Kaspersky for Security Operations Centers

Evaluating threat intelligence sources

kaspersky

Learn more on kaspersky.com
#bringonthefuture

With the expanding attack surface and the growing sophistication of threats, just reacting to an incident is not enough. Increasingly complex environments provide multiple opportunities for attackers. Each industry and each organization has its own unique data to protect, and uses its own set of applications, technologies, etc. All this introduces an enormous number of variables into possible methods of executing an attack, with new methods emerging daily.

Over the last couple of years, we have observed the blurring of boundaries between different types of threat and different types of threat actors. Methods and tools that were previously a threat to a limited number of organizations have spread to the broader market. One example of this is the dumping of code by the Shadow Brokers group, which put advanced exploits (allegedly developed by the NSA) 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 persistent threat (APT) campaigns focused not on cyberespionage, but on theft - stealing money to finance other activities that the APT group is involved in. And the list goes on.

A new approach is needed

Methods and tools that were previously a threat to a limited number of organizations **have spread to the broader market.**

With enterprises increasingly falling victim to advanced and targeted attacks, it's clear that a successful defense requires new methods. To protect themselves, businesses need to take a proactive approach, constantly adapting their security controls to the ever-changing threat environment. The only way to keep up with these changes is to build an effective threat intelligence program.

Threat intelligence has already become a key component of security operations established by companies of varying sizes across all industries and geographies. Provided in human-readable and machine-readable formats, threat intelligence can support security teams with meaningful information throughout the incident management cycle and inform strategic decision-making (Figure 1).

However, the growing demand for external threat intelligence has given rise to an abundance of threat intelligence vendors, each offering a host of different services. An extensive and competitive market with innumerable, complex options can make choosing the right solution for your organization highly confusing and extremely frustrating.

