Kaspersky® CyberTrace

The number of security alerts processed by Security Operations Center's Tier 1 analysts every day is growing exponentially. With this amount of data being analyzed, effective alert prioritization, triage and validation becomes nearly impossible. There are too many blinking lights coming from numerous security products, leading to significant 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 Tier 1 specialists remain extremely overloaded.

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 Tier 1 specialists with enough context to immediately identify alerts that need to be investigated or escalated to Incident Response (IR) 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 is provided 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.

The Kaspersky CyberTrace is a threat intelligence fusion and analysis tool enabling seamless integration of threat data feeds with SIEM solutions to help analysts leverage threat intelligence in their existing security operations workflow 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), supporting out-of-the-box integration with numerous SIEM solutions and log sources. By automatically matching the logs against threat intelligence feeds, the Kaspersky CyberTrace provides real-time 'situational awareness', allowing Tier 1 analysts to make timely and better informed decisions.

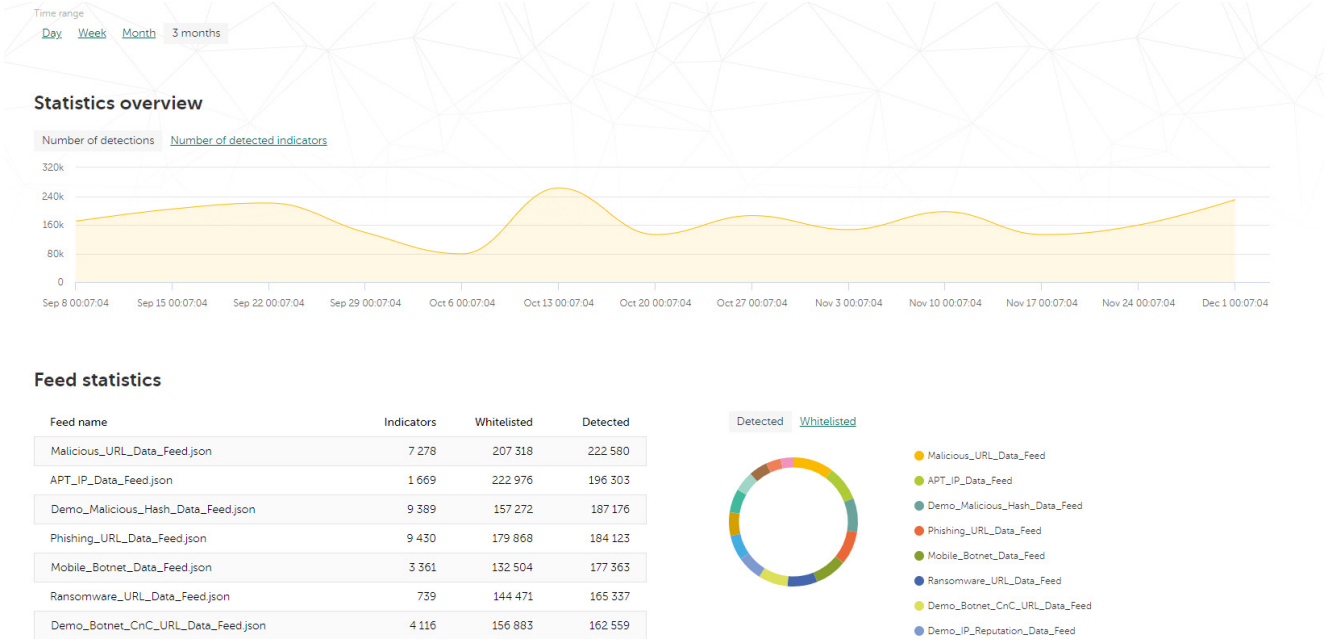


Figure 1. Kaspersky CyberTrace statistics

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

- Demo threat data feeds from Kaspersky Lab and OSINT feeds are available out-of-the-box
- SIEM connectors for a wide range of SIEM solutions to visualize and manage data about threat detections
- Feed usage statistics for measuring the effectiveness of the integrated feeds
- On-demand lookup of indicators (hashes, IP addresses, domains, URLs) for in-depth threat investigation
- A web user interface providing data visualization, access to configuration, feed management, log parsing rules, blacklists and whitelists
- Advanced filtering for feeds (based on the context provided with each of the indicators, including threat type, geolocation, popularity, time stamps and more) and log events (based on custom conditions)
- Export of lookup results matching data feeds to CSV format for integration with other systems (firewalls, network and host IDS, custom tools)
- Bulk scanning of logs and files
- Command-line interface for Windows and Linux platforms
- Stand-alone mode, where Kaspersky CyberTrace is not integrated with a SIEM but receives and parses the logs from various sources such as networking devices
- Installation in DMZ-supporting scenarios where it needs to be isolated from the Internet.

