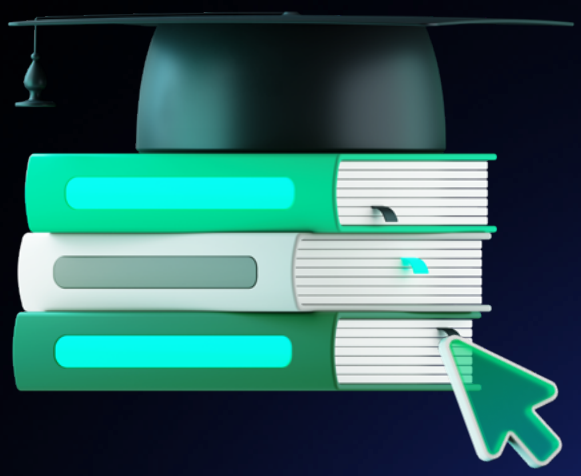
Threat intelligence: the clearer the data, the sharper the decision

kaspersky

This eBook explores why high-quality threat intelligence has become a strategic business advantage, and how the right data feeds can help your organization detect threats faster, reduce analyst workload and respond with greater confidence.

It is of particular interest to CISOs and other decision makers trying to overcome evolving security challenges, maintain business operationality and protect revenue.

Contents



Expert's view

Cybersecurity has never been better funded. Global spending on products and services is expected to reach **$302 billion by 2029**[1] as businesses strengthen their defenses against growing attacks. Yet breaches still happen.

Attackers are getting faster, more organized and more capable thanks to AI, with 72% of cybersecurity professionals noting a **significant increase in attacks**.[2]

Security teams, on the other hand, are being asked to process growing volumes of fragmented data while working with limited resources. Nearly half of them report **significant cybersecurity skills shortages**,[3] making it harder still to manage growing alert volumes.

This challenge can't be solved by simply deploying another security product. It's a challenge of decision-making. Every day security leaders make decisions that shape business resilience: which alerts can be ignored? Which vulnerabilities pose a business risk? Which incidents require immediate containment?

These are **business decisions made in the context of cyber risk**. That's why threat intelligence is more than "just another security capability" – it's the foundation for faster, more confident decision-making.

Better visibility. Better decisions. Better outcomes.

Security teams don't lack information. They have the opposite problem – they're drowning in it. Every security tool, be it a firewall, cloud platform or identity service, generates telemetry. SIEM platforms aggregate millions of events while threat detection engines produce a constant stream of indicators.

Visibility has expanded but clarity hasn't. Having a broad view of the threat landscape is no good if you don't know what to focus on. It's like trying to follow one conversation in a stadium full of people.

Analysts are expected to process more information than they can handle. Valuable time is spent correlating disconnected events and deciding which alerts warrant investigation. The consequence is familiar to every SOC: more operational effort, slower investigations and increasing analyst fatigue.

The mean time to investigate and respond to security incidents has increased by 48%, despite continued investment in security technologies.[4]

But the issue isn't visibility alone. It's visibility without context. Security leaders need more than raw data – they need intelligence that helps them understand what they're seeing, how it relates to their organization and what action should be taken next.

[1] Maxim Merritt et al., Global Cybersecurity Market Forecast 2024 To 2029 (Forrester, 2025)

[2] World Economic Forum, Global Cybersecurity Outlook 2025 (World Economic Forum, 2025)

[3] IBM, Cost of a Data Breach Report 2025 (IBM, 2025)

[4] Kaspersky, MDR Report 2025, (Kaspersky, 2025)

Effective decision-making depends on three things

Decision requirement	Why it matters
Visibility	A complete view of threats across the attack surface **eliminates blind spots** and identifies what matters most
Context	Understanding how indicators relate to threat actors and business risk **enables confident prioritization**
Efficiency	AI-assisted analysis and automation **reduces operational workload**, allowing analysts to focus on genuine threats rather than noise

When these elements come together, security teams don't simply detect threats faster. They make better decisions under pressure.

