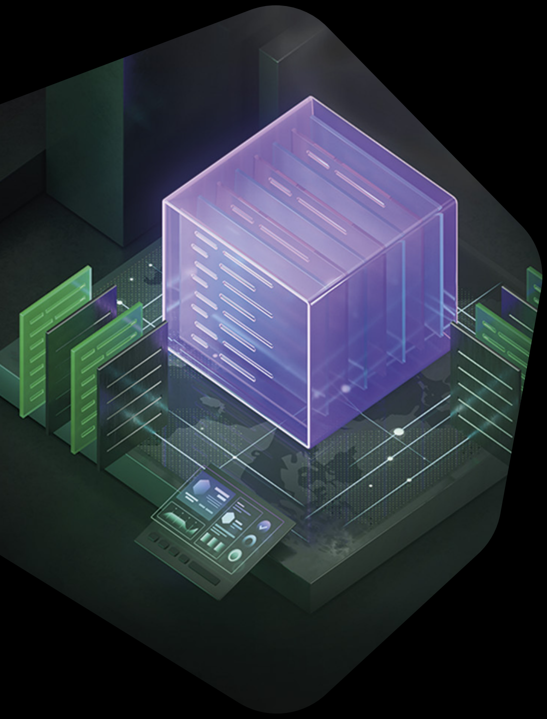
kaspersky BRING ON THE FUTURE

Threat Intelligence: maximizing the benefits



Threat intelligence: a vital tool in proactive threat defense

According to analysis by Kaspersky, the global threat intelligence (TI) market was worth US$1.386 billion in 2022, and set grow at a CAGR of 15.8% from 2022-25.

For many organizations – especially those that are vulnerable to targeted attacks and advanced persistent threats (APTs) – TI is a vital tool in enabling proactive threat defense.

But while the uses and benefits of TI are many and varied, so are its sources, to the extent that trying to identify what will work best for your particular organization can be a challenge in itself. So what should you be looking out for in 2023, and how can you ensure TI delivers the maximum benefits to your enterprise?

Avoiding making existing problems even worse

To help you navigate the various options, the single most important thing to bear in mind is that TI that isn't tailored to or customized for the specifics of your business can exacerbate your problems.

In many organizations, security analysts spend more than half their time sorting out false positives instead of proactive threat hunting and response, leading to significant increases in detection times. Feeding your security operations with irrelevant or inaccurate intelligence will drive the number of false alerts even higher, with serious negative impacts on both your response capabilities and your overall security. So how can you avoid this?

Evaluating commercial TI sources

While there are no universally agreed criteria for evaluating commercial TI offerings, things to take account of when doing so include:

- With an extensive range of providers to choose from, look for TI that transforms your understanding of your specific threat landscape - for example through detailed analysis of historical and emerging threats targeting your particular industry, region or individual enterprise - to improve the performance of functions such as vulnerability management, threat hunting, incident response and more.
- Assuming you already have security controls and processes in place, and want to combine TI with the tools you already use and know, look for delivery methods, integration mechanisms and formats that support smooth integration of TI into your existing security operations.
- Also, look for intelligence with global reach. As attacks have no borders, does the vendor source information globally and collate seemingly disjoined activities into cohesive campaigns? This kind of intelligence will help you take more appropriate action.
- If you're looking for more strategic content to inform your long-term security planning, look for a TI provider with a proven track record of continuously uncovering and investigating complex threats in your region and/or industry. The provider's ability to tailor their research capabilities to the specifics of your business is also critical.

Utilizing a TI platform

A threat intelligence platform (TIP) helps you aggregate, manage and operationalize TI – vital when your security tools are utilizing TI from multiple sources. Specifically, a TIP should enable you to:

- Respond to threats more effectively by checking any threat indicator that you consider to be suspicious, whether it's a file, file hash, IP address or web address.
- Analyze files to detect advanced commodity, evasive and APT-like threats.
- Submit IP addresses, file hashes, domains or web addresses you consider suspicious, to quickly validate and prioritize alerts and incidents using risk levels and supporting contextual information to determine which are real threats.
- Receive regular reports on the behavior of specific files or web addresses.
- Automate security workflows by connecting your applications with the TIP.

How Kaspersky can help

Kaspersky's Threat Intelligence portfolio covers a full range of security scenarios including prevention, detection, investigation, response and strategic reporting – all of which can be tailored to the needs of individual organizations. Our Global Research and Analysis Team (GReAT) are an elite group of security experts who, by infiltrating closed communities and dark forums worldwide, have discovered and dissected more than 50 of the world's most sophisticated targeted attacks. And our knowledge, experience and deep intelligence on every aspect of cybersecurity have made us a trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and leading CERTs.

Kaspersky
Threat
Intelligence

Learn more

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/about/transparency

Proven.
Transparent.
Independent.