kaspersky

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

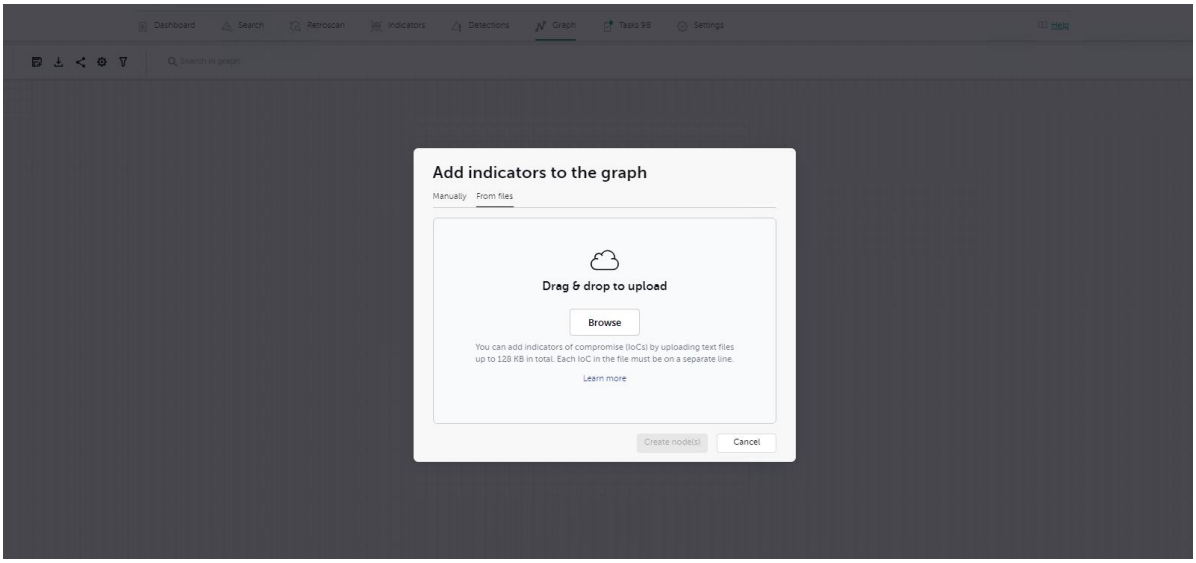
RELEASE DATE: 31.03.2022

OPERATING SYSTEM: WINDOWS AND LINUX

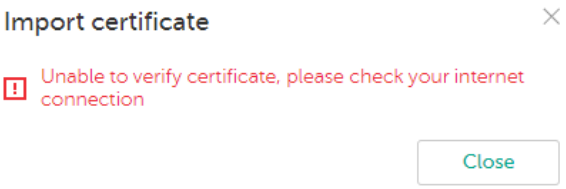
HARDWARE PLATFORM: X86_64

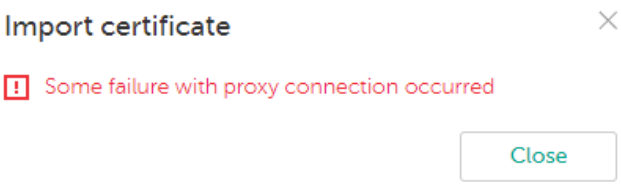
New features:

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



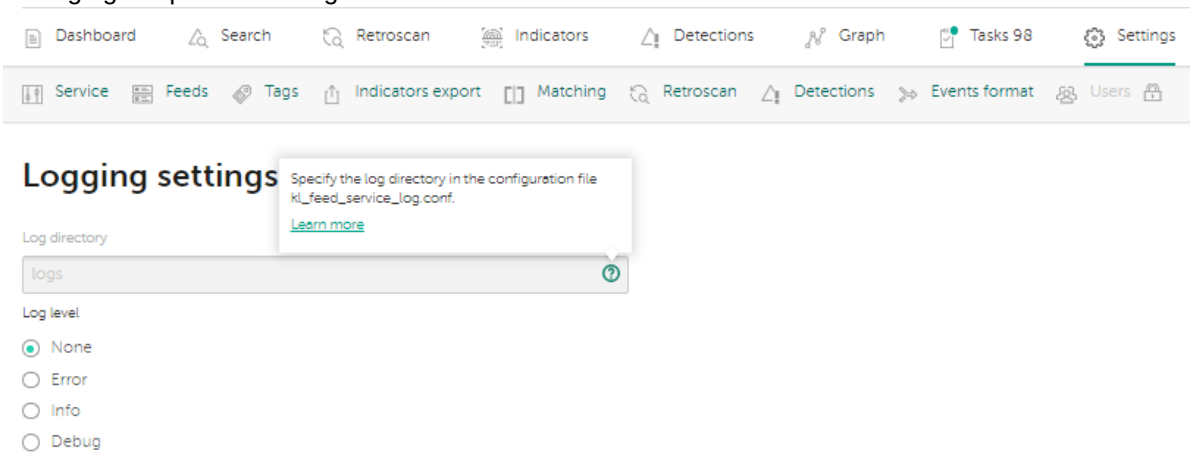
- Kaspersky CyberTrace displays a message when a certificate is added and there is no Internet connection or the proxy settings are incorrect.



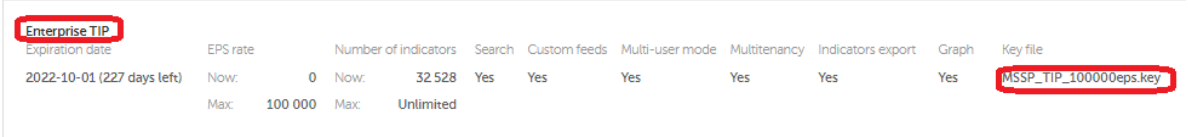


Change log

- 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.



- 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.