Threat intelligence as a business enabler

Threat intelligence was historically viewed as a specialist resource used primarily by SOC analysts during investigations. That role has changed. According to IDC, "It is no longer just a cybersecurity asset – it's a business enabler."[5]

Rather than serving as another source of technical information, it lets security teams **prioritize risk effectively, strengthen operational resilience and respond with confidence**. And this makes it a wise investment. The average data breach costs $4.4 million – but organizations that identify and contain breaches quickly consistently reduce the financial impact of an incident.[6]

> "The shorter the time to detect and respond, the lower the potential business loss."
>
> Oleg Shaburov, Business Development Manager (Technology Solutions), Kaspersky

[5] Soltysik Monika, Kissel Christopher, Worldwide Threat Intelligence Forecast, 2025–2029: from Data to Decisions – the Intelligence-Driven Security of the Future (IDC Research, 2025)

[6] IBM, Cost of a Data Breach Report 2025 (IBM, 2025)

Better intelligence leads to faster decisions, which shorten detection and response times and can ultimately reduce the cost and impact of a breach. Threat intelligence is therefore an investment in better business outcomes. But if many organizations already consume it, why do their security teams still struggle with false positives, alert fatigue and delayed response?

The answer lies in its quality. **Not all threat intelligence is created equal** – and the foundation of its effectiveness is the data that feeds it.

Data feeds: the foundation of every security decision

Threat intelligence is often described as a finished product, such as a report or dashboard. But those outputs are just the tip of a much larger process. Every investigation, every detection rule and every automated response depends on one fundamental ingredient: **trusted threat data**.

SIEM, XDR, EDR, SOAR and next-generation firewalls all rely on external intelligence to understand whether an event is benign, suspicious or dangerous. Data feeds provide that intelligence. They don't replace the security stack, but they do make it smarter.

Without that context, security platforms can only process events; with it, they begin to understand them. This distinction is key now that organizations are automating more of their security operations. AI, behavioral analytics and automation are only as effective as the data they're trained on and the intelligence they're consuming. Better decisions don't start with better algorithms but with better data.

> Threat data feeds aren't another security tool. They're the intelligence layer that makes existing security investments more effective.
>
> Alexander Mazikin, Head of Threat Intelligence Product Line, Kaspersky

The power of diverse data sources

One of the first questions organizations ask when evaluating threat intelligence is one of the hardest to answer: where does the data come from? Most vendors claim broad visibility. They say they combine commercial intelligence, open-source information and proprietary research.

But the reality is very different. The quality of a threat intelligence feed depends not simply on the number of sources it draws from, but on the uniqueness, quality and validation of those sources. High-confidence intelligence isn't created by collecting information from everywhere. It's created by continuously correlating, validating and enriching data from multiple perspectives before it ever reaches an analyst.

One of Kaspersky's strengths it its broad, unique visibility. The Kaspersky Security Network (KSN) receives anonymized telemetry from millions of protected devices worldwide, including the regions most heavily targeted by cybercriminals. Because attacks evolve differently across regions, combining **telemetry from diverse geographies helps identify emerging campaigns earlier** and provides businesses intelligence that reflects the threats most relevant to their environment.

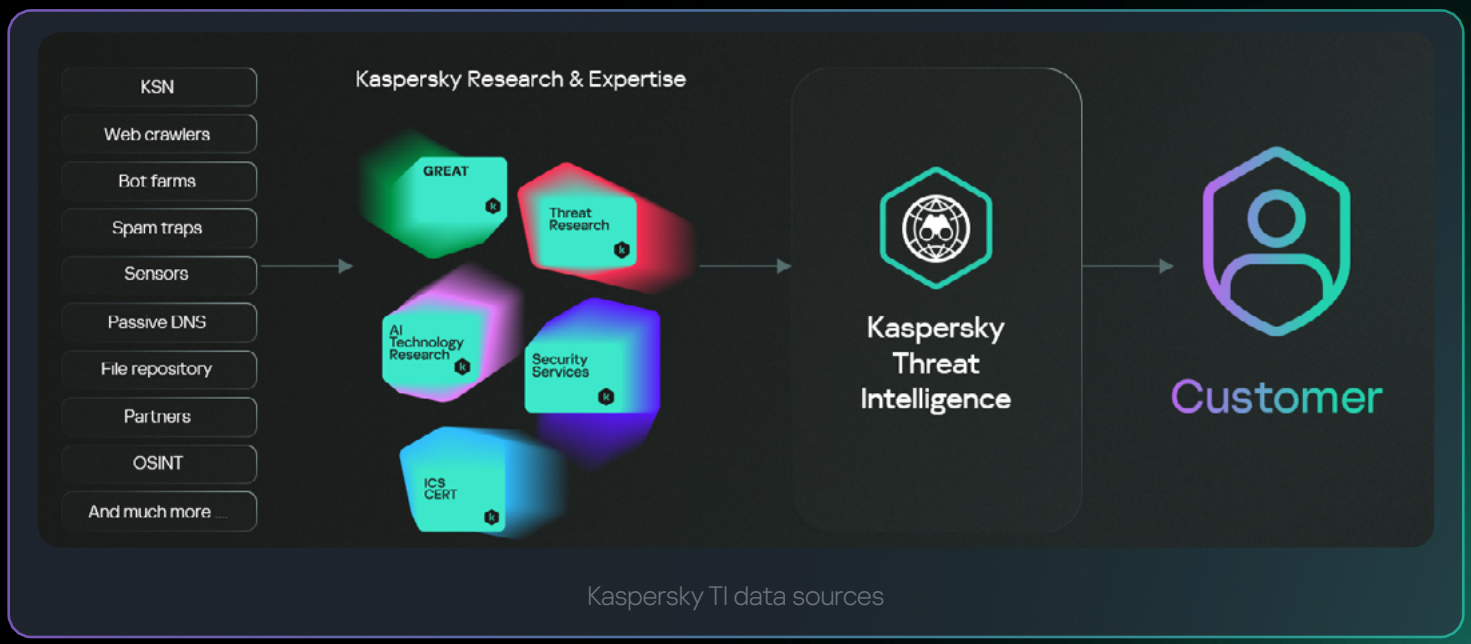
The data gathered through KSN is then enriched with intelligence from:

- malware research
- incident response
- digital footprint investigations
- industrial cybersecurity specialists
- spam traps
- passive DNS
- OSINT
- Plus, other sources

Think of it as a jigsaw puzzle. Each source contributes another piece, and only when enough pieces come together does the full picture emerge. This is important because modern attacks rarely reveal themselves through a single indicator.

> The broader and more diverse the intelligence base, the sharper the defensive decision.
>
> Alexander Mazikin, Head of Threat Intelligence Product Line, Kaspersky

An IP address on its own, for example, tells only part of the story. A malicious file hash is useful, but when combined with campaign intelligence you can move beyond simply blocking. Quality additional sources help transform isolated indicators into actionable intelligence.



Kaspersky TI data sources

Expertise turns information into intelligence

Every day, security platforms collect huge amounts of telemetry. Left unfiltered, much of that information has little operational value. Some indicators are duplicated while others quickly become obsolete. Many are plain irrelevant to a particular organization.

Technology discovers indicators, experts determine whether they matter – and that's an important distinction.

> Almost every vendor can collect data. The difference lies in how consistently that data is verified, prioritized and transformed into intelligence that organizations can trust.
>
> Oleg Shaburov, Business Development Manager (Technology Solutions), Kaspersky

A network of specialist research teams contributes a different perspective on the evolving threat landscape. No single team sees the whole picture. APT researchers uncover nation-state campaigns and advanced attacker techniques. Incident Response and MDR teams contribute intelligence from real-world investigations. Threat Research specialists analyze emerging malware, while ICS CERT experts focus on attacks targeting industrial environments. AI specialists accelerate discovery at scale, helping identify patterns and relationships that would otherwise remain hidden.

Combined, they continuously validate, enrich and refine intelligence before it reaches analysts. The result is intelligence that is not only broader in coverage, but also more accurate, contextual and ready to support decision-making. This combination of automation and human expertise ultimately provides security teams with confidence.

1. Confidence that an indicator has been verified
2. Confidence that context has been added
3. Confidence that analysts can act without spending valuable time validating the information themselves

The objective is to provide more intelligence that analysts can trust.

Why fresh intelligence wins

Threat intelligence is one of the few security investments that starts decreasing in value the moment it's created. Some indicators remain valuable for years, while others become obsolete in just hours. Freshness therefore isn't about how often a feed is updated but about **understanding when information stops being useful**.

