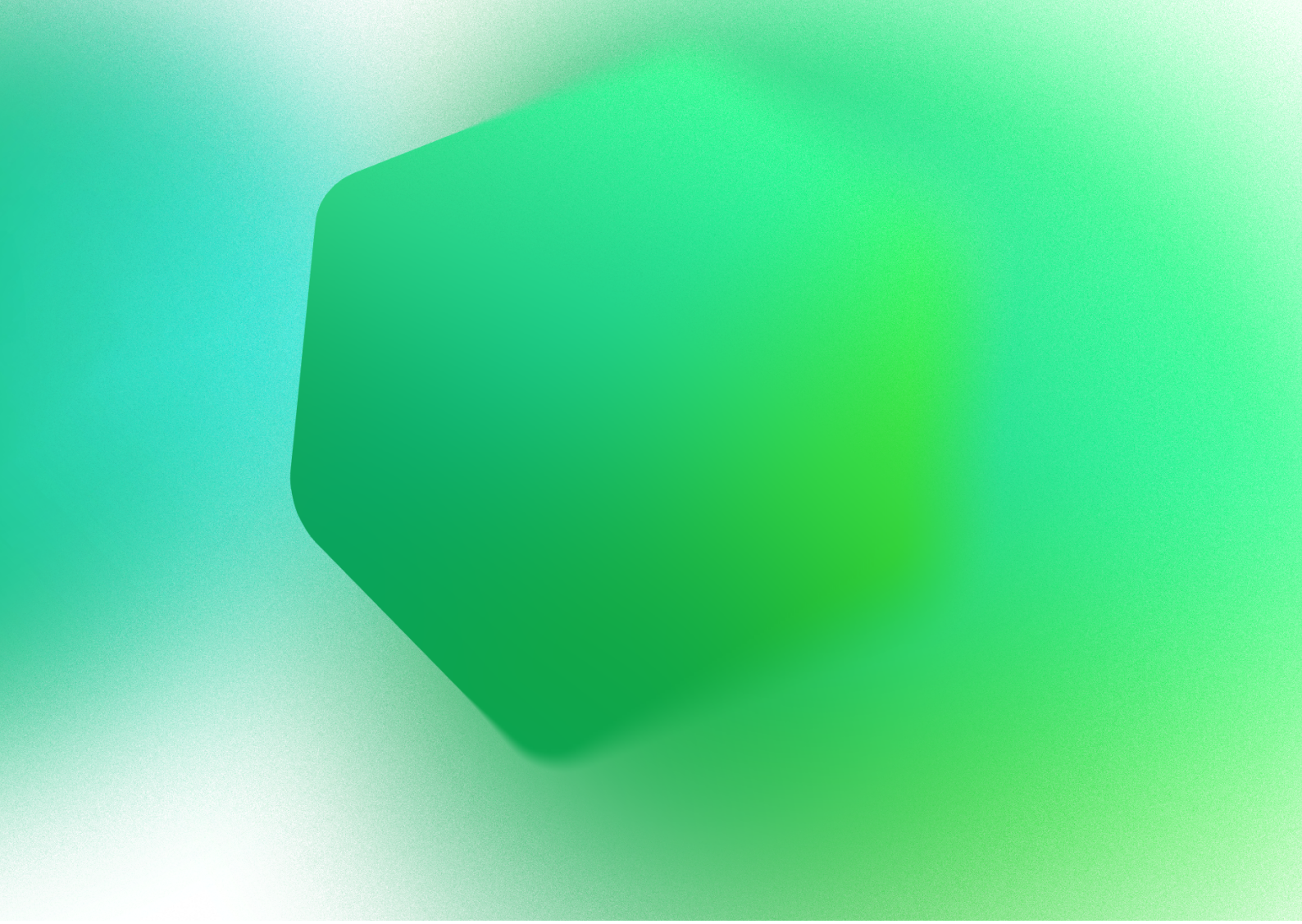


Kaspersky solutions to increase awareness and understanding for better cybercrime prevention, detection, response and prediction

Supporting the fight against cybercrime

2019

kaspersky

Keeping up the fight against cybercrime

Governments across the world are exploring strategies that efficiently balance the need for digitalization of society's core functions to safeguard the competitive position of their national economies, and measures to tackle cybercrime effectively to ensure the safety and wellbeing of their citizens.