kaspersky

RELEASE 4.1 FP1

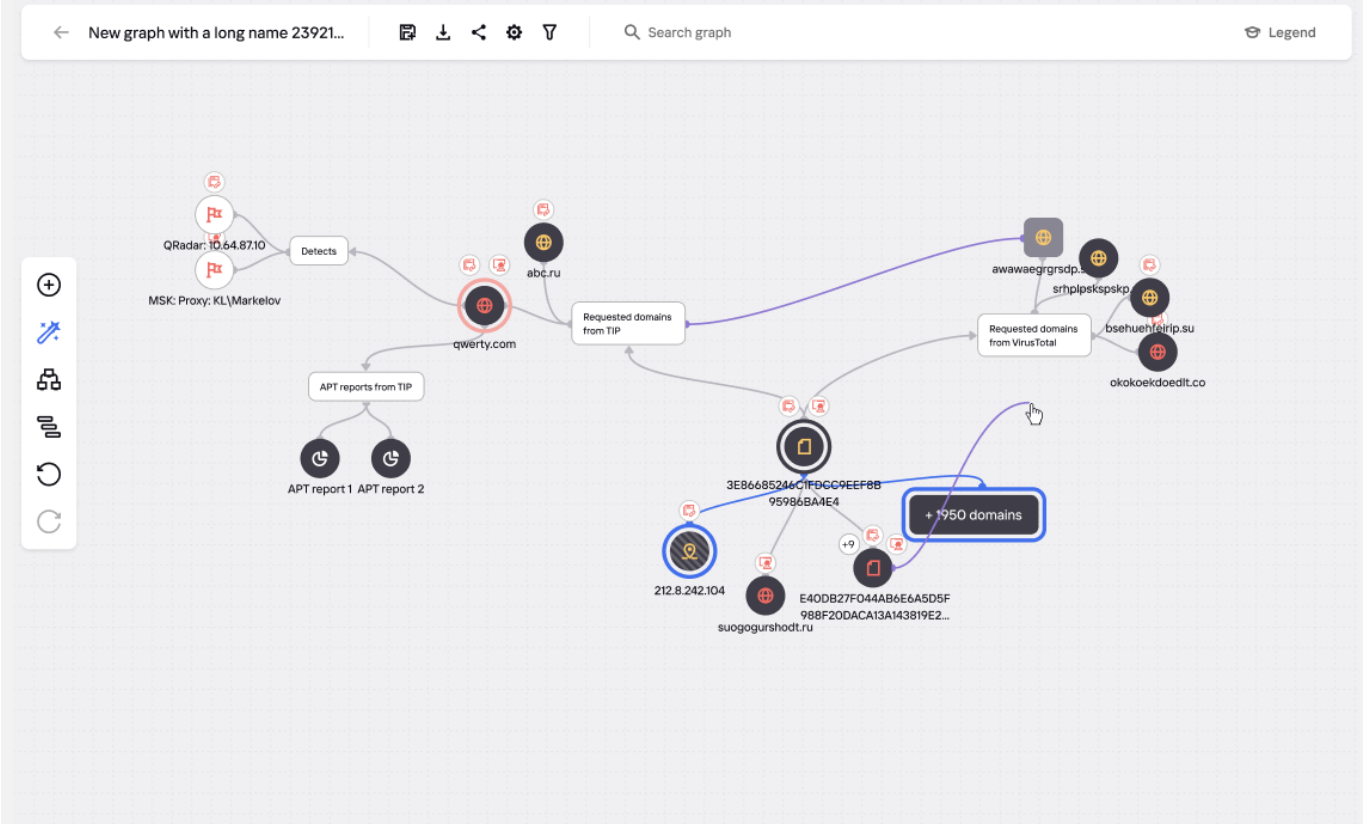
RELEASE DATE: 15.10.2021

OPERATING SYSTEM: WINDOWS AND LINUX

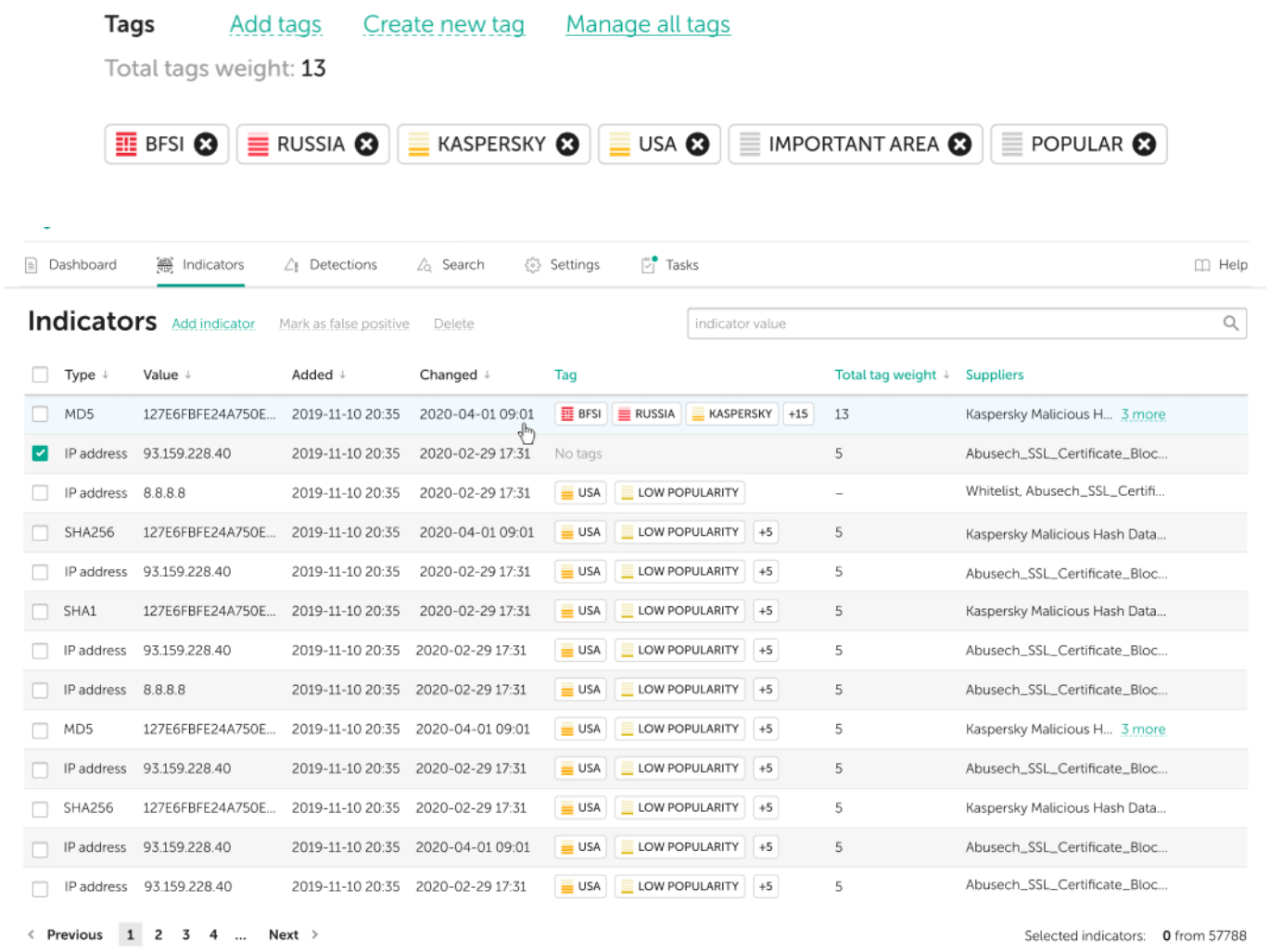
HARDWARE PLATFORM: X86_64

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.