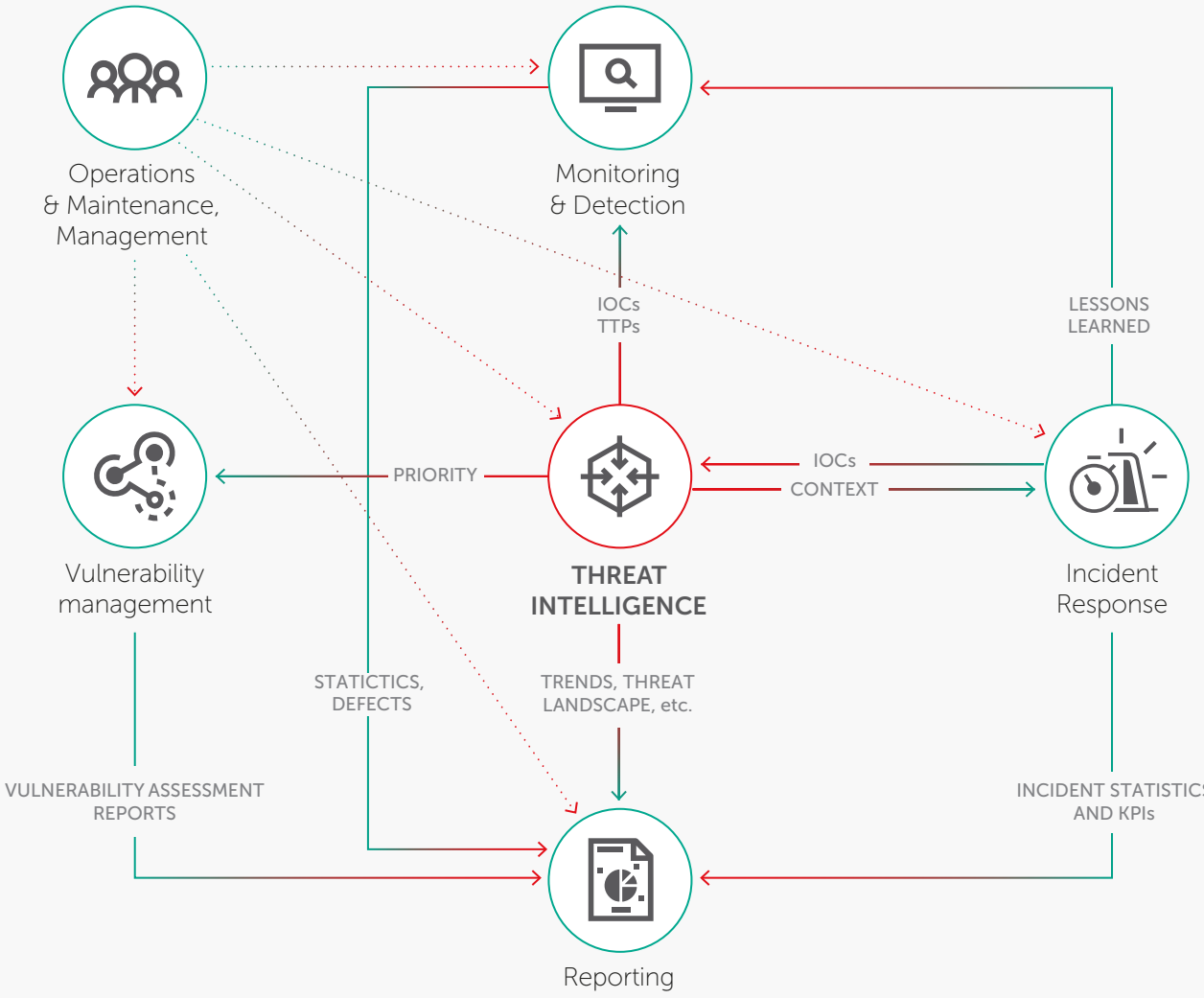

Figure 1
Threat Intelligence-driven Security Operations

Threat intelligence that isn't tailored to the specifics of your business can exacerbate the situation. In many companies today, security analysts spend more than half their time sorting out false positives instead of proactive threat hunting and response, leading to a significant increase in detection times. Feeding your security operations with irrelevant or inaccurate intelligence will drive the number of false alerts even higher and have a serious, negative impact on your response capabilities – and the overall security of your company.

Where the best intelligence lives...

So how do you evaluate the numerous threat intelligence sources, identify the ones that are most relevant to your organization, and effectively operationalize them? How do you navigate through the enormous amounts of meaningless marketing with almost every vendor claiming that its intelligence is the best?

These questions, although valid, are definitely not the first ones that you should be asking. Attracted by flashy messages and lofty promises, many organizations believe that an external vendor can provide them with some kind of superpower x-ray vision, completely overlooking the fact that the most valuable intelligence resides within the perimeter of their own corporate networks...

Data from intrusion detection and prevention systems, firewalls, application logs and logs from other security controls can reveal a lot about what's going on inside a company's network. It can identify patterns of malicious activity specific to the organization. It can differentiate between a normal user and network behavior and help to maintain a trail of data-access activity.