The complex and alien nature of cybercrime means that today they are difficult not only to combat, but also to detect and understand. Kaspersky has become a trusted partner with INTERPOL, Europol, major CERTS, government bodies and law enforcement agencies around the world, sharing our cutting-edge knowledge of cyberthreats and helping find and implement effective defensive mechanisms.

While there are no 'silver bullet' solutions, and instead a complex approach to fighting cybercrime is required, we firmly believe in an effective combination of threat intelligence collection and sharing, together with constant improvement of security awareness. In this document we present a tailored approach consisting of three core components for Law Enforcement Agencies (LEAs) to maximize their efforts in tackling borderless cybercrime. Kaspersky provides a limited subscription to these components to our trusted and most valuable partners free of charge.

Kaspersky provides access to the Kaspersky Threat Intelligence Portal with a subscription for a year, including:

- Unlimited access to the first page with a map and specification of threats for different countries;
- Limited access to Kaspersky Threat Lookup for 1000 requests per year with the option to increase the number of requests;
- Limited access to APT and Financial Threat Intelligence Reports (executive summaries only) with the option to request a full report or certain indicators;
- Limited access to our Cloud Sandbox for 1 request per day with the option to request an extension of this
- Limited access to WHOIS Tracking for 3 lookups and 1 hunt per day
- Unlimited access to Data Feeds page with descriptions of all available feeds, IR tools, documentation etc. and SIEM connectors/CyberTrace. CyberTrace includes Demo Data Feeds out-of-the-box.

Threat intelligence reporting

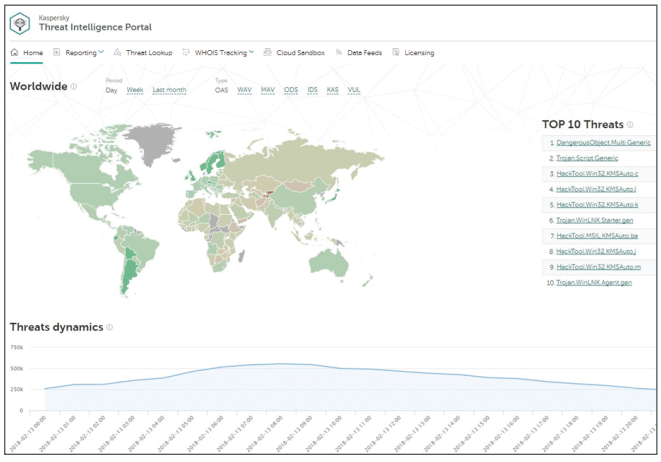
Counteracting modern cyberthreats requires a 360-degree view of the tactics, techniques and procedures used by threat actors. While command & control servers and tools used in attacks change frequently, it is difficult for the attackers to change their behavior and the methods they employ during attack execution. Being able to identify these patterns quickly and expose them to users helps organizations deploy effective defensive mechanisms in advance.

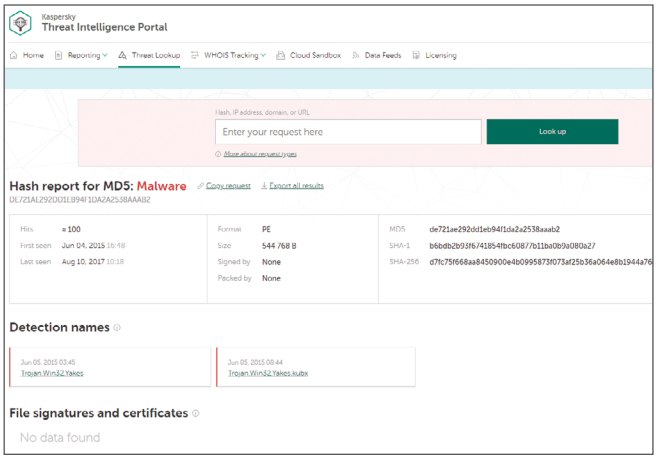
For LEAs' awareness and knowledge of the tactics, techniques and procedures used by threat actors in high-profile cyber-espionage campaigns worldwide, we provide limited access to comprehensive practical threat intelligence reporting, which covers executive summaries of APT campaigns with cross-sector targeting and advanced threats tailored to attack financial institutions, free of charge. The information provided in APT and Financial Threat Intelligence Reporting helps keep computer incident investigations informed so they can plan effective defensive strategies.