Change log

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

kaspersky

RELEASE 4.0.1.319

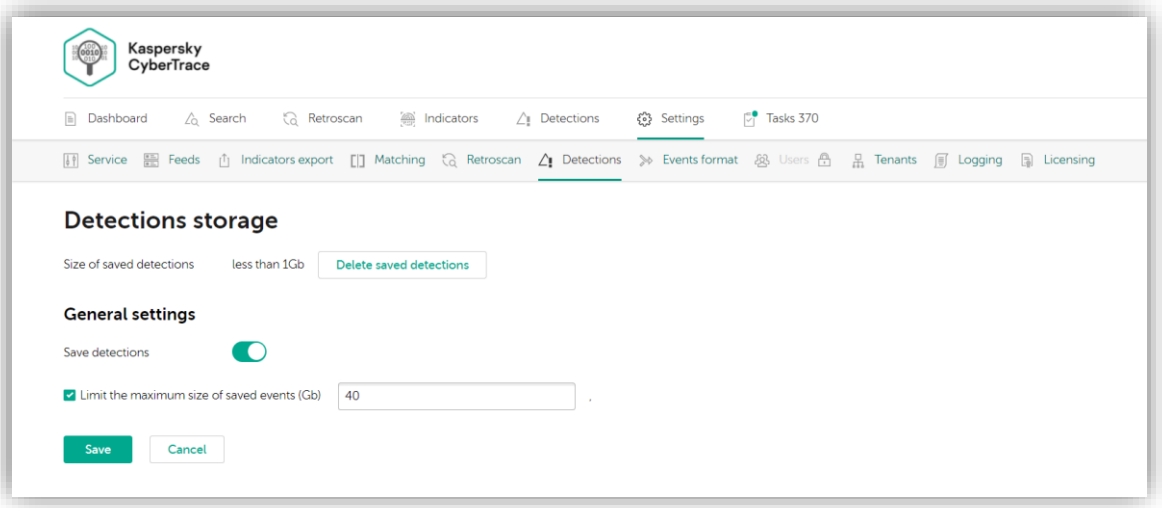
RELEASE DATE: 1.06.2021

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;



- High Availability mode (HA) for the following CyberTrace features was added to increase fault tolerance:
  - 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)

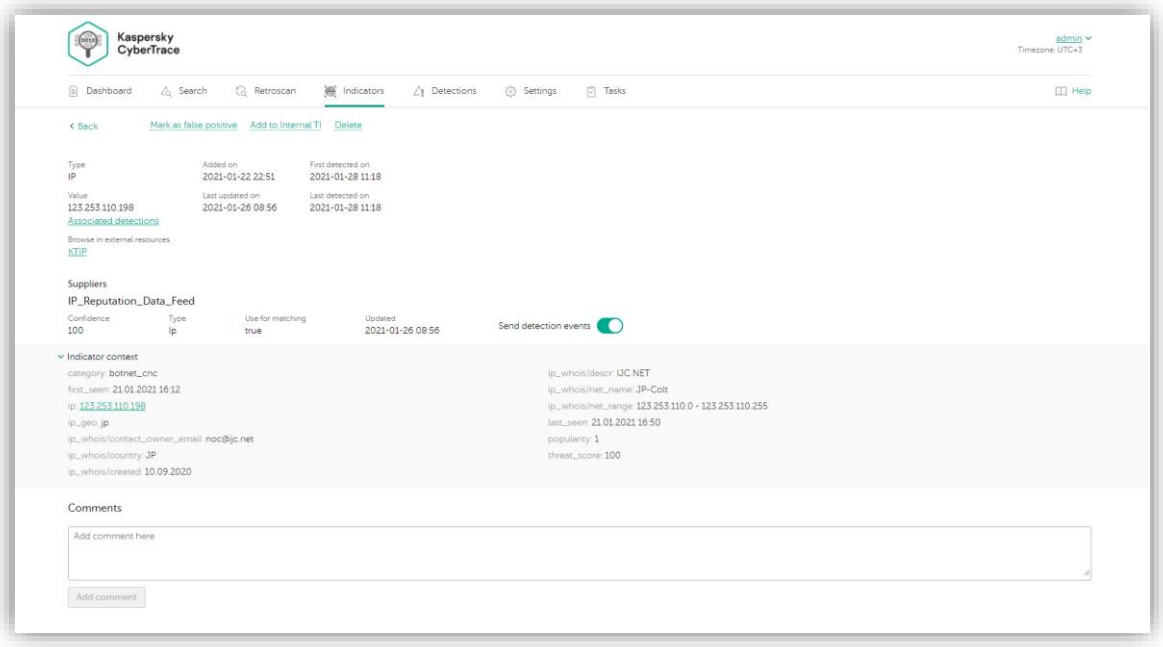
RELEASE DATE: 26.01.2021

OPERATING SYSTEM: WINDOWS AND LINUX

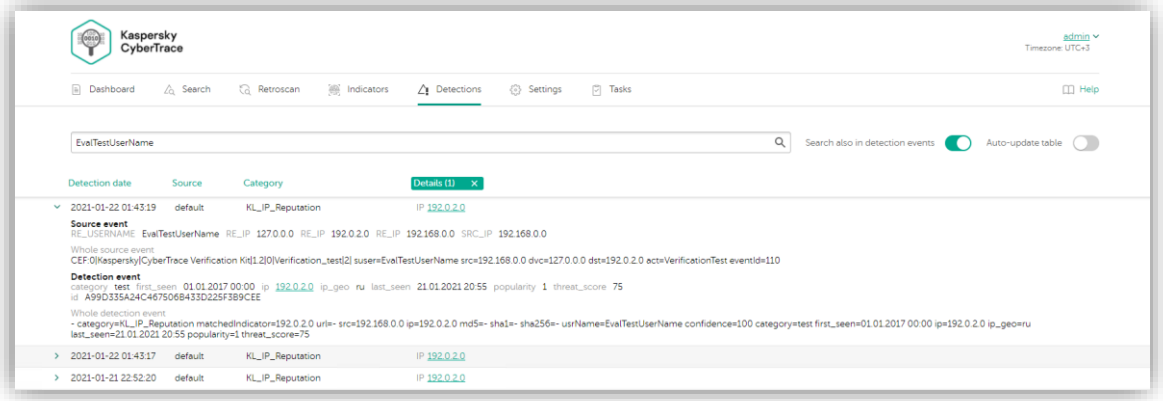
HARDWARE PLATFORM: X86_64

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.



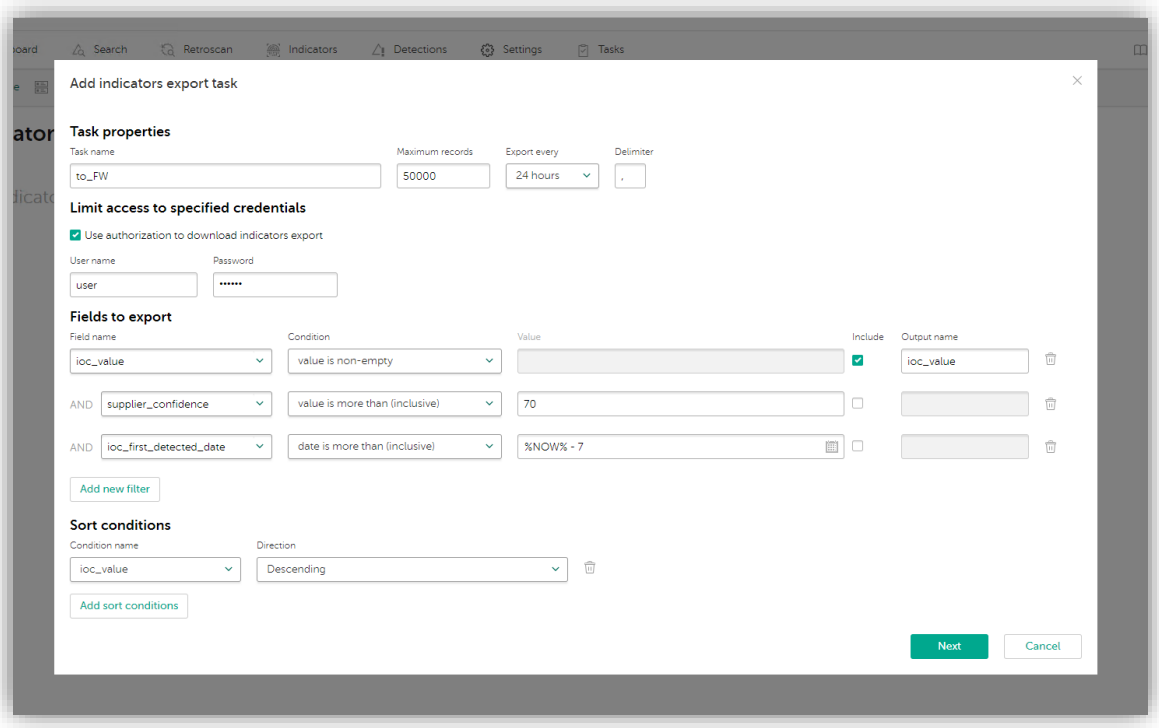
- Storage for detections was added to simplify security monitoring and alerts triage processes. The raw event from the source and full information about the detection are saved to the database for future analysis. The detection list supports searching over the saved data to find all detections by threat,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