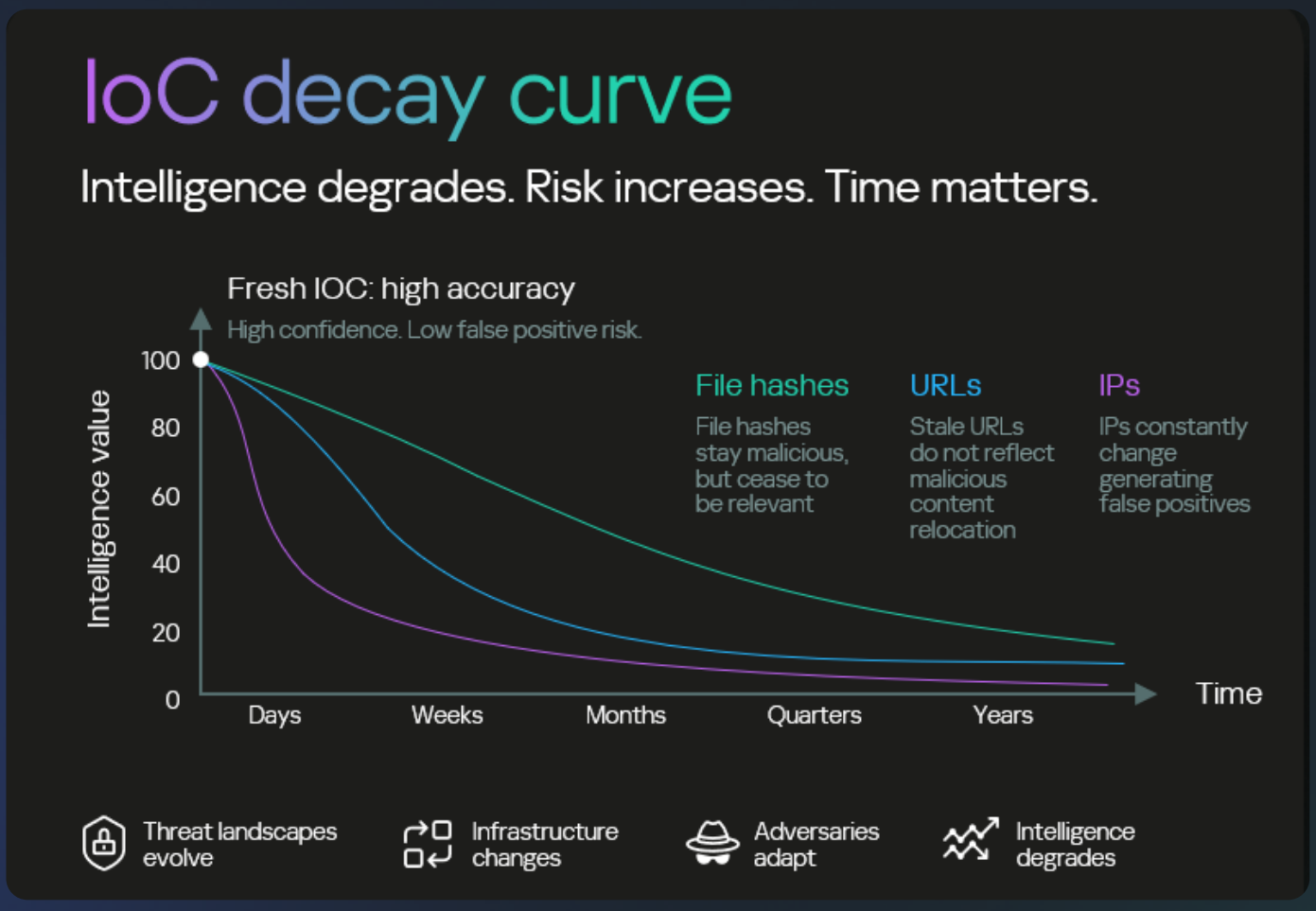
Consider the difference between a malicious file hash and malicious IP address.

A malicious file hash remains malicious indefinitely. Even years later, identifying that file is still accurate. However, if the file is no longer being used by attackers, its operational value declines because it's less likely to help detect an active threat.

IP addresses are different. Attackers constantly rotate infrastructure, abandon compromised servers and establish new command-and-control networks. An IP address that was a threat yesterday could belong to a legitimate business tomorrow. Continuing to block it doesn't strengthen security; it paves the way for unnecessary disruption.

> Freshness is especially critical for IP addresses. Attack infrastructure changes quickly, so outdated indicators don't improve security. They increase false positives.
>
> Alexander Mazikin, Head of Threat Intelligence Product Line, Kaspersky

This is illustrated by what security researchers call the **threat intelligence decay curve**. The value of many indicators naturally declines over time as attackers adapt their infrastructure and tactics. Meanwhile, the risk of false positives increases if outdated intelligence remains active.



IoC decay curve

Kaspersky continuously validates and refreshes its feeds, removing stale indicators and updating intelligence as the threat landscape evolves. Some feeds are refreshed as frequently as every ten minutes, ensuring organizations act on intelligence that reflects today's threat landscape.

Fresh intelligence doesn't just improve detection. It delivers the confidence businesses need to respond faster.

