kaspersky BRING ON THE FUTURE

Kaspersky Threat Intelligence

Strategic threat intelligence use cases

For a long time, common wisdom held that a passive strategy — protecting the network perimeter and workstations — sufficed. But with enterprises increasingly falling victim to advanced and targeted attacks, it's now clear that protection requires new methods, based on Threat Intelligence.
Generating this intelligence requires constant dedication and high levels of expertise. With petabytes of rich threat data to mine and a unique pool of world experts to draw upon, Kaspersky works to help organizations maintain immunity against cyber-attacks.

Understanding the risks allows making informed decisions when, for example, launching a new initiative, opening a new regional office or planning a technology investment. It also helps to develop proactive mitigation strategies and justify associated budget and staffing requirements.

Our lives are highly dependent on the internet. The low cost and high speed of the communications it provides make it an integral and critical component of the very foundation of successful businesses and governments. Dynamic and inter-connected environments provide various important functions with the power to improve communications, protect personal, confidential and other data and provide oversight and control of critical systems and business processes, all while stimulating competitiveness. However, ever-increasing interconnectivity is expanding the attack surface, and adversaries are ready to exploit every possible vulnerability at every level.

Over the last couple of years, we have observed the blurring of boundaries between different types of threat and different types of threat actor. One example of this is the dumping of code by the Shadow Brokers group, which put advanced exploits at the disposal of criminal groups that would not otherwise have had access to that kind of sophisticated code. Another example is the emergence of advanced targeted threat (APT) campaigns focused not on cyberespionage, but on theft - stealing money to finance other activities that the APT group is involved in.

The motivations of threat actors vary widely – from money theft to undermining competitors, identity theft and fraud. Furthermore, every industry and organization has its own unique data to protect, a unique set of applications, technologies they use, etc. All this brings tremendous variability in the ways attacks are executed, with new methods emerging every day.

In this rapidly changing threat landscape, driving business growth through digital transformation can be exceptionally challenging, and business leaders need to take a strategic approach by constantly weighing up cyber risks against overall business goals and priorities.

Strategic threat intelligence provides a high-level view of the attack trends, techniques and methods used by attackers, including their motivations and attributions and helps answer a specific set of questions:

- Who are your adversaries? What do they want?
- What threat groups are active in your sector or region?
- What are the attack vectors being used?
- What is the best way to mount an attack against your organization?
- Which routes and what information is available to an attacker specifically targeting you?
- Has an attack already been mounted? Are you about to be threatened?
- What actions are necessary to reduce your risk profile?

Understanding these questions and mapping the answers to your critical assets, systems and business processes enables you to perform a thorough risk analysis, and communicate clear, relevant risk scenarios to your executive leadership team - and in doing so, justify investments in specific programs, technologies and staff. Empowered by these insights, a company can focus its information security strategy on the areas pinpointed as cybercriminals' prime targets and act quickly and with precision to repel intruders and minimize the risk of a successful attack.

Kaspersky offers

Report type	Intelligence provided	Use case
APT Intelligence Reporting	· Descriptions of tactics and methods used by attackers in cyberespionage campaigns with cross-sector targeting · Threat actor profiles with the TTPs (Tactics, Techniques and Procedures) they use · Mapping the associated TTPs to MITRE ATT&CK – a knowledge base of adversary TTPs based on real-world experience.	· Understand the threat actors targeting your industry or region and what TTPs they use · Identify what information assets and systems are at risk, the potential impact of compromise and how to prioritize accordingly · Adjust information security strategies, plan and justify investments in certain technologies, staff and programs covering potential attack vectors.
Financial Threat Intelligence Reporting	· Descriptions of tactics and methods used by attackers targeting the financial sector · Information about attacks on specific infrastructures, like ATMs or Point of Sale devices · Information about specific tools tailored to attack financial networks that are used, developed and sold by cybercriminals on the Darknet communities and forums in various geographies.	· Identify the adversaries targeting financial institutions globally, and the TTPs they use · Identify what information assets and systems are at risk, the potential impact of compromise and how to prioritize accordingly · Adjust information security strategies, plan and justify investments in certain technologies, staff and programs covering potential attack vectors.
Digital Footprint Intelligence	· Passive identification of the network perimeter, available services and existing vulnerabilities · Tailored vulnerability and exploit analysis · Identification, monitoring and analysis of any active or inactive malware samples targeting your organization · Data and credential leaks · Phishing threats targeting customers' brands · Evidence of threats and botnet activity specifically targeting a company's customers, partners and suppliers · Industry-specific analysis, including relevant cybercriminal TTPs.	· Ensure the availability and correct allocation of resources to mitigate the identified security flaws · Inform complex third-party due diligence projects to counteract supply chain attacks · Adjust policies and controls to mitigate potential insider threats · Increase internal staff security awareness by developing a specific program based on findings (e.g. corporate credentials compromised through third-party services) · Mitigate potential reputational damage by monitoring unauthorized use of company brands for phishing purposes · Plan and justify investments in certain technologies, staff and programs covering relevant attack vectors.

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

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/transparency

Proven.
Transparent.
Independent.