

Buyer's Guide

Cyber Threat Intelligence

A Comprehensive Guide
to Your Threat Defense

Jakub FILIP



Digital Security
Progress. Protected.

July 2023



Digital Security
Progress. Protected.

© 1992–2023 ESET, spol. s r.o. – All rights reserved.
Trademarks used herein are trademarks or registered
trademarks of ESET, spol. s r.o. or ESET North Ameri-
ca. All other names and brands are registered trade-
marks of their respective companies.

Table of Contents

Introduction	4
Understanding Threat Intelligence (TI)	6
2.1 Before Jumping In	6
2.2 Threat Intelligence Market	8
2.2.1 What to Look for When Choosing a TI Provider?	8
2.2.2 How Do Organizations Usually Consume TI?	11
2.2.3 Why Does the Maturity of Organizations Matter?	13
2.2.4 Overall TI Market Outlook	14
ESET Threat Intelligence	18
3.1 What is ESET Threat Intelligence (ETI)?	18
3.1.1 What can ETI Provide?	19
3.1.2 ETI Data Feeds	21
3.1.3 APT Reports	22
Conclusion	26
About ESET	28

Introduction

It is essential for organizations to stay informed and well-equipped to effectively tackle cyber threats, and the adoption of cyber threat intelligence is one way to do so.

The guide that you are about to read is specifically designed to serve three vital purposes:

- **First, it provides you with a comprehensive understanding of what cyber threat intelligence truly entails.**

- **Second, it sheds light on how the current threat intelligence market operates to help you understand the topic holistically.**


- **Third, it helps you answer the fundamental question of whether your organization needs threat intelligence, and what to look for if it does.**

Furthermore, this guide emphasizes the importance of considering your organization's broader context and needs when evaluating threat intelligence solutions. It highlights the essential features and criteria that should be assessed during the purchase decision-making process. By demanding

solutions that align with your specific requirements, you can ensure that the chosen threat intelligence solution effectively addresses your organization's unique challenges.

We conclude this guide by introducing a solution from ESET that has been developed to help you cover your needs as well as enhance your overall threat defense strategy. With ESET's human expertise, the solution offers a comprehensive suite of features and capabilities that is designed to meet the evolving threat landscape.

By providing valuable insights, comprehensive knowledge, and a solution-oriented approach, this guide aims to equip security specialists, analysts, IT managers, and C-suite members with the necessary tools to navigate the complex world of cyber threat intelligence. With this knowledge, you can make informed decisions, enhance your organization's security posture, and safeguard against emerging cyber threats.



This guide aims to equip security specialists, analysts, IT managers, and C-suite members with the necessary tools to navigate the complex world of cyber threat intelligence.

Understanding Threat Intelligence (TI)

2.1 Before Jumping In

Cyber threat intelligence refers to the ways of thinking and the method of a practical approach to dealing with real or potential cyber threats.

It [includes](#) gathering, analyzing, and contextualizing information about the potential and ongoing threats to an organization's information technology systems. It is a proactive approach to cybersecurity that enables organizations to identify, assess, and mitigate the risks posed by cyber threats.

Special attention needs to be paid to the aspect of **contextualization**. It is critical for generating unique expert knowledge, and speaking about complementarity of TI, contextualization is the right spot where human expertise comes into play. That is also where crucial differences in the quality of such service can occur. Threat intelligence can be obtained from various sources, such as open-source intelligence, commercial intelligence services, government intelligence agencies, and in-house threat intelligence teams.

The reason why we can conceive of threat

intelligence as a way of thinking is that it changes the overall threat protection paradigm, and it shapes the course of action and the decision-making processes. This can result in identifying vulnerabilities and potential attack vectors, which can be used in the process of improving an organization's cybersecurity posture.

The ultimate goal of threat intelligence is to:

- Enable organizations to **take proactive measures to prevent** or mitigate **cyber-attacks**,
- Enable you to **prioritize** where to focus limited **resources** to mitigate the biggest risks,
- Help you with **triaging events** and reducing the damage from potential attacks,
- **Minimize the overall negative impact** once an organization is attacked,

- **Respond effectively** to such security incidents.

From the practical point of view, threat intelligence is highly useful in situations where, for instance, IP addresses associated with malicious infrastructure, Bot IPs, tactics, techniques, and procedures (TTPs), compromised credentials or web injects inserting HTML or JavaScript code occur. However, there are [more real-life situations](#) where TI can be helpful. Some of them will be tackled in the present paper.

