

Custom feed

Feed name *

Path to the feed *

Certificate

Feed type * json

* Required fields

Kaspersky APT Hash Data Feed — No certificate

Kaspersky APT IP Data Feed — No certificate

Kaspersky APT URL Data Feed — No certificate

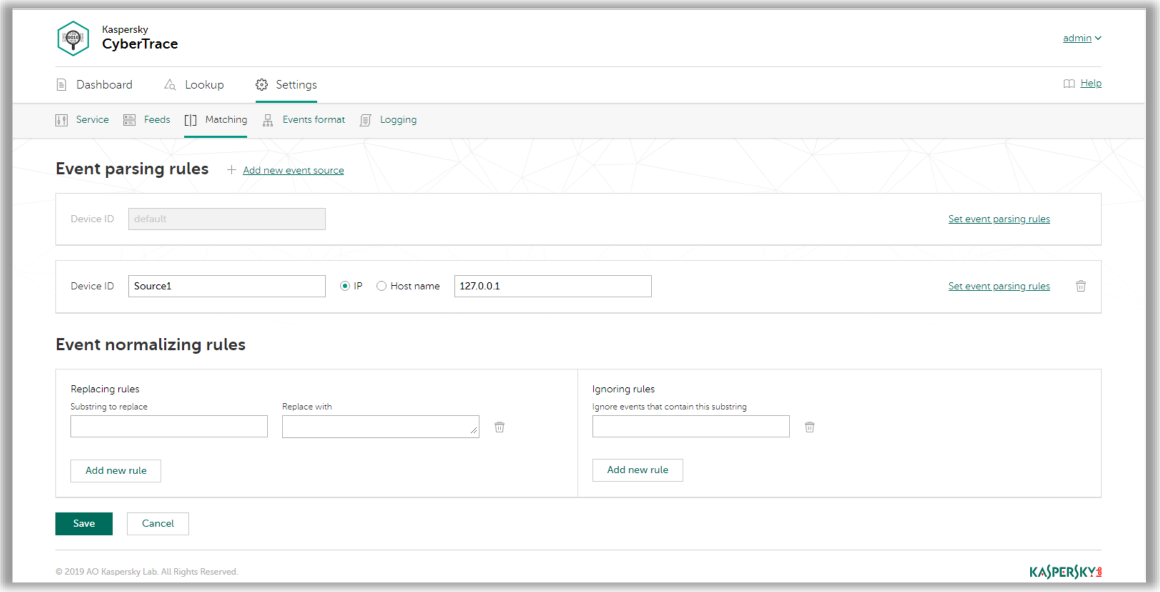
Kaspersky Botnet CnC URL Data Feed — No certificate

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.



