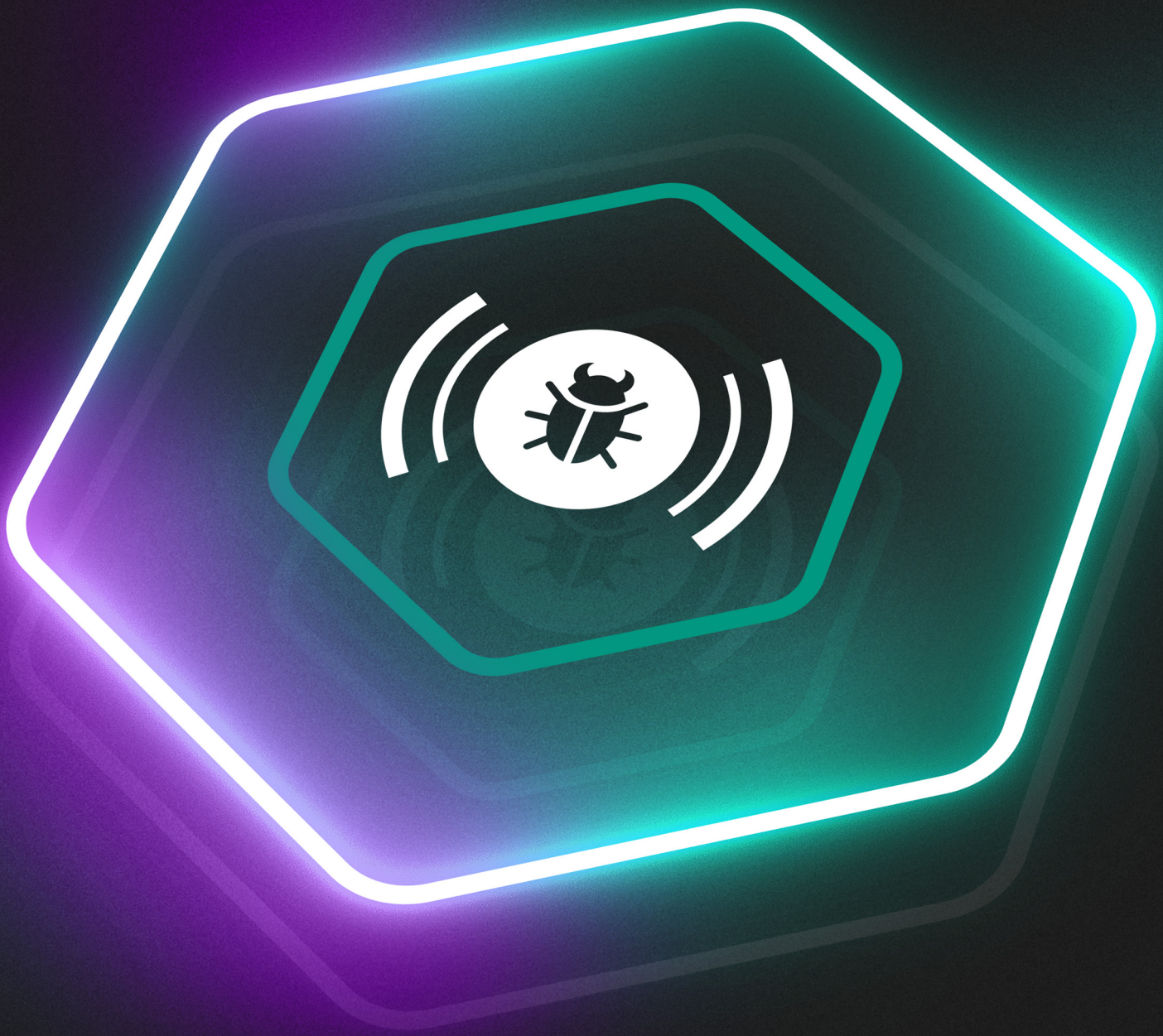

Kaspersky Threat Data Feeds

kaspersky BRING ON THE FUTURE

Kaspersky Threat Data Feeds

Cyberattacks happen every day. Cyberthreats are constantly growing in frequency, complexity and obfuscation, as they try to compromise your defenses. Adversaries use complicated intrusion kill chains, campaigns and customized Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your customers. It's clear that protection requires new methods, based on threat intelligence.

By integrating up-to-the-minute threat intelligence feeds containing information on suspicious and dangerous IPs, URLs and file hashes into existing security systems like SIEM, SOAR and Threat Intelligence Platforms, security teams can automate the initial alert triage process while providing their triage specialists with enough context to immediately identify alerts that need to be investigated or escalated to incident response teams for further investigation and response.

- IP REPUTATION FEED
- HASH FEED (WIN / *nix / MacOS / AndroidOS / iOS)
- URL FEEDS (Malicious, Phishing and C&C)
- RANSOMWARE URL FEED
- APT IOC FEEDS
- CRIMEWARE FEEDS
- VULNERABILITY FEED
- PASSIVE DNS (pDNS) FEED
- IoT URL FEED
- ALLOWLISTING FEED
- ICS HASH FEED
- INDUSTRIAL VULNERABILITY FEED IN OVAL
- CLOUD ACCESS SECURITY BROKER (CASB) FEED
- OPEN SOURCE SOFTWARE THREATS FEED

Contextual data

Every record in each Data Feed is enriched with actionable context (threat names, timestamps, geolocation, resolved IP addresses of infected web resources, hashes, popularity etc). Contextual data helps reveal the 'bigger picture', further validating and supporting the wide-ranging use of the data. Set in context, the data can more readily be used to answer the 'who, what, where, when' questions to identify your adversaries, and help you make quick decisions and take action.

Highlights

Data Feeds are automatically generated in real time, based on findings across the globe (Kaspersky Security Network provides visibility to a significant percentage of all internet traffic, covering tens of millions of end-users in more than 213 countries) providing high detection rates and accuracy

Ease of implementation. Supplementary documentation, samples, a dedicated technical account manager and technical support from Kaspersky all combine to enable straightforward integration

Simple lightweight dissemination formats (JSON, CSV, OpenIoC, STIX) via HTTPS, TAXII or ad-hoc delivery mechanisms support easy integration of feeds into security solutions

Data Feeds littered with false positives are valueless, so very extensive tests and filters are applied before releasing feeds, to ensure that 100% vetted data is delivered

Hundreds of experts, including security analysts from across the globe, world-renowned security experts from GReAT and R&D teams contribute to generating these feeds. Security officers receive critical information and alerts generated from the highest quality data, with no risk of being deluged by superfluous indicators and warnings

All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability

Collection and processing

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

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, analyst validation and allowlisting verification.

Benefits

Reinforce your network defense solutions, including SIEMs, Firewalls, IPS/IDS, Security Proxy, DNS solutions, Anti-APT, with continuously updated Indicators of Compromise (IOCs) and actionable context to deliver insights into cyberattacks and provide a greater understanding of the intent, capabilities and targets of your adversaries. Leading SIEMs (including HP ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) and TI Platforms are fully supported

Improve and accelerate your incident response and forensic capabilities by automating the initial triage process while providing your 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

Prevent the exfiltration of sensitive assets and intellectual property from infected machines to outside the organization. Detect infected assets fast to protect your brand reputation, maintain your competitive advantage and secure business opportunities

As an MSSP, grow your business by providing industry-leading threat intelligence as a premium service to your customers. As a CERT, enhance and extend your cyberthreat detection and identification capabilities

www.kaspersky.com