The reason why we can conceive of threat intelligence as a way of thinking is that it changes the overall threat protection paradigm, and it shapes the course of action and the decision-making processes.

2.2 Threat Intelligence Market

2.2.1 WHAT TO LOOK FOR WHEN CHOOSING A TI PROVIDER?

When choosing a threat intelligence provider for your company, there are several factors that you should consider in order to ensure that the provider that you select meets your organization's needs. However, before you proceed to identify them, you should bear in mind that there is a general distinction between four types of threat intelligence: **strategic**, **tactical**, **technical**, and **operational**.

It might not be the case that all three are equally represented in the vendors' service offerings. The focus very much depends on such aspects as the target market, business goals, vendors' own capabilities, how sophisticated the threats are that require attention, what

the attack surface is, etc.

However, such distinction is also driven by consumers of TI and organizational hierarchies in such companies, respectively. Strategic leaders, C-suite, or board members are most likely to be interested in **strategic TI**. **Tactical TI** may be better suited for security practitioners like SOCs, threat analysts, threat hunters, or incident responders. Security practitioners at the operational level who are responsible for the efficient allocation of IT resources and security controls would then be interested in **operational TI**.



STRATEGIC

Strategic TI is meant to identify broad trends that can comprehensively enhance knowledge and put the information in the respective context. It could come in the form of white papers, briefings, or reports.



TACTICAL

Tactical TI is used to identify the how and where of the attacks and, therefore, provides a more detailed and retrospective look at the very incident. Examples include privilege escalation, defensive evasion, or lateral movement



TECHNICAL

Technical TI helps to identify the what, and so it mostly covers what types of indicators of compromise (IOCs) occur

**\$44
billion**

is the forecasted value for
the cyber threat intelligence market by 2033.

Source: Statista Research Department, [Cyber threat intelligence \(CTI\) market size worldwide from 2023 to 2033](#), March 31, 2023.

during incidents. This information can be best utilized by SOC analysts or incident response engineers.