Full reports provide:

- Exclusive access to technical descriptions of the very latest threats during the ongoing investigation, before public announcements;
- Insight into non-public investigations. Not all high-profile threats are subject to announcement to the public. Some – due to implications for the victims who are impacted, sensitivity of the data, the nature of the vulnerability fixing process, or associated law enforcement activity – are never made public. But all are reported to our customers;
- Detailed supporting technical data, including an extended list of indicators of compromise (IOCs), available in standard formats, including OpenIOC or STIX, and access to our YARA rules;
- Continuous campaign monitoring. Access to actionable intelligence during an investigation (information on campaign distribution, IOCs, C&C infrastructure).

Figure 1. Kaspersky Threat Intelligence Portal





The Kaspersky Threat Intelligence Portal (TIP) equips LEAs' security teams with as much data as possible, preventing cyberattacks before they may have a negative impact. The TIP retrieves the latest detailed threat intelligence about: URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, file attributes, geolocation data, download chains, timestamps, etc. WHOIS Tracking allows to lookup domains and IP addresses by setting specific search criteria within WHOIS data (e.g. domain contact, creation date etc.) and submit specific fields of WHOIS data for regular and automatic hunting for WHOIS records that meet your criteria. Email notifications about new records in WHOIS database that match search criteria are automatically sent to required recipients.

So, while the Portal retrieves all this invaluable data, our Cloud Sandbox allows that knowledge to be linked to the IOCs generated by the analyzed file sample.

Threat Intelligence Portal content is generated and monitored in real time by highly fault-tolerant infrastructure ensuring continuous availability and consistent performance. Hundreds of experts, including security analysts across the globe, our world-famous Global Research and Analysis Team (GReAT) experts, and cutting-edge R&D teams, all contribute to generating valuable real-world threat intelligence.

Kaspersky provides a demo toolkit of Threat Data Feeds (Botnet C&C Data Feed, Malicious Hash Data Feed, IP Reputation Data Feed) and CyberTrace.

Please note that Kaspersky Demo Data Feeds provide a lower Detection Rate level than the commercial versions.