Event parsing rules

Device ID default

Device ID Source1 ● IP ○ Host name 127.0.0.1

Event normalizing rules

Replacing rules

Substring to replace

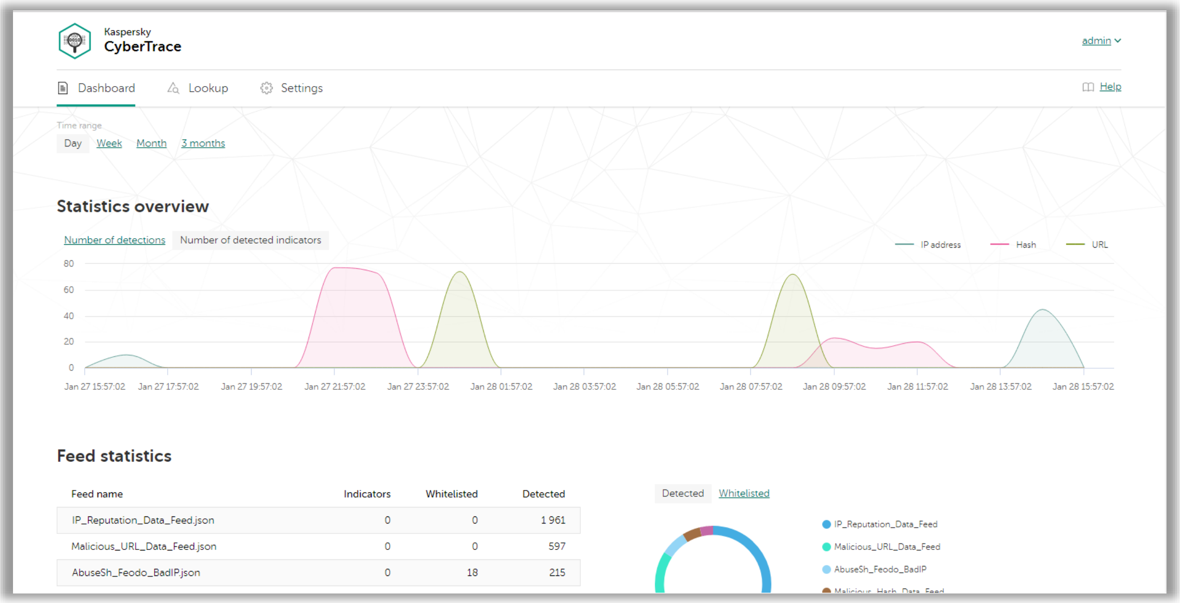
Replace with

Ignoring rules

Ignore events that contain this substring

© 2019 AO Kaspersky Lab. All Rights Reserved.

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

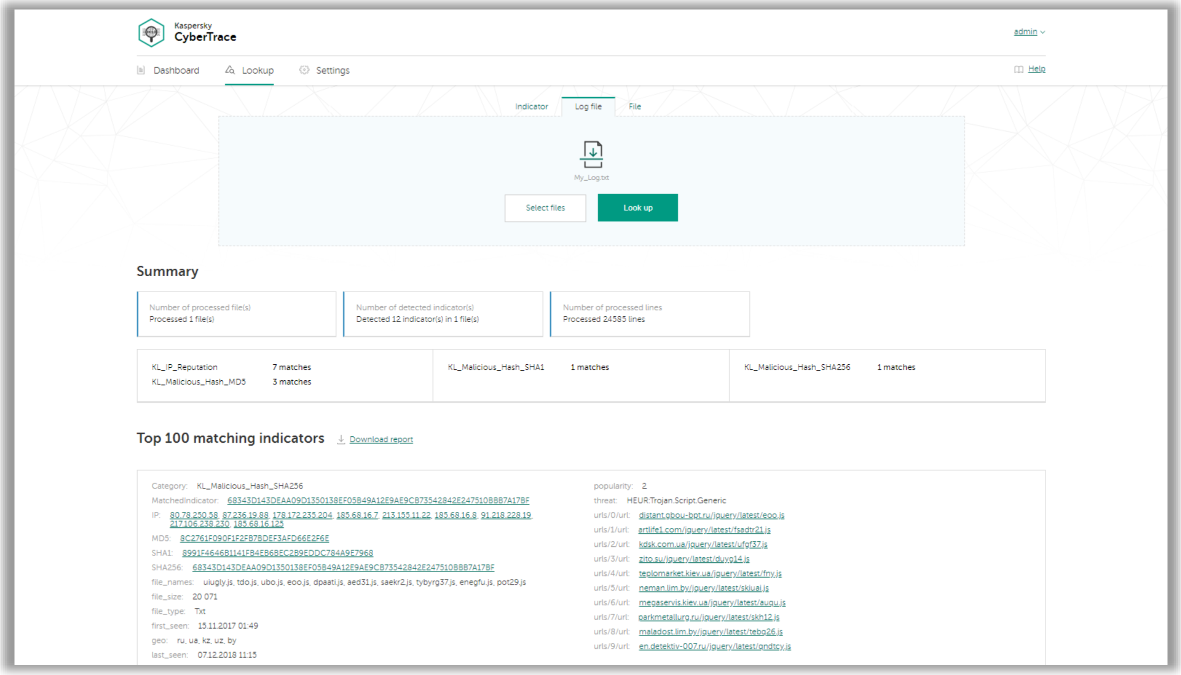


Statistics overview

Feed statistics

Feed name	Indicators	Whitelisted	Detected
IP_Reputation_Data_Feed.json	0	0	1 961
Malicious_URL_Data_Feed.json	0	0	597
AbuseSh_Feodo_BadIP.json	0	18	215