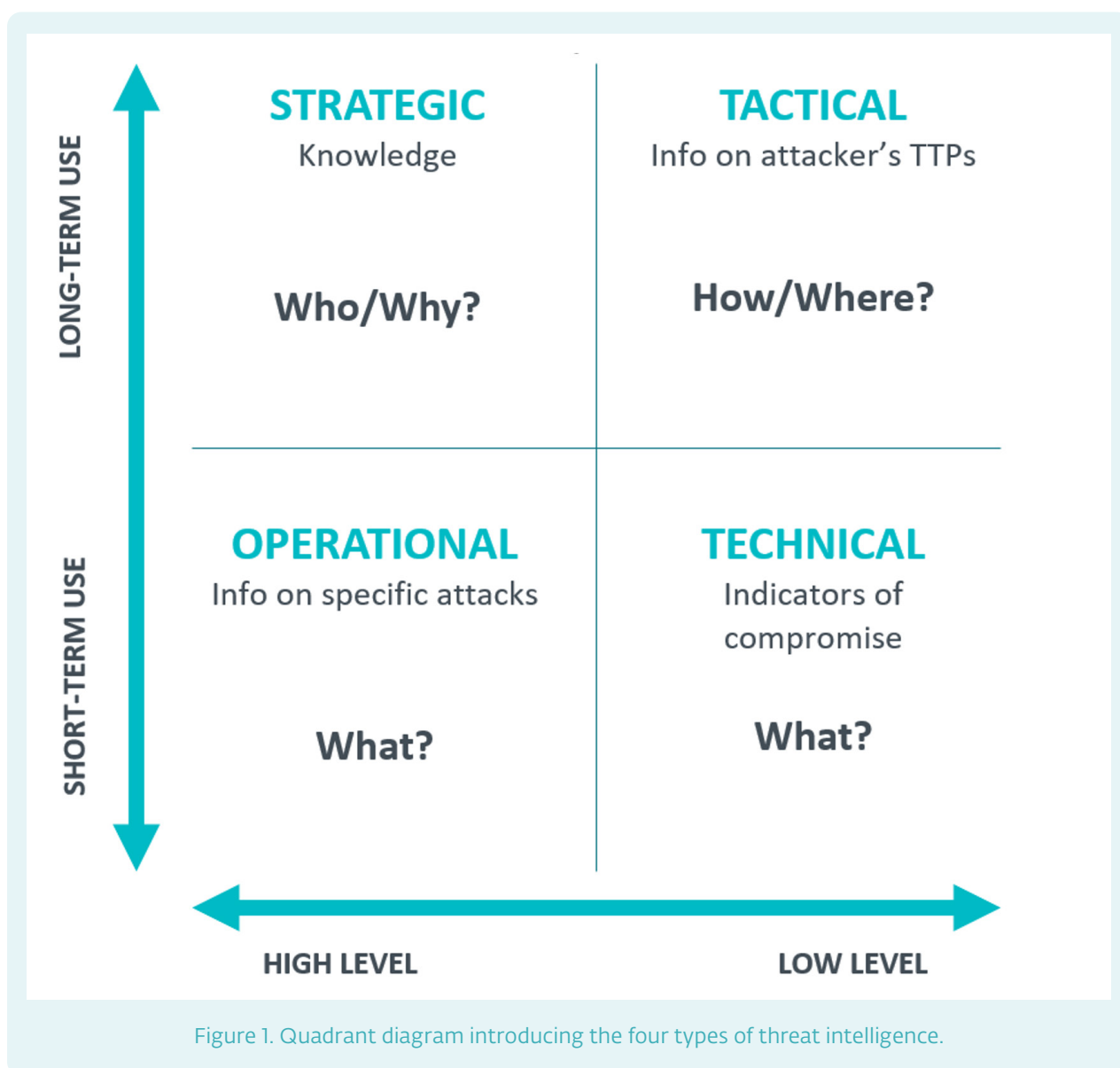
OPERATIONAL

Operational TI primarily focuses on tracking adversary movements as well as understanding the techniques being used during an attack. Examples of IOCs that the operational level focuses on include URLs, file hashes, malicious IPs, registry keys, or network traffic patterns and protocols.

To be capable of assessing the qualities of TI, a company must consider various factors, including the following.

COMPLETENESS

Look for a provider that offers comprehensive threat intelligence covering a wide range of threat actors and respective threat vectors that include malware, phishing, and other types of cyber threats. This can help you take the appropriate action to reduce risks. The provider should have access to a



variety of data sources, including internal telemetry, open-source intelligence, and other external feeds.

ACCURACY

A provider should help you save resources through implementing a successful solution rather than a costly one resulting from inaccurate TI. Inaccurate intelligence can lead to unfavorable signal-to-noise ratios in your SOC, placing security controls in the wrong locations, or simply establishing the wrong configuration. This needs to be mastered comprehensively to reliably defend your organization.

RELEVANCE

Addressing a threat within a particular and unique environment is another important aspect. Look for a provider that can tailor the feeds to your industry or company size, and that provides insights that are relevant to your specific threat landscape. Focusing on either the

tactical or strategic level and deciding what is relevant for you in the short- and long-term period is also important.

TIMELINESS

Ensure that the provider offers real-time updates to their threat intelligence feeds. Cyber threats evolve rapidly, and so it's crucial to have up-to-the-minute information to stay ahead of emerging threats. Delivering a warning signal after an attack has already begun has very little value to an organization.

Additional factors that you should consider include the following:

Customization: Look for a provider that can customize its threat intelligence feeds to the specific needs of your organization. Clearly defined needs help you find a match with a potential provider.

Scalability: Customization alone might not be sufficient. Therefore, ensure that

40%

will be invested by C-suite leaders of G2000 on enterprise and market intelligence by the end of 2025.

Source: [*IDC FutureScape: Worldwide Future of Intelligence 2023 Predictions.*](#)

80%

of G2000 companies will increase investment in intelligence about threats by 2024.

Source: [*IDC FutureScape: Worldwide Future of Intelligence 2023 Predictions.*](#)

the provider can scale their services to meet the needs of your organization as it grows. This includes the ability to support a large number of users, provide customized reporting and analytics, and integrate them with your existing security tools.

Reputation: Look for a provider with a strong reputation in the industry that also has a track record of providing reliable and effective TI services to organizations that are similar to yours. By working with such a TI provider, your organization can stay ahead of cyber threats thanks to the protection of

your critical assets and infrastructure. A good reputation is still regarded as an indication of quality and capabilities.

