kaspersky BRING ON THE FUTURE

Kaspersky CyberTrace

The number of security alerts processed by information security analysts every day is growing exponentially. With this amount of data being analyzed, effective alert prioritization, triage and validation is nearly impossible. There are too many blinking lights coming from numerous security products, leading to important alerts getting buried in the noise, and analyst burnout. SIEMs, log management and security analytics tools aggregating security data and correlating related alarms all help to reduce the number of alerts warranting additional examination, but security analysts remain extremely overloaded.

Threat intelligence comes in different formats and includes a huge number of Indicators of Compromise (IoCs), making it hard for SIEMs or network security controls to digest them.

Enabling effective alert triage and analysis

By integrating up-to-the-minute machine-readable threat intelligence into existing security controls, like SIEM systems, Security Operation Centers can automate the initial triage process while providing their security analysts with enough context to immediately identify alerts that need to be investigated or escalated to incident response teams for further investigation and response. However, the continuing growth in the number of threat data feeds and available threat intelligence sources makes it difficult for organizations to determine what information is relevant for them. Threat intelligence comes in different formats and includes a huge number of Indicators of Compromise (IoCs), making it hard for SIEMs or network security controls to digest them.

Kaspersky CyberTrace is a Threat Intelligence Platform that enables seamless integration of threat data feeds with SIEM solutions to help analysts leverage threat intelligence in their existing security operations workflows more effectively. It integrates with any threat intelligence feed in JSON, STIX, XML and CSV formats you might want to use (threat intelligence feeds from Kaspersky, other vendors, OSINT or your custom feeds), and supports out-of-the-box integration with numerous SIEM solutions and log sources.

Kaspersky CyberTrace uses an internalized process of parsing and matching incoming data, which significantly reduces SIEM workload. It parses incoming logs and events, rapidly matches the resulting data to feeds, and generates its own alerts on threat detection. A high-level architecture of the solution integration is shown in the Figure below:

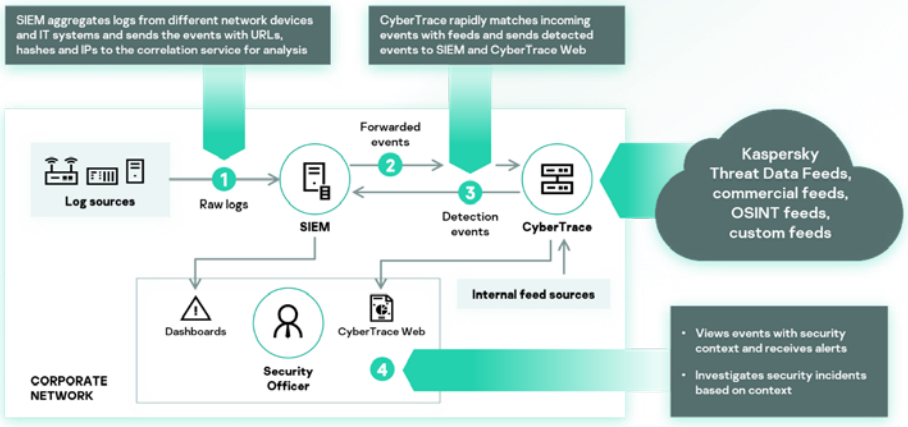

Figure 1. Kaspersky CyberTrace integration scheme

Product features

Kaspersky CyberTrace provides a set of instruments to operationalize threat intelligence for conducting effective alert triage and initial response:

- A database of indicators with full text search and the ability to search using advanced search queries enables complex searches across all indicator fields, including context fields. Filtering results by intelligence supplier simplifies the process of analyzing threat intelligence.
- Pages with detailed information about each indicator provide even deeper analysis. Each page presents all information about an indicator from all threat intelligence suppliers (deduplication) so analysts can discuss threats in the comments and 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.

