Remediate threats with intelligence

Kaspersky Threat Data Feeds for Microsoft Sentinel

kaspersky BRING ON THE FUTURE

Partnership

Kaspersky partners with Microsoft to help Microsoft Sentinel users extend their cyberthreat detection capabilities and increase the effectiveness of initial alert triage, threat hunting and incident response.

Intelligence-driven defense

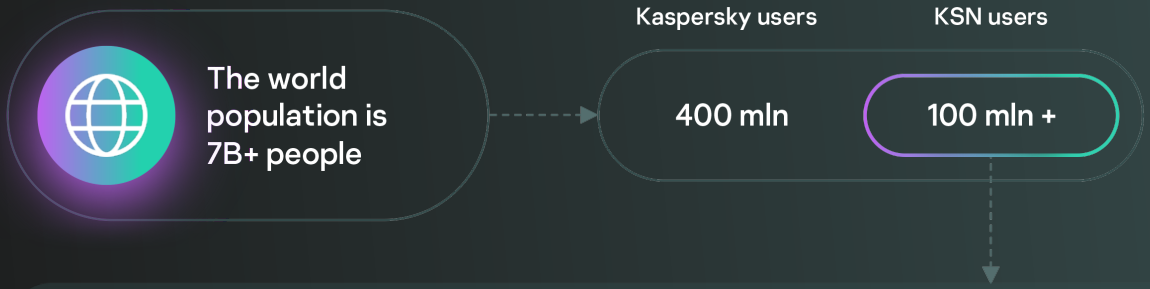
The number of security alerts analyzed each day in most cases exceeds the existing capacity of security teams. Amid a million alerts, we need accurate and relevant threat intelligence to find and respond to the most dangerous attacks.

Integrated with Microsoft Sentinel, Kaspersky Threat Data Feeds expands a company's capacity to make timely, informed decisions about adversaries' actions by leveraging globally sourced, context-rich and immediately actionable threat information.

Global visibility into cyberthreats

Threat Data Feeds are aggregated from fused, heterogeneous and highly reliable sources, such as Kaspersky Security Network, collecting anonymized threat data from 100 mln+ users worldwide, our own web crawlers, Botnet Monitoring service (24/7/365 monitoring of botnets, their targets and activities), spam traps, honeypots, different kind of sensors, passive DNS, partners and OSINT.

Then, in real-time, all the aggregated data is carefully inspected, dissected and interpreted by our in-house threat research teams, with threat research centers established in each region. The data is processed by numerous automated expert systems (such as sandboxes, heuristic engines, similarity tools etc.), transforming it into finished intelligence to deliver 100% vetted information to our customers.



We detect 420k new pieces of malware every day

We have more than 1000 researchers & developers

Figure 1. How we know about threats

Actionable context in feeds includes threat names, timestamps, geolocation, resolved IP addresses of infected web resources, hashes, popularity or other search terms. With this data, security teams or SOC analysts can accelerate the initial alert triage by making informed decisions for investigation or escalation to an incident response team.

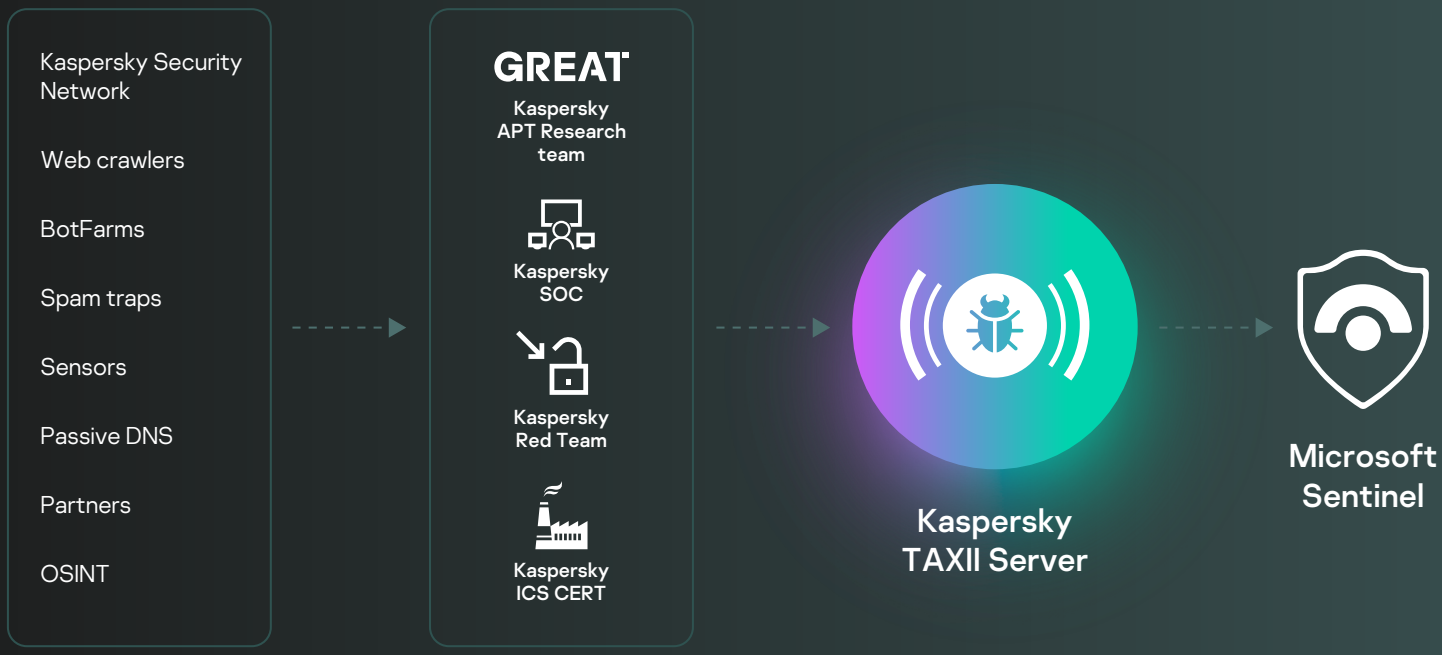


Figure 2. Importing threat data from Kaspersky into Microsoft Sentinel

How it works

Microsoft Sentinel uses the TAXII protocol and gets data feeds in STIX format so it allows configuration of Kaspersky Threat Data Feeds as a TAXII Threat Intelligence source in the interface. Once it is imported, cybersecurity teams can use out-of-the-box analytic rules to match threat indicators from feeds with logs.

With the Kaspersky TAXII server, it is extremely easy to bring in the Threat Data Feeds from Kaspersky into Microsoft Sentinel by leveraging the built-in TAXII client of Microsoft Sentinel. This data can then be easily utilized by SOC analysts in your organization for further hunting, investigation and analysis of threats.

Benefits

Protect your networks against threats aimed at your organization

Quickly identify critical incidents requiring immediate escalation to incident response teams

Fight analyst burnout with highly-validated contextual information

Highlights

- All feeds are automatically generated in real time based on findings across the globe, providing high detection rates and accuracy
- Extensive tests and filters are applied before releasing feeds, to ensure that 100% vetted data is delivered
- All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability
- Straightforward and easy integration by using Microsoft Sentinel TAXII Data connector

Kaspersky Threat Data Feeds for Microsoft Sentinel

Learn more

www.kaspersky.com