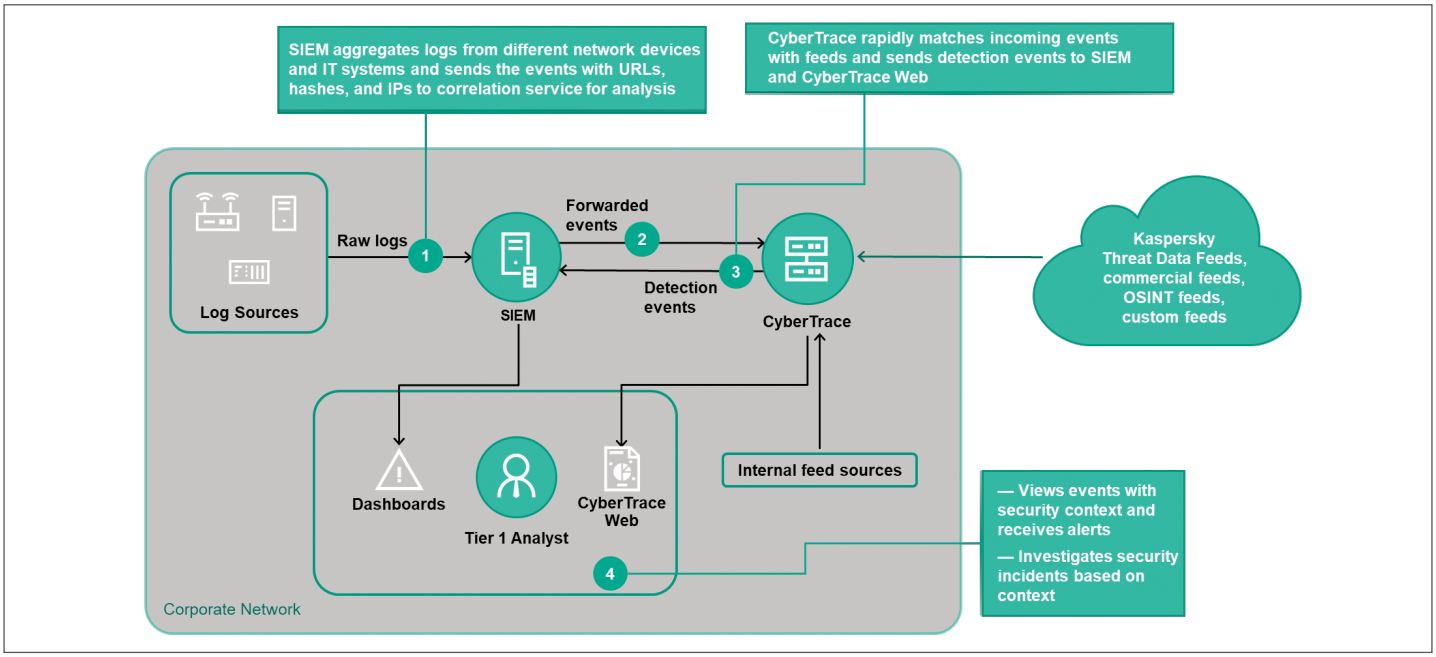
Threat Data Feeds

Kaspersky offers continuously updated Threat Data Feeds and CyberTrace, a threat intelligence fusion and analysis tool, to inform organizations about risks and implications associated with cyberthreats, helping mitigate threats more effectively and defend against attacks even before they are launched. Full list of feeds which are available in the commercial subscription includes IP Reputation Data Feed, Malicious and Phishing URL Feed, Botnet C&C URL Feed, Mobile Botnet C&C URL Feed, Ransomware URL Feed, APT IoC Feeds, Passive DNS (pDNS) Feed, IoT URL Feed, Malicious Hash Feed, Mobile Malicious Hash Feed, P-SMS Trojan Feed, Whitelisting Data Feed and Kaspersky Transforms for Maltego. Then, in real-time, all the aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, sandboxes, heuristics engines, similarity tools, behavior profiling, etc., analysts' validation and whitelisting verification.

Data Feeds are aggregated from fused, heterogeneous and highly reliable sources, such as the Kaspersky Security Network and our own web crawlers, the Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams and partners.

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 security analysts to make timely and better informed decisions.

Figure 2. Kaspersky CyberTrace integration scheme



Kaspersky provides the Automated Security Awareness Platform (ASAP) only for the purposes of demonstration, including:

- A script program to install and use the ASAP modules.

Kaspersky ASAP: Automated Security Awareness Platform

More than 80% of all cyber-incidents are caused by human error, and many organizations still go for a one-off educational effort (like 'Cybersecurity 101 in an Hour') than well-structured professional training programs. Doing so is of course much less time consuming, but a lot less effective too.

- Kaspersky offers its Automated Security Awareness Platform (ASAP) – an online tool to build strong and practical cyber-hygiene skills for LEA employees. Launching and managing the Platform does not require specific resources or arrangements since the Platform:
- adjusts to the individual pace and learning abilities of each employee;
- automatically ensures that the user learns and passes tests on basics before going on to study further;
- provides dashboards with all the information needed to estimate progress and help with suggestions on what to do to improve results;
- uses gamification to improve training skills, not just knowledge, so practical exercises and employee-related tasks are at the core of each module.

Training topics are:

· Email · Web browsing · Passwords · Social networks & messengers · PC security · Mobile devices · Confidential data · Personal data/GDPR · Social engineering · Security at home and while traveling.

Beginner To avoid mass (cheap and easy) attacks	**Elementary** To avoid mass attacks on a specific profile	**Intermediate** To avoid well-prepared focused attacks	**Advanced** To avoid targeted attacks
13 skills, including: – Set up your PC (updates, antivirus) – Ignore obviously malicious websites (those which ask to update software, optimize PC perfomance, send SMS, install players, etc.) – Never open executables from websites	**20 skills, including:** – Sign-up/Login with trusted sites only – Avoid numeric links – Enter sensitive information on trusted sites only – Recognize the signs of a malicious website	**14 skills, including:** – Recognize faked links – Recognize malicious files and downloads – Recognize malicious software	**13 skills, including:** – Recognize sophisticated fake links (including links looking like your company websites, links with redirects) – Avoid black-SEO sites – Log out when finished – Advanced PC setup (turn off Java, adblock, noscript, etc.)
	+ reinforcement of elementary skills	+ reinforcement of the previous skills	+ reinforcement of the previous skills

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky BRING ON THE FUTURE