kaspersky

THE ARTICLE

Clear data, faster decisions: why CISOs can't afford stale threat intelligence

Attackers are moving faster, security teams are stretched thinner, and cyber decisions are becoming business decisions. According to 2025 cybersecurity data, 72% of cybersecurity professionals have seen a significant increase in attacks, while two out of three organizations report moderate-to-critical cybersecurity skills gaps.[1] At the same time, global cybersecurity spending is expected to reach $302 billion by 2029.[2]

Yet breaches still happen. The issue is not only how much organizations spend, but whether their tools have the right intelligence to act on. The average cost of a breach is $4.4 million,[3] and mean time to investigate and respond has increased by 48%.[4] For CISOs, the question is clear: how can teams detect earlier, respond faster, and reduce noise without adding more operational burden?

Threat data feeds provide machine-readable intelligence that can be integrated into existing security systems, including SIEM, SOAR, NGFW, EDR, XDR, TIP, firewalls, proxies, and threat hunting platforms. They help teams detect malicious infrastructure, dangerous URLs, phishing resources, APT indicators, crimeware activity, vulnerable open-source packages, and other relevant threats.

But not all threat data is equal. Stale or unverified indicators can increase false positives, overload analysts, and even disrupt legitimate business traffic. Kaspersky Threat Data Feeds are built on data gathered anonymously from users in 200+ countries and territories, supported by 25+ years of expertise and verified by five Kaspersky Expertise Centers. The most frequent feeds are updated every 10 minutes, helping teams act on fresh, relevant intelligence.

For organizations with a SOC, threat data feeds enrich alerts, support correlation, improve prioritization, and enable threat hunting. For organizations without a SOC, they can support automated blocking through firewalls, proxies, and network security controls. With Kaspersky CyberTrace, incoming events can be matched against threat data feeds in real time and retrospectively, helping offload SIEM workloads and triple detection accuracy.

[1] World Economic Forum, Global Cybersecurity Outlook 2025 (World Economic Forum, 2025)
[2] Maxim Merritt et al., Global Cybersecurity Market Forecast 2024 To 2029 (Forrester, 2025)
[3] IBM, Cost of a Data Breach Report 2025 (IBM, 2025)
[4] Kaspersky, MDR Report 2025, (Kaspersky, 2025)

Before choosing a threat data feed provider, every CISO should ask five questions:

1

Where does the data come from?

Is it based on proprietary telemetry, open sources, partners, expert research, or a combination?

2

How is it verified?

Are indicators validated through real-world detections, automated filtering, expert review, and continuous re-checking?

3

How fresh is the intelligence?

How often are feeds updated, and how quickly is stale data removed?

4

How relevant is the context?

Does the feed include threat score, geography, industry, campaign, actor, MITRE mapping, or infrastructure relationships?

5

Can we pay only for what fits?

Is licensing modular enough to match your risks, maturity, use cases, and budget?

Kaspersky offers **30+ out-of-the-box threat data feeds**, including IP Reputation, Dangerous URLs, Malicious Hashes, APT IoCs, Crimeware IoCs, Mobile IoCs, ICS IoCs, Network Security Feeds, Vulnerabilities, Open Source Software Threats, and YARA, SIGMA, and Suricata rules.

This breadth of coverage means security teams can enrich detection, investigation and response with intelligence tailored to their specific environment and risk profile. Instead of relying on generic indicators, organizations can prioritize the threat data that matters most to their infrastructure, improve detection accuracy, reduce false positives and respond to incidents with greater speed and confidence.

The practical next step is simple: **get a sample, run a test, and talk to an expert**. Test Kaspersky Threat Data Feeds in your own environment, validate the coverage and quality against your real threats, and tailor the right feed mix to your business. Clearer data leads to faster decisions, and faster decisions reduce cyber risk.



www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.