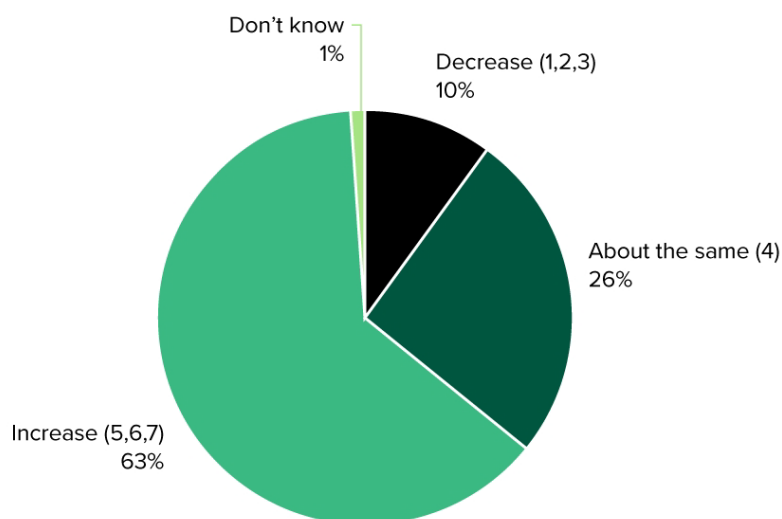
2.2.2 HOW DO ORGANIZATIONS USUALLY CONSUME TI?

Understanding how organizations usually consume TI services might help you acquire better and more prospective knowledge regarding the options that you can benefit from when considering adopting TI in your company.

Organizations are faced with a myriad of cyber threats that can jeopardize their business, reputation, and financial

Which of the following describes any change in your budget for security technologies for threat intelligence (including employees, products, and services) from 2022 to 2023?

(5, 6, or 7 on a scale of 1 [decrease] to 7 [increase])



Base: 3,580 security decision-makers with seniority level of manager or above

Source: Forrester's Security Survey, 2022

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: [The State Of Threat Intelligence, Forrester, April 13, 2023](#)

stability. Reliable and actionable TI services are, therefore, a must.

There are various ways in which organizations consume TI. These include industry feeds, open source intelligence, peer-to-peer sharing, and vendors.

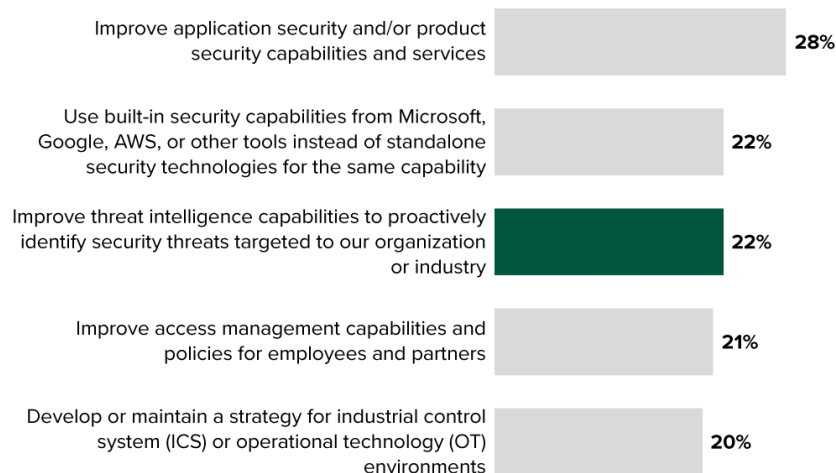
1. INDUSTRY FEEDS are information-sharing platforms that bring together organizations in the same industry verticals or various analyst centers and firms. These feeds provide organizations with timely and relevant information on emerging threats, attack techniques, and indicators of compromise (IOCs) that are specific to their industry. Some industry

feeds are paid, while others are free of charge.

2. OPEN SOURCE INTELLIGENCE (OSINT) as a way of gathering and analyzing information includes working with public records, news articles, government websites, community forums, blogs, and social media platforms that provide a wealth of information on cyber threats. [OSINT](#) has a similar goal as industry feeds, but it is traditionally utilized by small groups or individuals and is more open and accessible in terms of sharing information that can be of an unofficial nature.

“Which of the following initiatives are likely to be your organization’s top tactical information/IT security priorities over the next 12 months?”

(Multiple responses accepted)



Note: Not all response options are shown.

Base: 2,355 global security technology decision-makers

Source: Forrester’s Security Survey, 2022

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: [The State Of Threat Intelligence, Forrester, April 13, 2023](#)

3. PEER-TO-PEER SHARING is another way in which organizations consume TI. In this case, organizations share information within the same industry vertical, but only in a small subset of such a vertical. Peer-to-peer sharing usually happens between businesses of the same size and with the same business capabilities.

4. VENDORS. Finally, organizations can also rely on vendors that provide intelligence as a part of their product services. You can see vendors as independent threat intelligence providers, security vendors, or managed security service providers (MSSPs). These vendors provide a range of services, including TI feeds, reports, threat hunting services, and managed security services.