The tool uses an internalized process of parsing and matching incoming data, which significantly reduces SIEM workload. Kaspersky CyberTrace 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:

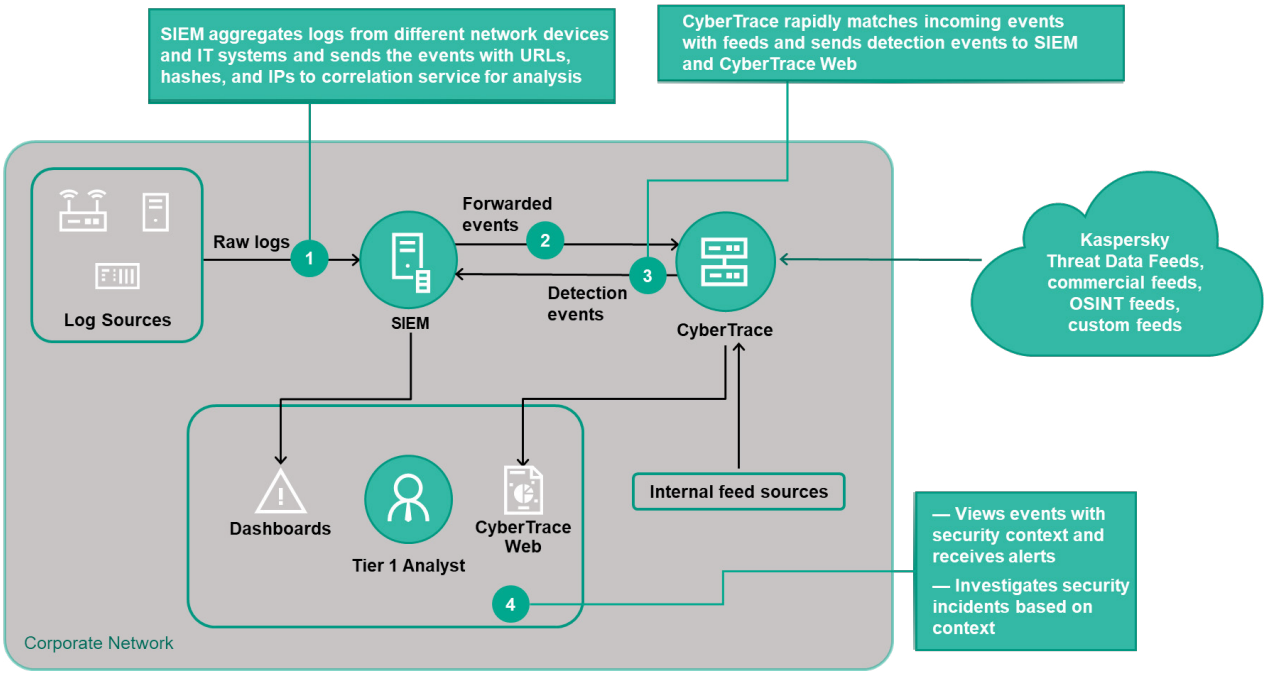


Figure 2. Kaspersky CyberTrace integration scheme

Kaspersky Lab also offers a set of continuously updated threat data feeds that can be integrated with the Kaspersky CyberTrace enabling global threat visibility, timely detection of cyber threats, prioritization of security alerts and effective response to information security incidents:

- IP reputation feed – a set of IP addresses with context covering different categories of suspicious and malicious hosts
- Malicious and phishing URL feed – covering malicious and phishing links and websites
- Botnet C&C URL feed – covering desktop botnet C&C servers and related malicious objects
- Mobile botnet C&C URL feed – covering mobile botnet C&C servers

- Ransomware URL feed – covering links that host ransomware objects or that are accessed by them
- APT IoC feeds – covering malicious domains, hosts, malicious IP addresses, malicious files used by adversaries to commit APT attacks
- Passive DNS (pDNS) feed – a set of records that contain the results of DNS resolutions for domains into corresponding IP addresses[1]
- IoT URL feed – covering websites that were used to download malware that infects IoT devices[2]
- Malicious hash feed – covering the most dangerous, prevalent and emerging malware
- Mobile malicious hash feed – covering malicious objects that infect Android and iOS mobile platforms
- P-SMS Trojan feed – covering SMS Trojans that enable attackers to steal, delete and respond to SMS messages, as well as clocking-up premium charges for mobile users
- Whitelisting data feed – providing third-party solutions and services with a systematic knowledge of legitimate software

Data feeds are aggregated from a combination of fused, heterogeneous and highly reliable sources, including Kaspersky Security Network and its 100 million+ global users who voluntarily share their data on cyber threats with us, our own web crawlers, botnet monitoring system (24/7/365 monitoring of all known botnets, their targets and activities), spam traps, threat research teams and trusted partners.