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



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 24585 lines

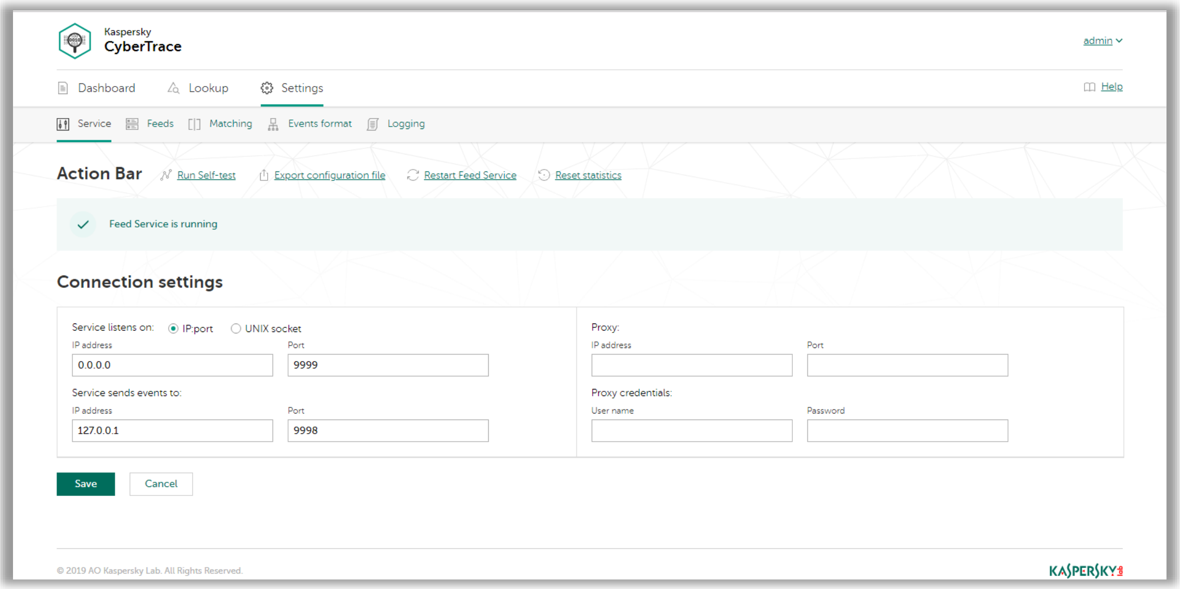
KL_IP_Reputation	7 matches	KL_Malicious_Hash_SHA1	1 matches	KL_Malicious_Hash_SHA256	1 matches
KL_Malicious_Hash_MD5	3 matches				

Top 100 matching indicators

Category: KL_Malicious_Hash_SHA256
MatchedIndicator: 68343D143DEAA09D1350138EF05B49A12E9AE9CB73542842E247510BBB7A17BF
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, 217.106.238.230, 185.68.16.125
MD5: 8C2761F090F1F2FB7BDEF3AFD66E2F6E
SHA1: 8991F4646B1141FB4EB6BEC2B9EDDC784A9E7968
SHA256: 68343D143DEAA09D1350138EF05B49A12E9AE9CB73542842E247510BBB7A17BF
file_names: uiugly.js, tdo.js, ubo.js, eoo.js, dpaati.js, aed31.js, saekr2.js, tybyrg37.js, enegfu.js, pot29.js
file_size: 20 071
file_type: Txt
first_seen: 15.11.2017 01:49
geo: ru, ua, kz, uz, by
last_seen: 07.12.2018 11:15

popularity: 2
threat: HEUR:Trojan.Script.Generic
urls/0/url: distant.gbou-bpt.ru/jquery/latest/eoo.js
urls/1/url: artlife1.com/jquery/latest/fsadtr21.js
urls/2/url: kdsk.com.ua/jquery/latest/ufgf37.js
urls/3/url: zito.su/jquery/latest/duyg14.js
urls/4/url: teplomarket.kiev.ua/jquery/latest/fny.js
urls/5/url: neman.lim.by/jquery/latest/skiuai.js
urls/6/url: megaservis.kiev.ua/jquery/latest/augu.js
urls/7/url: parkmetallurg.ru/jquery/latest/skh12.js
urls/8/url: maladost.lim.by/jquery/latest/tebq26.js
urls/9/url: en.detektiv-007.ru/jquery/latest/gndtcy.js

- 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.