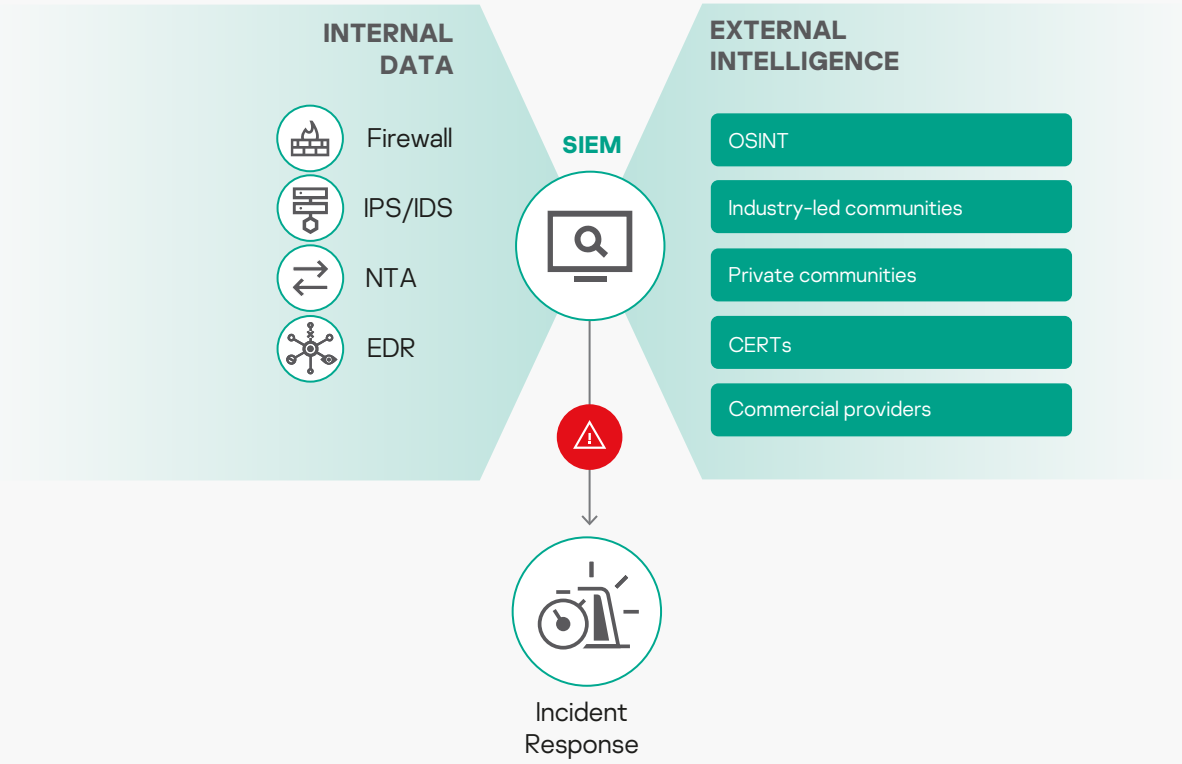

Figure 2
Operationalizing External Threat Intelligence

Think like an attacker

To build an effective threat intelligence program, companies, including those with established Security Operations Centers, must think like an attacker, identifying and protecting the most likely targets. Deriving real value from a threat intelligence program requires a very clear understanding of what the key assets are, and what data sets and business processes are critical to accomplishing the organization's objectives. Identifying these 'crown jewels' allows companies to establish data collection points around them to further map the collected data with externally available threat information. Considering the limited resources that information security departments usually have, profiling an entire organization is a massive undertaking. The solution is to take a risk-based approach, focusing on the most susceptible targets first.

Once internal threat intelligence sources are defined and operationalized, the company can start thinking about adding external information into its existing workflows.

It's a question of trust

External threat intelligence sources vary in trust levels:

- Open sources are available for free, but they often lack context and return a significant number of false positives.
- A good option to start with is accessing industry-specific intelligence-sharing communities, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). These communities provide extremely valuable information, although they are often gated and membership is required to gain access.
- Commercial threat intelligence sources are much more reliable, although buying access to them can be expensive.

The guiding principle for choosing external threat intelligence sources should be quality over quantity. Some organizations may think that the more threat intelligence sources they can integrate, the better visibility they will get. This may be true in some instances - for example, when it comes to highly trusted sources, including commercial ones, providing threat intelligence tailored to the organization's specific threat profile. Otherwise, there is a significant risk of overwhelming your security operations with irrelevant information.

The overlap in information supplied by specialized threat intelligence vendors can be very small. Because their intelligence sources and collection methods vary, the insights they provide will be unique in some aspects. For example, one vendor, due to being a major presence in a specific region, provides more details about threats emanating from that region, while another provides more details on specific types of threat. So gaining access to both sources may be beneficial – when used together, they may help to reveal a bigger picture and guide more effective threat hunting and incident response missions. Bear in mind, though, that these kinds of trusted sources also require careful prior evaluation to ensure that the supplied intelligence is appropriate for your organization's specific needs and use cases, like security operations, incident response, risk management, vulnerability management, red teaming, etc.

Issues to consider when evaluating commercial threat intelligence offerings

There are still no common criteria for evaluating various commercial threat intelligence offerings, but here are some things to bear in mind when doing so:

- Look for intelligence with global reach. Attacks have no borders - an attack targeting a company in Latin America can be initiated from Europe and vice versa. Does the vendor source information globally and collate seeming disjoined activities into cohesive campaigns? This kind of intelligence will help you to take appropriate action.
- If you are looking for more strategic content to inform your long-term security planning, like:
  - High-level view of attack trends
  - Techniques and methods used by attackers
  - Motivations
  - Attributions etc.,

then look for a threat intelligence provider with a proven track record of continuously uncovering and investigating complex threats in your region or industry. The ability of the provider to tailor its research capabilities to the specifics of your company is also critical.

- Context makes intelligence from data. Threat indicators without context are of no value - you should look for providers that help you to answer the important 'why does this matter?' questions. Relationship context (e.g. domains associated with the detected IP addresses or URLs where the specific file was downloaded from etc.) provides additional value, boosting incident investigation and supporting better incident 'scoping' through uncovering newly acquired related Indicators of Compromise in the network.
- It's assumed that your company already has some security controls in place, with the associated processes defined, and that it's important for you to use threat intelligence with the tools you already use and know. So look for delivery methods, integration mechanisms and formats that support smooth integration of threat intelligence into your existing security operations.

At Kaspersky we've been focusing on threat research for over two decades. With petabytes of rich threat data to mine, advanced machine-learning technologies and a unique pool of global experts, we work to support you with the latest threat intelligence from around the world, helping to keep you immune from even previously unseen cyberattacks.

For more information, please visit
https://www.kaspersky.com/enterprise-security/security-operations-center-soc/

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity 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.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.