Then, in real-time, all this aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, multi-scanners, similarity tools, behavior profiling, etc.), analyst validation and whitelisting verification.

Every record in each data feed is supplied with rich actionable context (threat scoring, geolocation, threat names, timestamps, resolved IPs addresses of infected web resources, hashes, popularity, etc.).

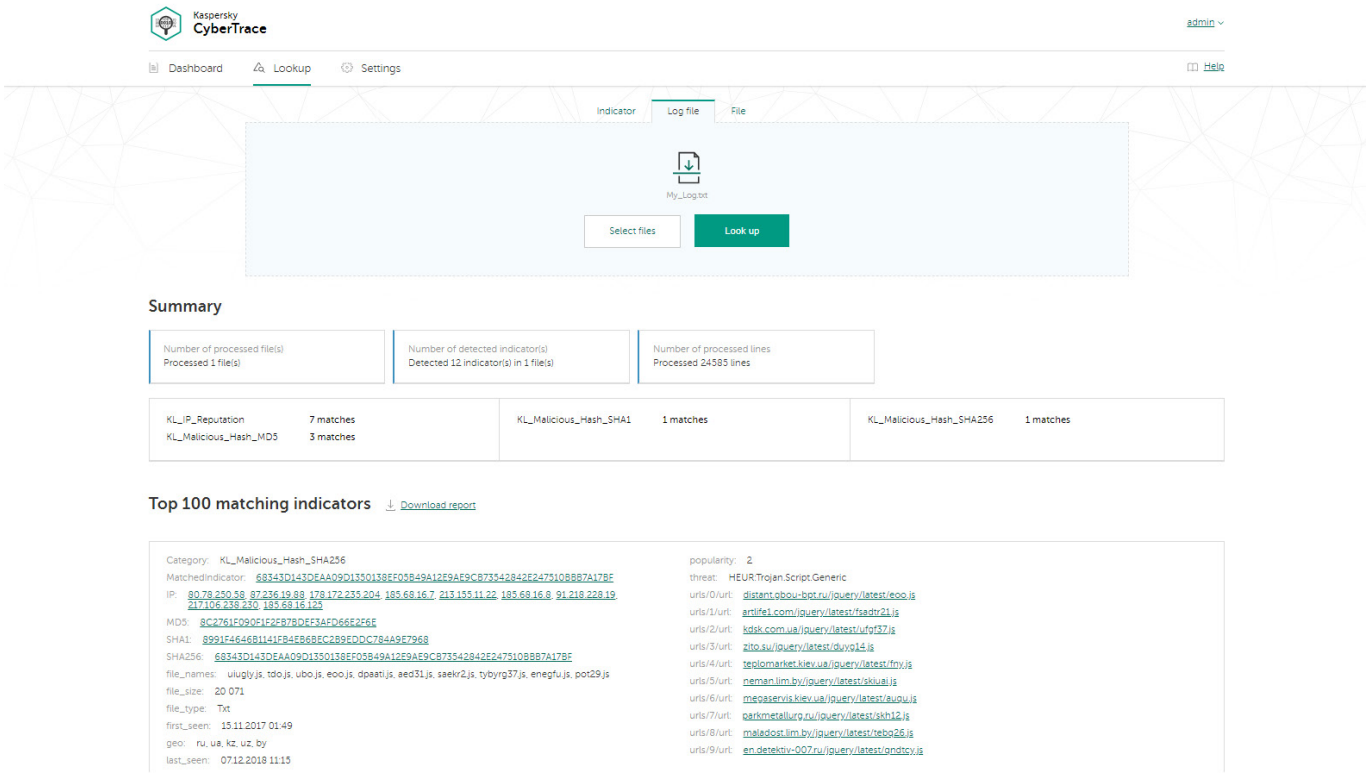


Figure 3. Kaspersky Threat Data Feeds context

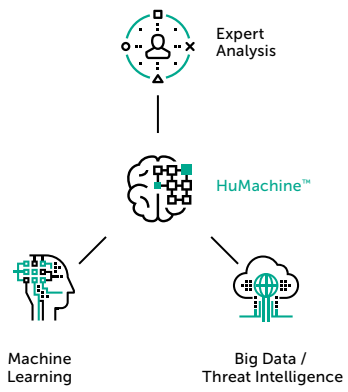
1 Integration will be supported in 2019

2 Integration will be supported in 2019

This contextual data helps reveal the 'bigger picture', further validating and supporting the wide-ranging use of the data. Set in context, the data can be more readily used to answer the 'who, what, where and when' questions which lead to identifying your adversaries and helping you make good decisions.

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, Security Operations Center's analysts are able to:

- Effectively distill and prioritize sweeping amounts of security alerts
- Improve and accelerate triage and initial response processes
- Immediately identify alerts critical for the enterprise and make more informed decisions about which should be escalated to IR teams
- Form a proactive and intelligence-driven defense.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com