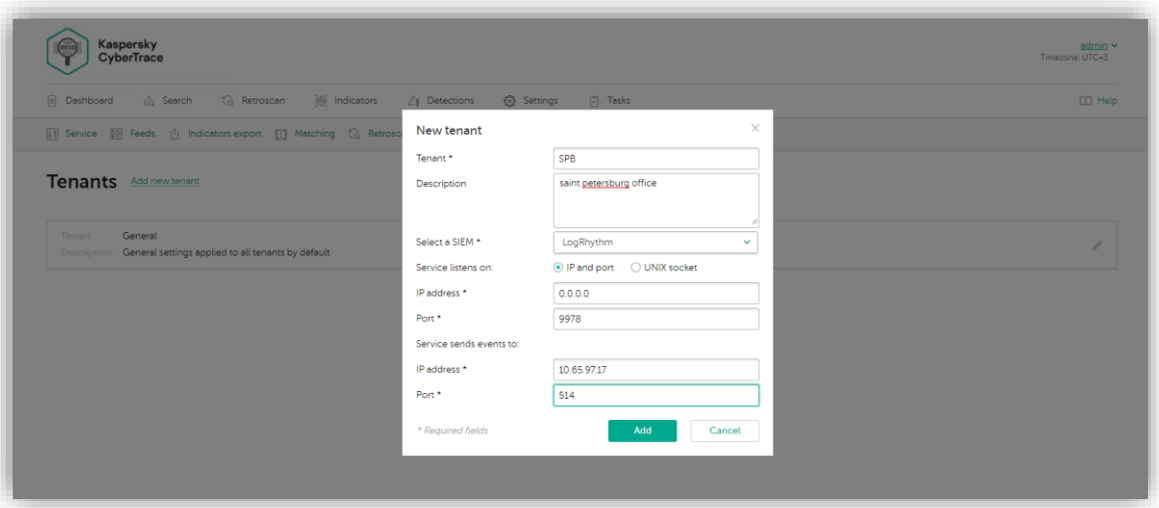
- Filter for sending detection events to SIEM solutions was added to reduce the load on the solutions and on the Analyst (fighting with alerts fatigue). It allows to send to SIEM solutions only the most dangerous and

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.



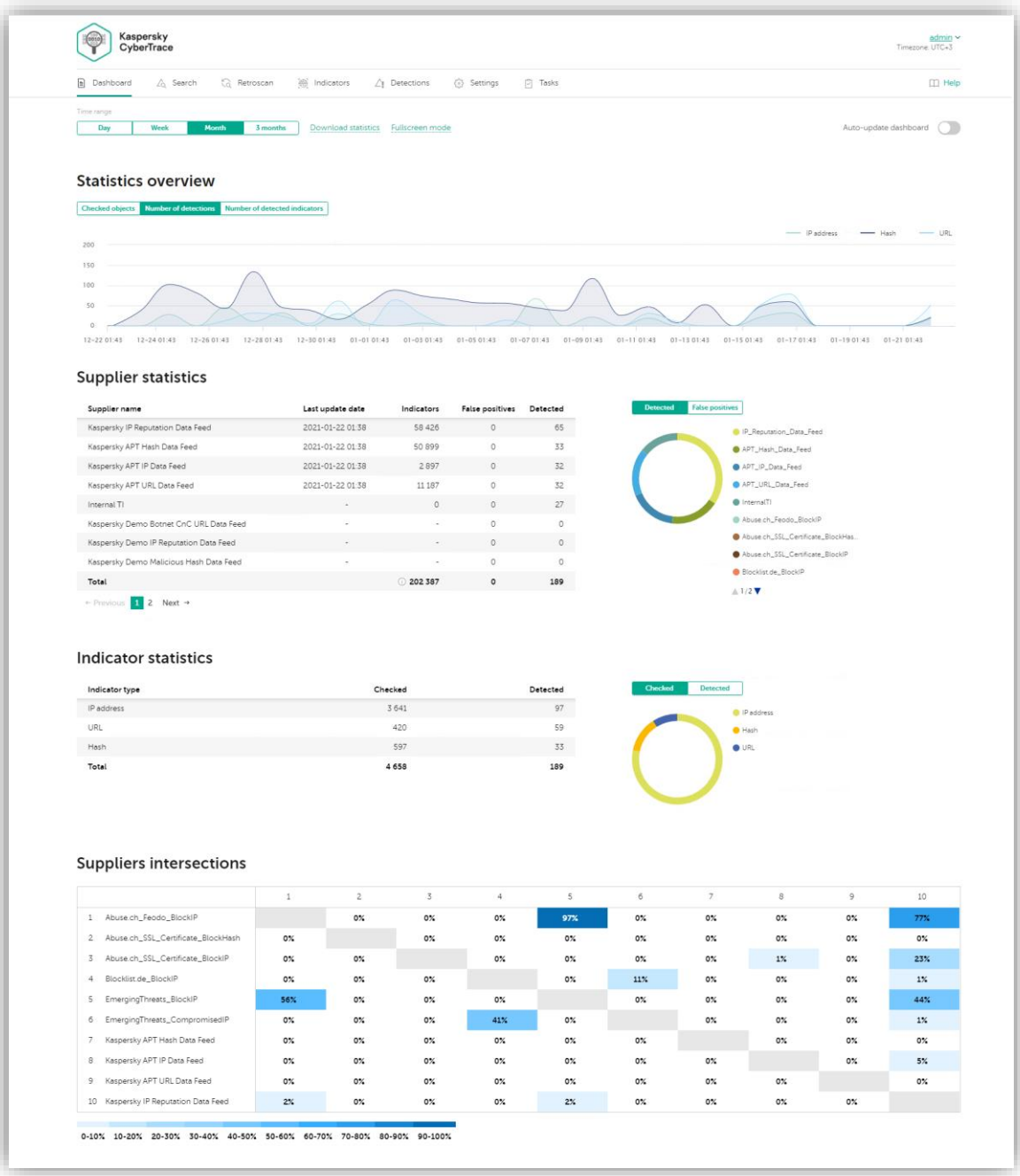
- Multitenancy feature was added to support MSSP or Large Enterprise use cases when a service provider (central office) needs to handle events from different branches (tenants) separately. The feature allows to connect a single Kaspersky CyberTrace instance with different SIEM solutions from different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



- 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.