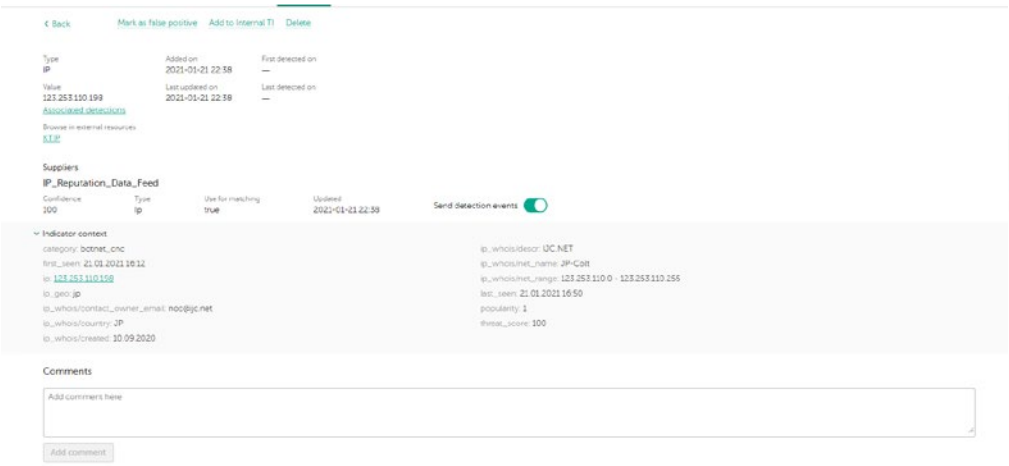

Figure 2. Detailed information about an indicator from all threat intelligence suppliers

- A Research Graph allows to visually explore data and detections stored in CyberTrace and discover threat commonalities. It allows graphic visualization of the relationship between URLs, domains, IPs, files, and other contexts encountered during investigations. The graph includes the following features: transformations, mini graph, grouping nodes, manually adding of links, adding indicators and searching for nodes on the graph.

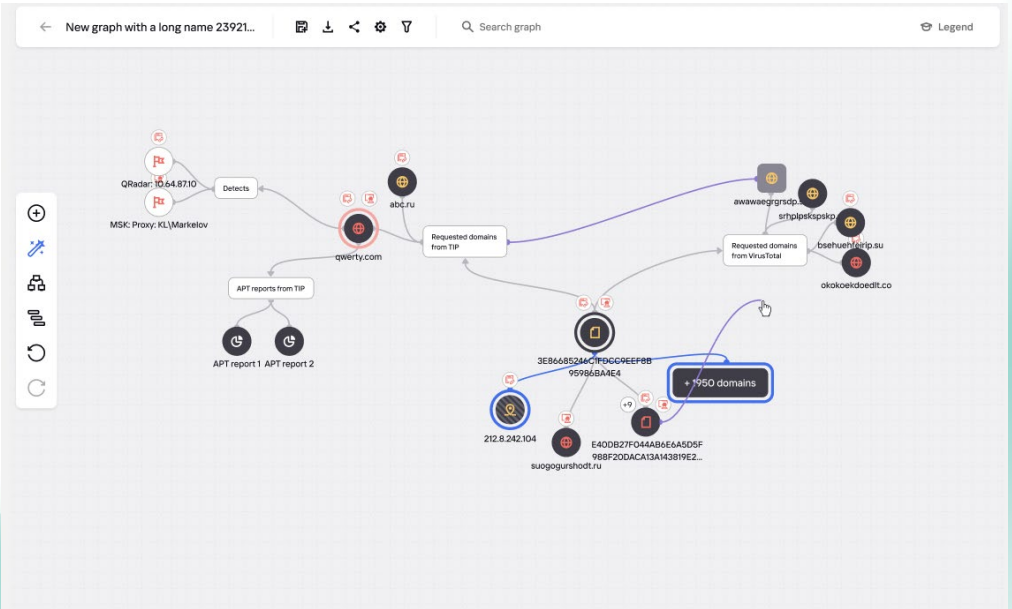

Figure 3. Research Graph

- The indicators export feature supports exporting indicator sets to security controls such as policies lists (block lists) as well as the sharing of threat data between Kaspersky CyberTrace instances or with other TI Platforms.