Turning intelligence into action

Threat intelligence creates value when it influences decisions. Many businesses subscribe to commercial feeds and receive reports, but that intelligence is often disconnected from day-to-day security operations. Analysts manually search for indicators; threat hunters correlate information across multiple platforms; incident responders spend valuable time gathering context. The intelligence exists – but the challenge is operationalizing it.

That's where machine-readable threat intelligence comes in. Unlike traditional intelligence reports designed for people to read, **threat data feeds are designed for security platforms to consume automatically**. Every update can be immediately applied across SIEM, XDR, EDR, SOAR and next-generation firewalls, enriching alerts, improving correlation and automating response without adding manual effort.

Platforms such as Kaspersky CyberTrace make this possible by **integrating threat data feeds directly into existing security workflows**. Instead of forcing analysts to search for indicators manually, CyberTrace enriches events with contextual intelligence automatically, helping teams to prioritize incidents faster and act with greater confidence.

Automation starts with trusted intelligence

Automation is a powerful cybersecurity tool, but without trusted intelligence it simply allows businesses to make mistakes faster.

Every automated workflow depends on the quality of the information driving it. If indicators are inaccurate or poorly validated, false positives multiply and confidence in automation quickly disappears.

High-quality threat data feeds solve this problem by providing verified, contextual intelligence that security tools can trust. They are not about looking through indicators one by one.

> “Instead of manually validating every indicator, analysts get enriched alerts with context attached. Instead of reviewing low-priority events, security teams can focus on incidents that matter.”
>
> Oleg Shaburov, Business Development Manager (Technology Solutions), Kaspersky

For overstretched SOC teams, that difference is significant. Reducing unnecessary investigations doesn't just improve efficiency. It reduces fatigue and allows experienced analysts to focus on high-value investigations rather than dismissing false positives.

Choosing the right data feeds for your organization

Threat intelligence shouldn't be consumed in the same way by every business. A mature SOC has very different requirements from a business with a lean security team. Those without a dedicated SOC often need actionable intelligence that integrates directly with existing security controls, allowing solutions to automatically identify and block high-confidence threats.

For organizations operating a mature SOC, its role expands considerably. Rather than acting purely as a blocking mechanism, it becomes an enrichment layer, providing analysts with additional context about infrastructure, malware, campaigns, vulnerabilities and threat actors to improve prioritization and investigation.

The goal is the same: reduce uncertainty, improve decision-making and respond faster. The path simply depends on organizational maturity.

Five questions every CISO should ask before choosing threat data feeds

Most providers claim to have broad coverage and visibility. The more important question is whether the intelligence will genuinely improve security operations.

Before investing in any threat data feed, CISOs should ask five simple questions.

	Question	Why it matters
1	Where does the intelligence come from?	Broad, unique sources provide visibility that recycled public data cannot
2	How is it validated?	Verification reduces false positives and increases analyst confidence
3	How fresh is the data?	Threat intelligence loses value quickly if indicators are not continuously updated
4	Does it provide meaningful context?	Context enables analysts to prioritize threats instead of simply collecting indicators
5	How flexible is it?	Data feeds should fit your business's risks, maturity, use cases and budget

The answers will often reveal more than the number of indicators a vendor claims to provide. The real value of threat intelligence isn't measured in volume but in decisions made with greater confidence.

Turning intelligence into your business advantage

Every business wants to detect threats earlier, respond faster and reduce the impact of cyber incidents. Threat intelligence helps achieve those outcomes, but only when the intelligence is trustworthy and actionable.

Kaspersky Threat Data Feeds combine global visibility with decades of threat research, expert validation and AI-assisted analysis to deliver trusted intelligence that enriches existing security operations.

The result is more than stronger detection. It's faster response, greater operational efficiency and better-informed security decisions. Because when the data is clearer, every decision becomes sharper.

Experience the difference for yourself

The best way to evaluate threat intelligence is by seeing how it performs in your own environment.

Getting started is simple.

1 Request a sample

Explore Kaspersky Threat Data Feeds and see how the intelligence is structured

2 Integrate with your environment

Connect the feeds to CyberTrace, OpenCTI or your existing security platform using readymade integration components

3 Speak with our experts

Discuss your environment, operational requirements and security goals with Kaspersky Threat Intelligence specialists

Request a free Kaspersky Data Feed sample and test the intelligence in your own environment.

Learn more

Lp.kaspersky.com/global/datafeeds

https://www.kaspersky.com/enterprise-security/threat-data-feeds

www.kaspersky.com