- 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.

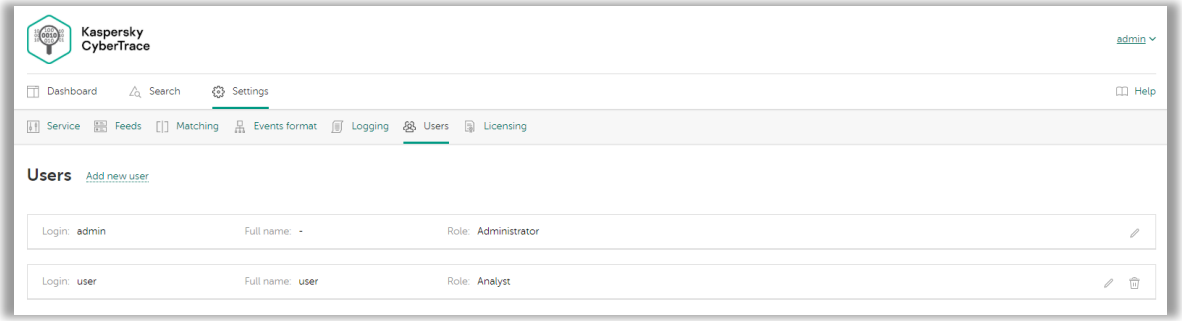
RELEASE 3.1.0.1204

OPERATING SYSTEM: WINDOWS AND LINUX

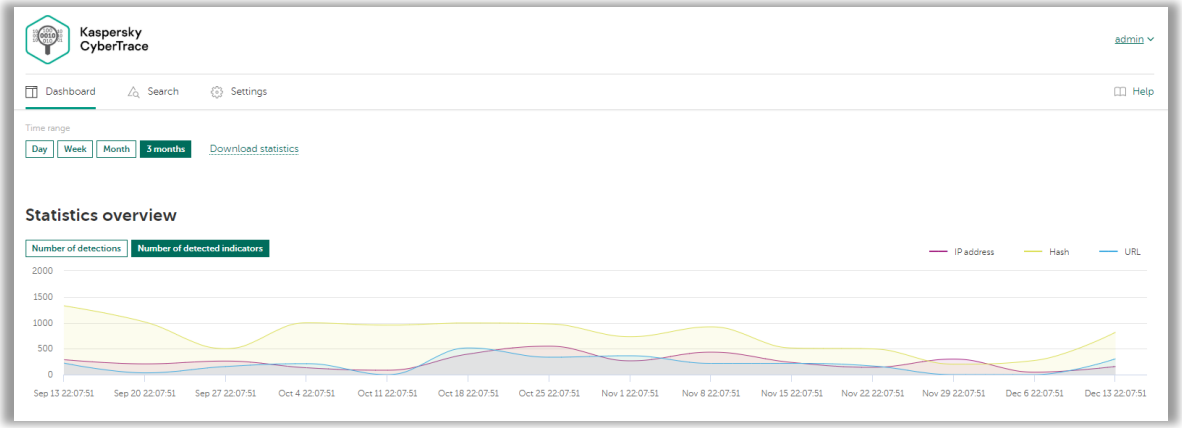
HARDWARE PLATFORM: X86_64

Change log

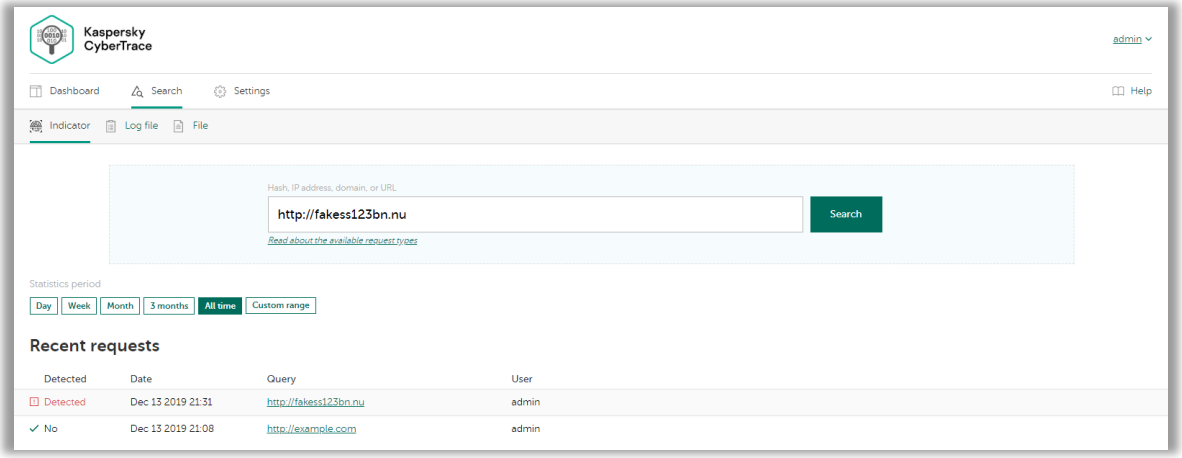
- Multiuser mode was added. Now you can use role-based access features to control the operations that different users manage. For example, only users with the Administrator role can manage Kaspersky CyberTrace configuration and browse the search results of all analysts.



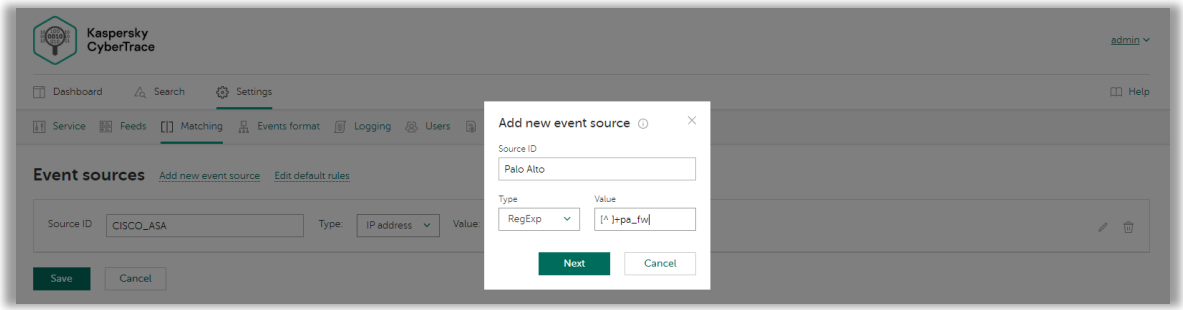
- Support for downloadable reports was added. The reports contain Kaspersky CyberTrace statistics that are valuable for measuring the effectiveness of Threat Intelligence to inform the management team about the value brought by each TI source.