Kaspersky CyberTrace

admin

Dashboard · Lookup · Settings

Help

Service · Feeds · Matching · Events format · Logging

Action Bar Run Self-test · Export configuration file · Restart Feed Service · Reset statistics

✓ Feed Service is running

Connection settings

Service listens on: ● IP:port ○ UNIX socket

IP address	Port
0.0.0.0	9999

Service sends events to:

IP address	Port
127.0.0.1	9998

Proxy:

IP address	Port

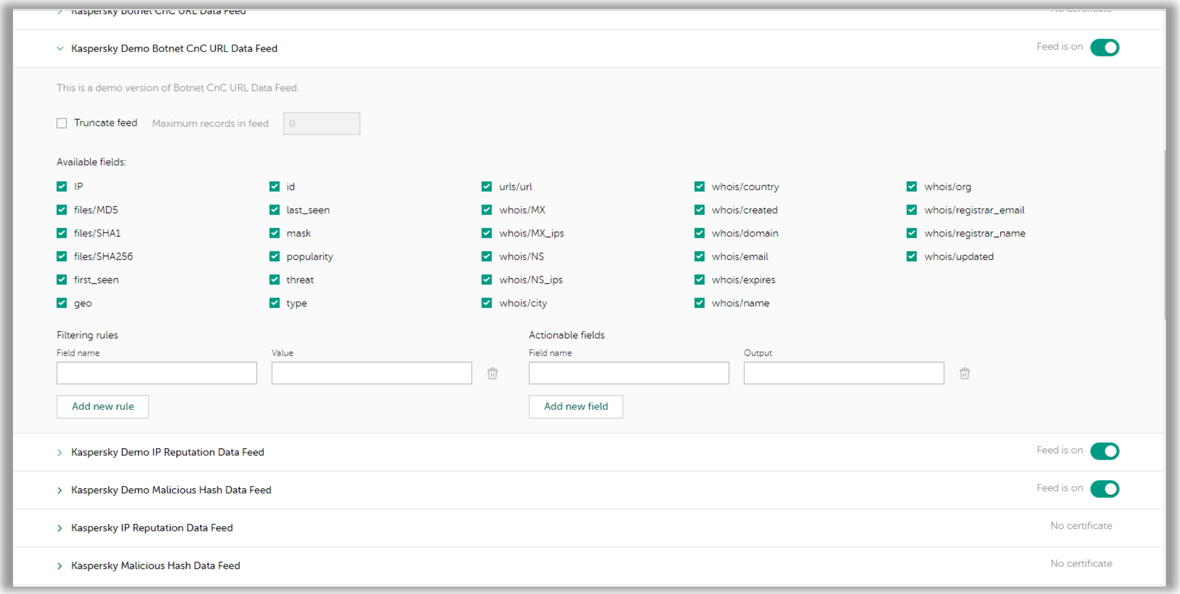
Proxy credentials:

User name	Password

Save · Cancel

© 2019 AO Kaspersky Lab. All Rights Reserved.

- 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.



› Kaspersky Botnet CnC URL Data Feed — No certificate

⌄ Kaspersky Demo Botnet CnC URL Data Feed — Feed is on

This is a demo version of Botnet CnC URL Data Feed.

□ Truncate feed Maximum records in feed: 0

Available fields:

☑ IP
☑ files/MD5
☑ files/SHA1
☑ files/SHA256
☑ first_seen
☑ geo
☑ id
☑ last_seen
☑ mask
☑ popularity
☑ threat
☑ type
☑ urls/url
☑ whois/MX
☑ whois/MX_ips
☑ whois/NS
☑ whois/NS_ips
☑ whois/city
☑ whois/country
☑ whois/created
☑ whois/domain
☑ whois/email
☑ whois/expires
☑ whois/name
☑ whois/org
☑ whois/registrar_email
☑ whois/registrar_name
☑ whois/updated