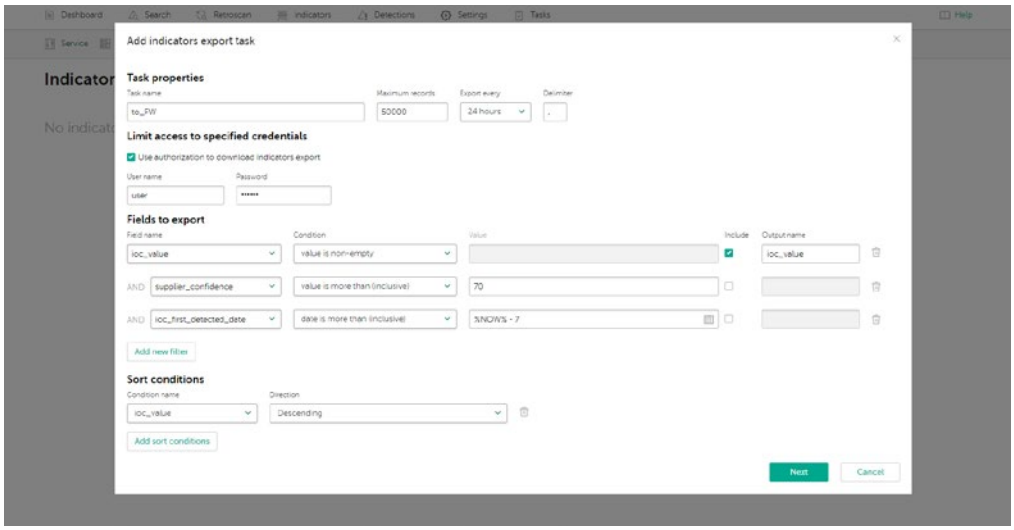

Figure 4. Indicators export task

- Tagging IoCs simplifies their management. You can create any tag and specify its weight (importance) and use it to tag IoCs manually. You can also sort and filter IoCs based on these tags and their weights.

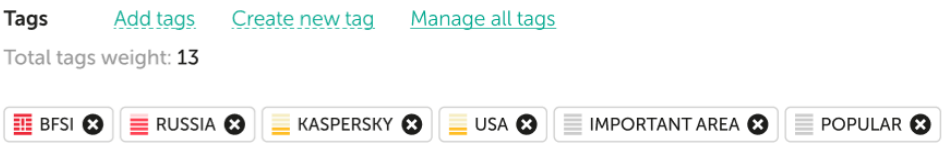

Figure 5. IoC tags

- The historical correlation feature (retroscan) lets you analyze observables from previously checked events using the latest feeds to find previously uncovered threats. All historical detections are included in the report for future investigations.
- A filter for sending detection events to SIEM solutions reduces the load on them and on the analyst battling alert fatigue. It allows you to send only the most dangerous detections, those that must be treated as incidents, to SIEM. All other detections are saved to the internal database and can be used during root cause analysis or in threat hunting.
- Multitenancy supports MSSPs or large enterprise use cases when a service provider (central office) needs to handle events from different branches (tenants) separately. This allows a single Kaspersky CyberTrace instance to be connected with different SIEM solutions from different tenants, and you can configure which feeds are to be used for each tenant.