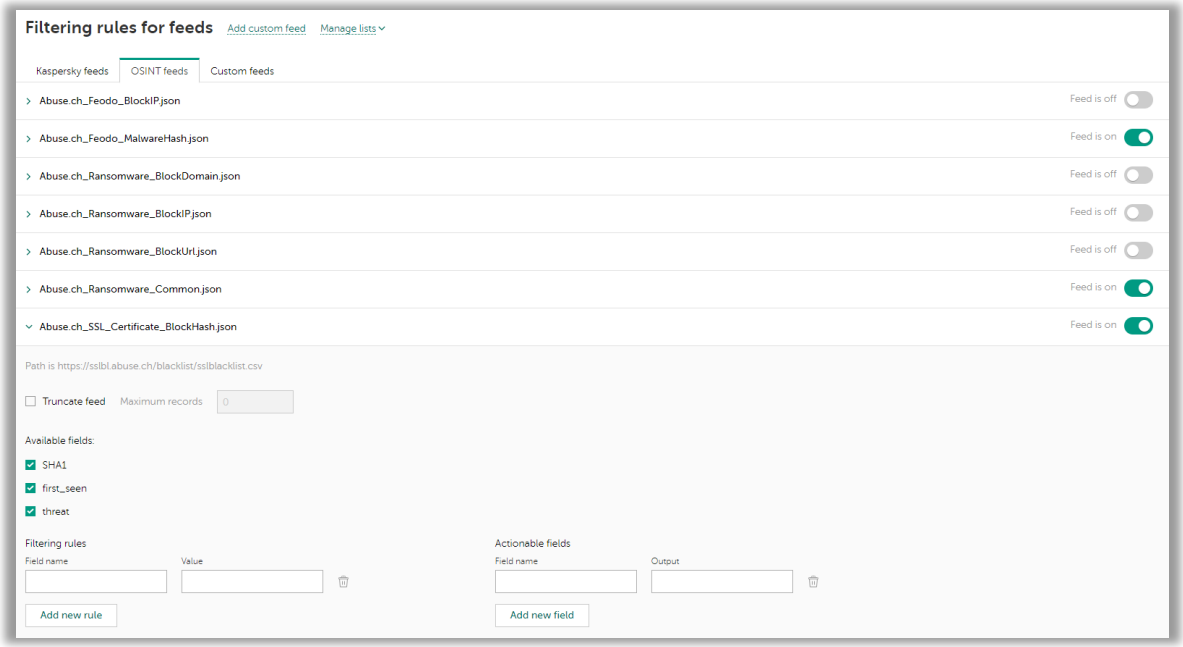
- Search history was added to improve the user experience during Incident Response activities. Analysts now have immediate access to full historical results of searched observables and log file checks.



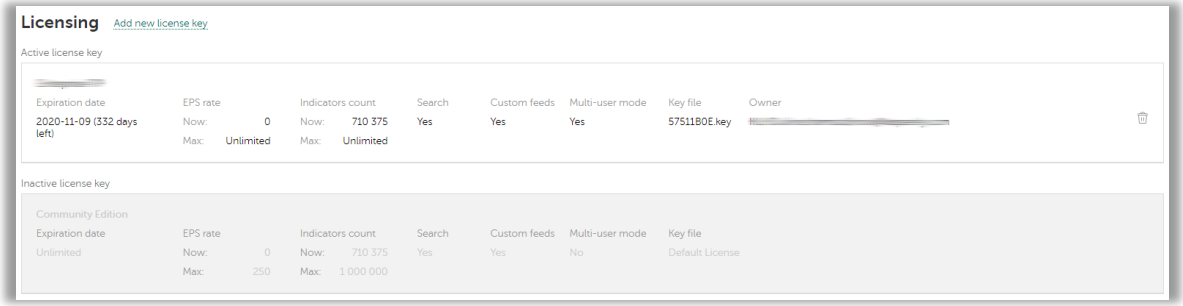
- Event Sources management was improved:
  - Normalization for each source was added to support events from a broad range of sources in a single Kaspersky CyberTrace instance. For example, from different SIEMs like McAfee and QRadar.
  - Determining the source based on regular expressions was added to 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.



- 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.



- 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).



- 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.