Filtering rules

Field name	Value

Add new rule

Actionable fields

Field name	Output

Add new field

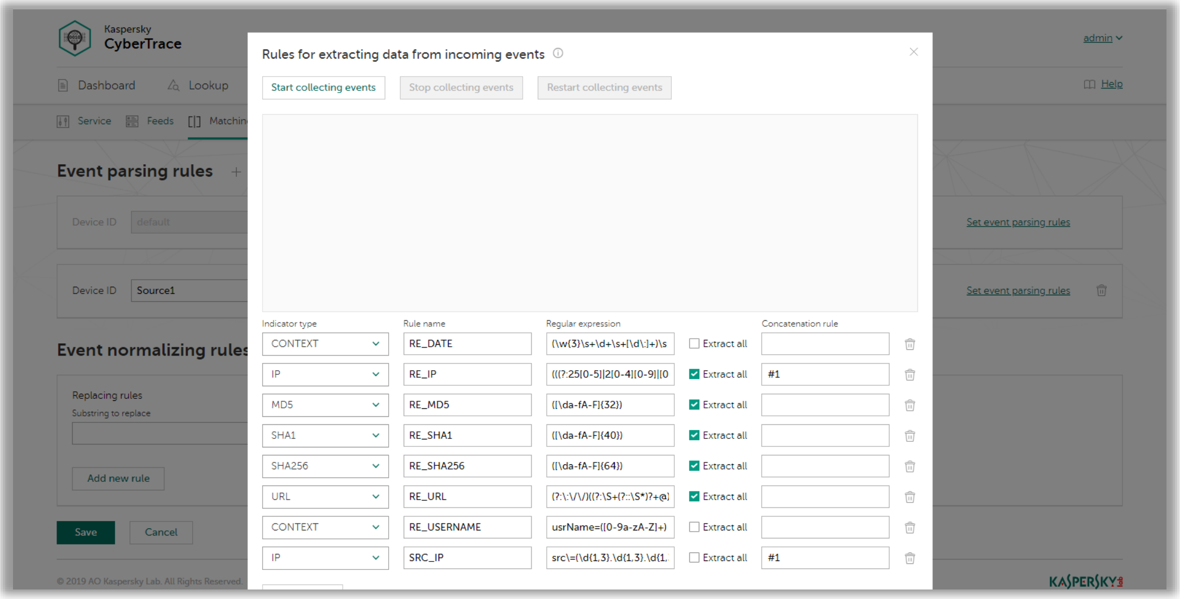
› Kaspersky Demo IP Reputation Data Feed — Feed is on

› Kaspersky Demo Malicious Hash Data Feed — Feed is on

› Kaspersky IP Reputation Data Feed — No certificate

› Kaspersky Malicious Hash Data 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.



Rules for extracting data from incoming events

<table>
<tr><th>Indicator type</th><th>Rule name</th><th>Regular expression</th><th></th><th>Concatenation rule</th></tr>
<tr><td>CONTEXT</td><td>RE_DATE</td><td>(\w{3}\s+\d+\s+[\d\:]+)\s</td><td>☐ Extract all</td><td></td></tr>
<tr><td>IP</td><td>RE_IP</td><td>(((?:25[0-5]|2[0-4][0-9]|[0</td><td>☑ Extract all</td><td>#1</td></tr>
<tr><td>MD5</td><td>RE_MD5</td><td>([\da-fA-F]{32})</td><td>☑ Extract all</td><td></td></tr>
<tr><td>SHA1</td><td>RE_SHA1</td><td>([\da-fA-F]{40})</td><td>☑ Extract all</td><td></td></tr>
<tr><td>SHA256</td><td>RE_SHA256</td><td>([\da-fA-F]{64})</td><td>☑ Extract all</td><td></td></tr>
<tr><td>URL</td><td>RE_URL</td><td>(?:\:\/\/)((?:\S+(?::\S*)?+@]</td><td>☑ Extract all</td><td></td></tr>
<tr><td>CONTEXT</td><td>RE_USERNAME</td><td>usrName=([0-9a-zA-Z]+)</td><td>☐ Extract all</td><td></td></tr>
<tr><td>IP</td><td>SRC_IP</td><td>src\=(\d{1,3}.\d{1,3}.\d{1,</td><td>☐ Extract all</td><td>#1</td></tr>
</table>

- 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:
  - Demo Botnet CnC URL
  - Demo IP Reputation
  - Demo Malicious Hash
  - APT Hash
  - APT IP
  - APT URL
  - Botnet CnC URL
  - Malicious URL
  - Phishing URL
  - IP Reputation
  - Malicious Hash
  - Mobile Botnet
  - Mobile Malicious Hash
  - P-SMS Trojan
  - Ransomware URL
- Out of the box supported OSINT Data Feeds:
  - Abuse.sh_Zeus_Hosts
  - Abuse.sh_Zeus_Configs
  - Abuse.sh_Zeus_Binaries
  - Abuse.sh_Zeus_Dropzones
  - Abuse.sh_Zeus_BadIP
  - Abuse.sh_Zeus_BadDomain
  - Abuse.sh_Zeus_BlockIP
  - Abuse.sh_Zeus_BlockDomain
  - Abuse.sh_Ransomware_Common
  - Abuse.sh_Ransomware_BlockUrl
  - Abuse.sh_Ransomware_BlockDomain
  - Abuse.sh_Ransomware_BlockIP
  - Abuse.sh_Feodo_BlockIP
  - EmergingThreats_BlockIP
  - 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