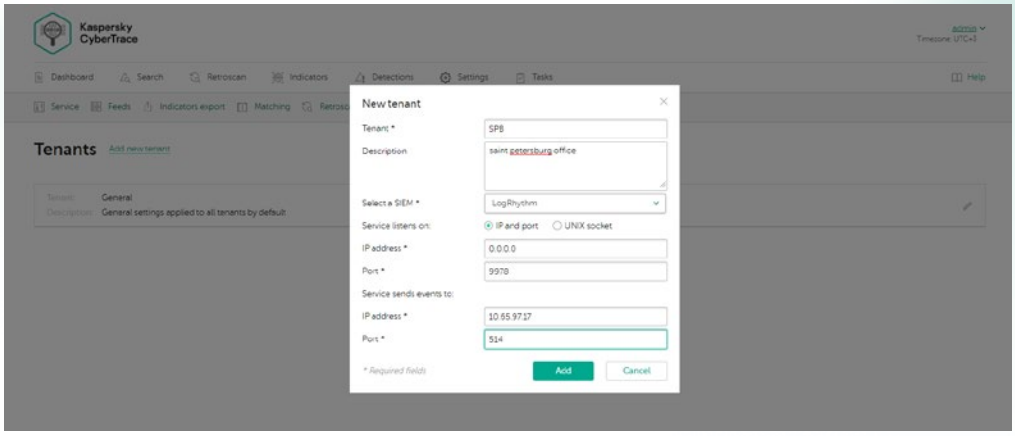

Figure 6. New tenant creation

- Feed usage statistics for measuring the effectiveness of the integrated feeds and feeds intersection matrix help choosing the most valuable threat intelligence suppliers.

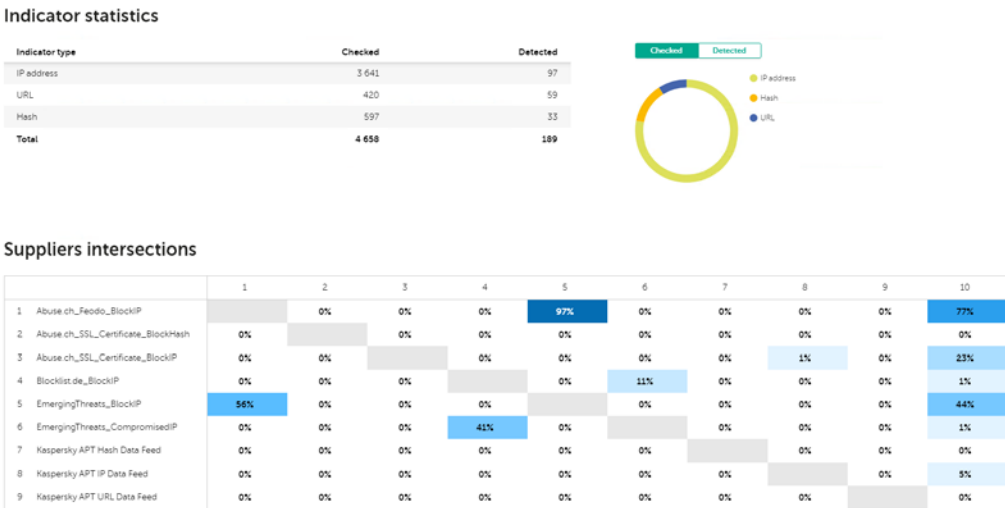

Figure 7. Indicator statistics and feeds intersection matrix

Other product features:

- SIEM connectors for a wide range of SIEM solutions to visualize and manage data about threat detections
- On-demand lookup of indicators (hashes, IP addresses, domains, URLs) for in-depth threat investigation
- Advanced filtering for feeds
- Bulk scanning of logs and files
- Command-line interface for Windows and Linux platforms
- Stand-alone mode, where Kaspersky CyberTrace receives and parses the logs from various sources such as network devices
- And much more

- HTTP RestAPI allows you to look up and manage threat intelligence. By using the Rest API, Kaspersky CyberTrace can be easily integrated into complex environments for automation and orchestration.
- Integration with Kaspersky Unified Monitoring and Analysis Platform (KUMA) is supported, including Web UI integration (single UI).

Although Kaspersky CyberTrace and Kaspersky Threat Data Feeds can be used separately, when used together they significantly strengthen your threat detection capabilities, empowering your security operations with global visibility into cyberthreats. With Kaspersky CyberTrace and Kaspersky Threat Data Feeds, organizations can:

- Effectively distill and prioritize security alerts
- Reduce analyst workload and prevent burnout
- Immediately identify critical alerts and make more informed decisions about which should be escalated to incident response teams
- Build a proactive and intelligence-driven defense.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. This is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Find out more at kaspersky.com/transparency

Proven.
Transparent.
Independent.