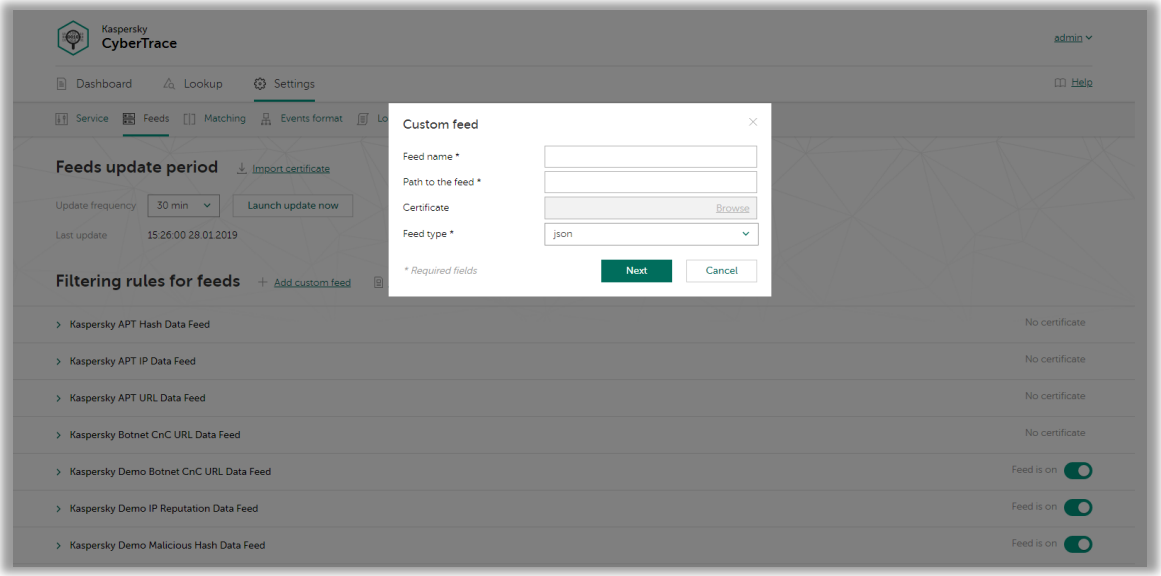
RELEASE 3.0.0.382

OPERATING SYSTEM: WINDOWS AND LINUX

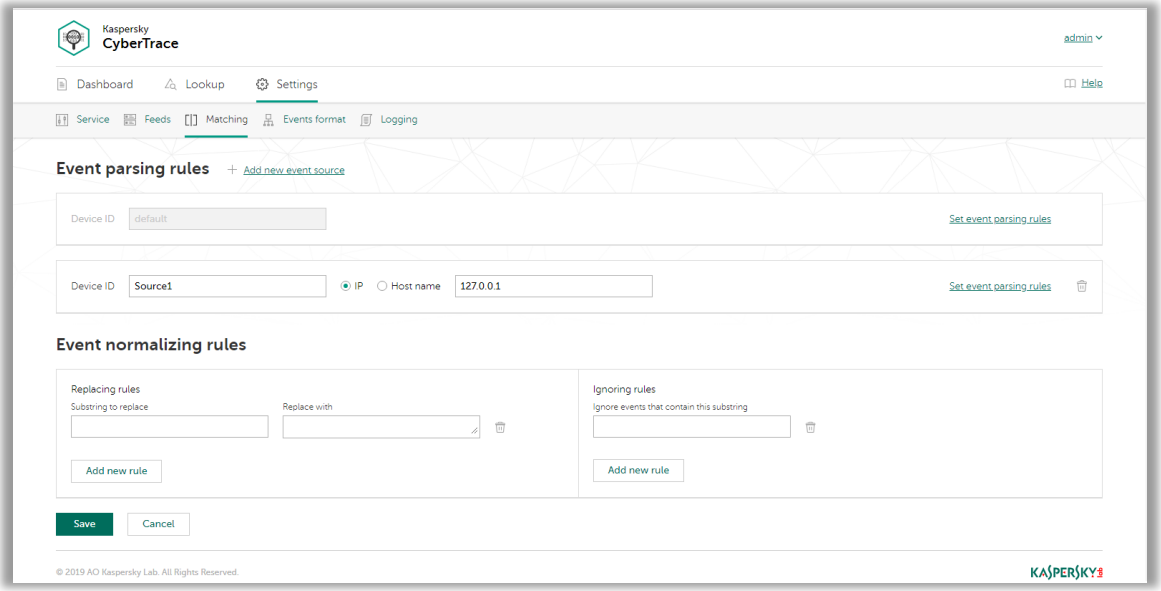
HARDWARE PLATFORM: X86_64

Features

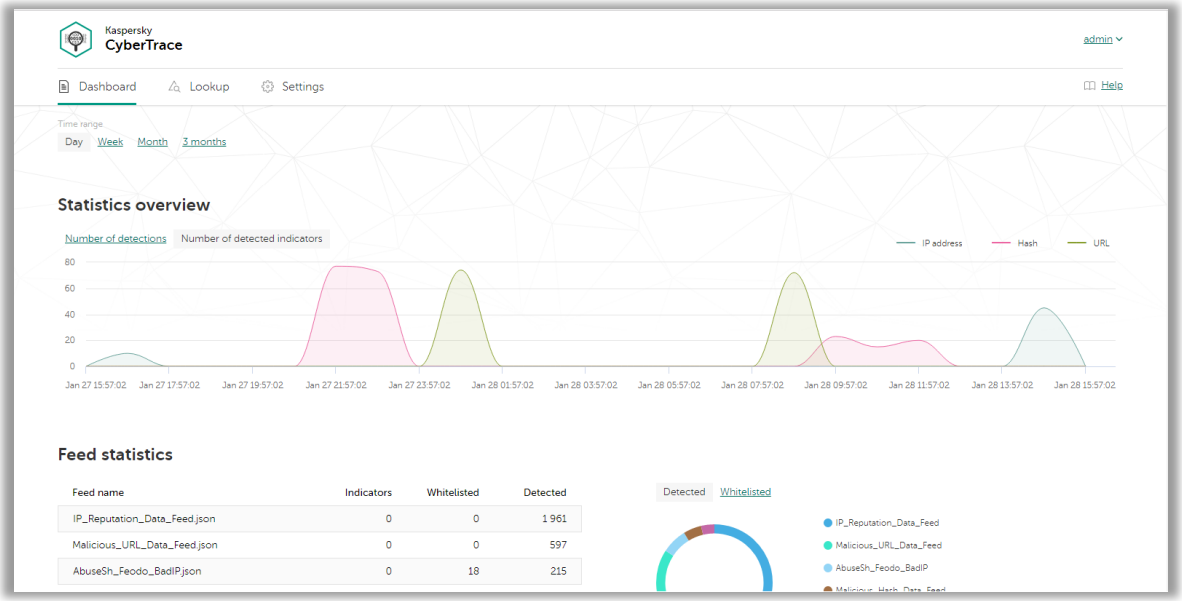
- Kaspersky CyberTrace Web, a web user interface for Kaspersky CyberTrace, provides data visualization, on-demand IoC lookup functionality and access to Kaspersky CyberTrace configuration. Kaspersky CyberTrace Web also supports the management of feeds, log parsing rules, blacklists and whitelists and 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.



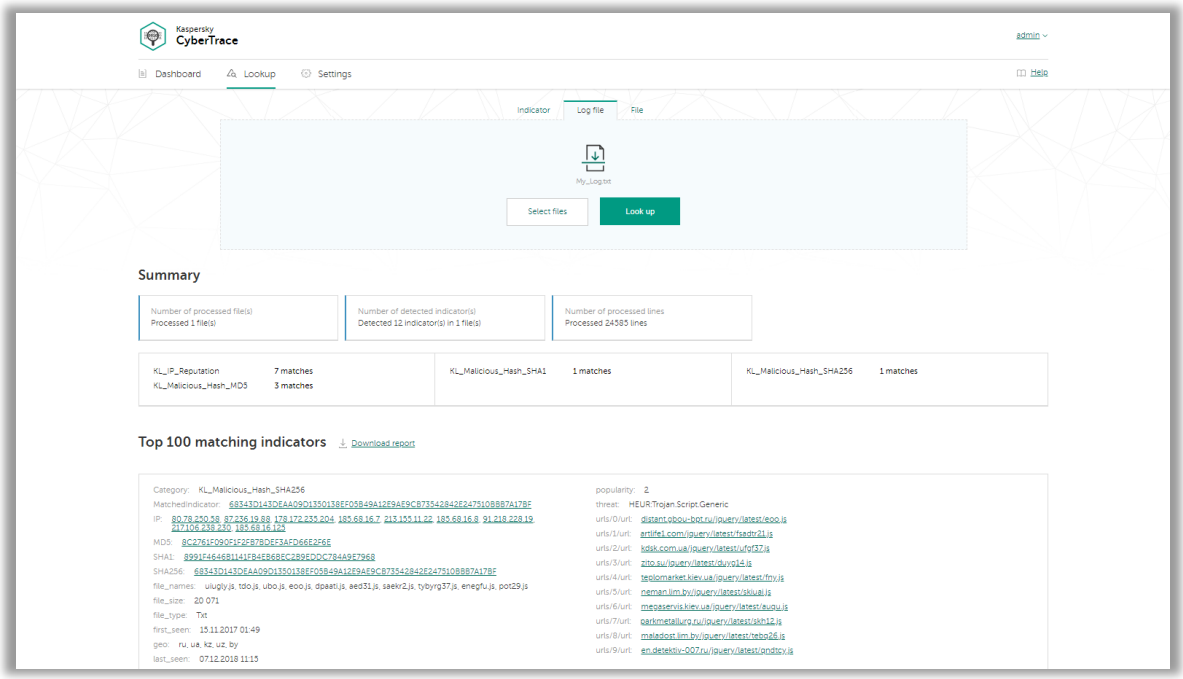
- Internalized process of parsing and matching incoming data significantly reduces SIEM solution load. Kaspersky CyberTrace parses incoming logs and events, matches the resulting data to feeds, and generates its own alerts on threat detection. Consequently, a SIEM solution has to process less data.



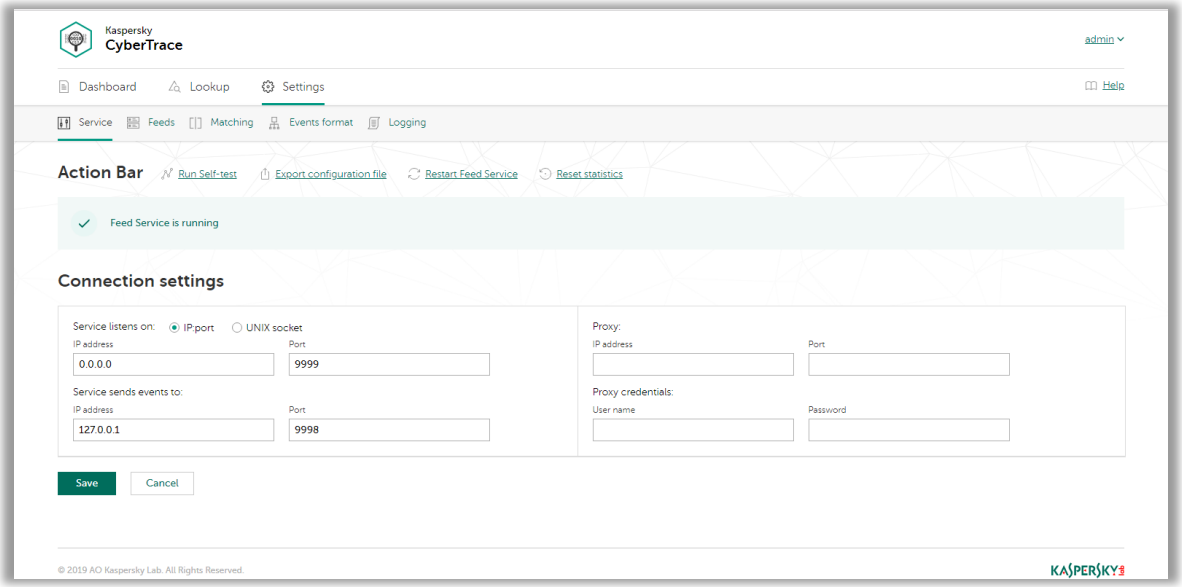
- Generates feed usage statistics for measuring the effectiveness of feeds.



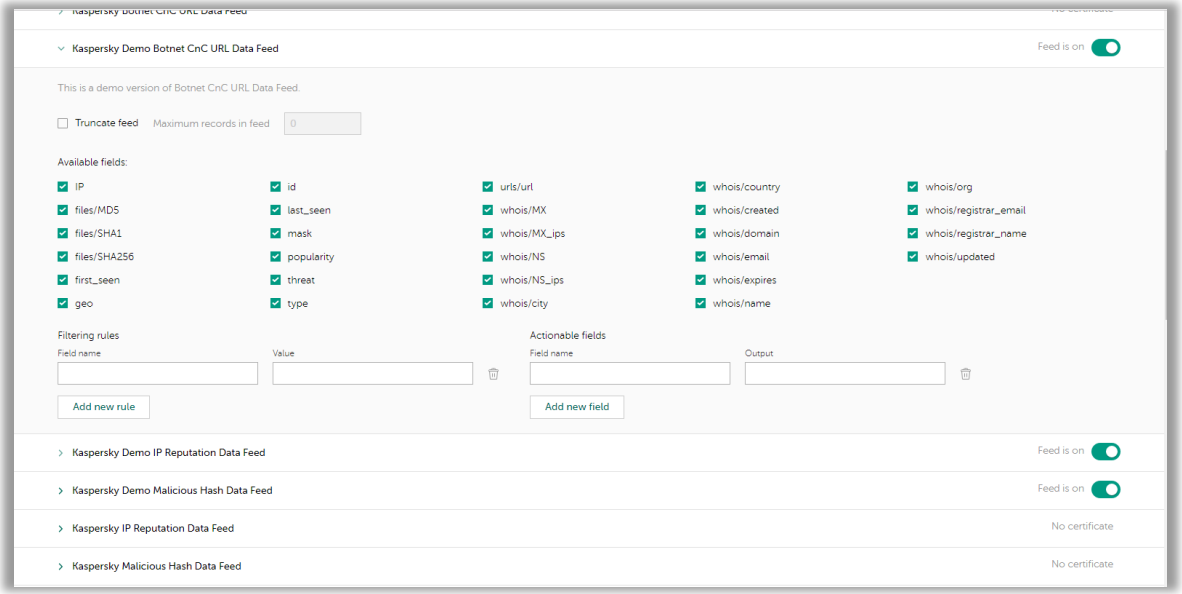
- In-depth threat investigation via on-demand lookup of indicators (hashes, IP addresses, domains, URLs). Bulk scanning of logs and files is also supported.



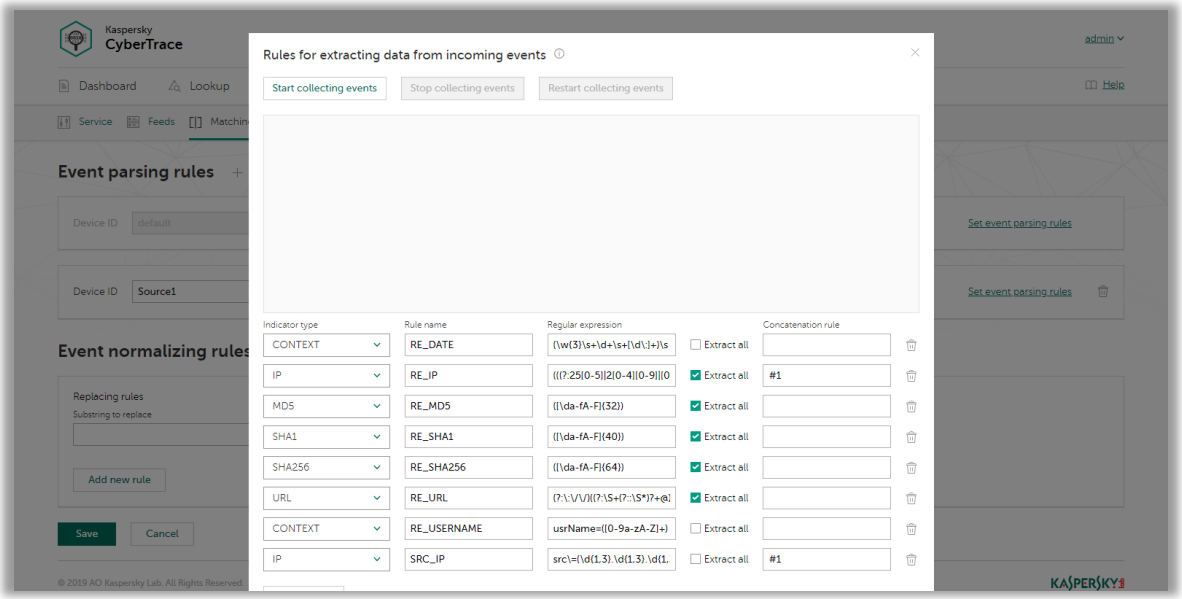
- Export lookup results that match data feeds to CSV format for integration with other systems (firewalls, network and host IDS, custom tools).
- Universal approach to integration of threat matching capabilities with SIEMs and other security controls. SIEM connectors for a wide range of SIEM solutions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



- 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.



- 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