Different ways of consuming TI very much depend on the organizations' specific needs, capabilities, and resources. Industry feeds, open source, peer-to-peer sharing, and vendors are all important sources of TI, and by leveraging these sources, organizations can improve their threat detection capabilities, enhance their incident response, and ultimately strengthen their overall security posture.

2.2.3 WHY DOES THE MATURITY OF ORGANIZATIONS MATTER?

The adoption of TI services is becoming increasingly important

across all industries, especially for large organizations. However, the level of an organization's maturity plays a crucial role in determining the type of TI services that an organization should adopt.

Mature organizations with dedicated TI teams often demand more features and functionality to collect, process, and disseminate their own intelligence. These organizations have a better understanding of their security posture and the specific threats that they face. They also usually consume from eight to fifteen sources of TI, which can include free, open source, CERTs, ISACs, and commercial providers. These organizations are looking for advanced features like graph analytics, link analysis, or threat actor tracking/modeling to improve their threat detection capabilities.

>50%

of G2000 organizations will face penalties by the end of 2025 if they do not use AI for detection and automatic remediation of data due to growing complexity, volatility, and resource scarcity.

Source: *IDC FutureScape: Worldwide Future of Intelligence 2023 Predictions.*

On the other hand, less sophisticated organizations with limited or no dedicated TI teams may choose TI point solutions that focus on aggregated machine-readable threat intelligence (MRTI) feeds. These organizations have integrations that are ready to go off the shelf and are not so much interested in advanced features. They are looking for a solution that is easy to deploy and provides them with the necessary TI to improve their security posture.

Mature organizations are at an advantage: With dedicated TI teams, they have the expertise and resources to fully leverage the capabilities of the TI services that they adopt. Furthermore, they can integrate TI with their existing security infrastructure, conduct a detailed analysis of threat data, and use it to inform their security strategy. All of this poses a better cybersecurity resilience.

Less mature organizations, on the other hand, may struggle to fully leverage the benefits of TI. They may lack the resources or expertise to effectively integrate TI with their existing security infrastructure and may not have the necessary skills to analyze and use the data to improve their security posture. That makes them more vulnerable and less prepared to face cyber threats. The good news is that every organization that is less sophisticated in terms of its capabilities can become a mature one and that means becoming more resilient.

2.2.4 OVERALL TI MARKET OUTLOOK

The cyber TI market nowadays is a [still-growing field](#) and it might seem like a maze full of uncluttered paths and indecipherable options. When considering adopting a TI solution, you should take a few aspects into account to understand and fully benefit from it. These can be defined as the following.

1. New Intelligence Categories

The first aspect to keep in mind when trying to understand the cyber TI market is that new intelligence categories are constantly emerging and, therefore, the market and solutions change dynamically. These new categories help evaluate new threats and provide intelligence that is reflected in the current offerings. Examples of these categories include climate risk intelligence and critical event intelligence that allow organizations to get tailored data and insights for a specific location and environment. Consider your specific needs from a long-term perspective to prevent the frequent reassessment of strategy.

2. Addressing Different Types of Threats

The second aspect is that large organizations usually require multiple TI services to address different types of threats. Organizations are investing in an

arsenal of products to account for each unique type of risk that they are facing. It may happen that a vendor that excels in a critical event intelligence capability may lack such capability in a different area, e.g., in malware analysis. It is, therefore, crucial to determine the level of complexity and particular capabilities to avoid disproportional and poorly targeted solutions.

3. IOC Feeds

The IOC feeds—once standalone products—are now features of more valuable intelligence services. Nowadays, standalone IOC feeds lack the context that they need for better security tactical decisions and, therefore, many security controls that vendors offer are part of other TI detection capabilities. As mentioned hereinabove, understanding the overall context in which threats emerge and which delimits your own playground is essential to your threat defense. We encourage you to seek holistic solutions allowing you to dive deep into the threat landscape.

4. Expansion of Use Cases, Personas, and Processes

The fact is that TI is expanding to support more use cases, personas, and processes, especially those related to improved visibility and the protection of digital assets. TI offerings now support not only

traditional security roles, such as CISOs and SOC analysts, but also roles that are not typically aligned with a TI. For instance, brand teams, marketing teams, compliance teams, and legal functions can all benefit from cyber TI. Understanding this shift as well as its background and reasoning is critical in evaluating the potential that a TI solution can bring you. The more enlightened your employees are, the more you can rely on them and, therefore, benefit from being receptive to the possible pitfalls and issues.

5. IP and TI Vendors Expanding into New Markets

The fifth aspect to keep in mind is that TIP and TI vendors are expanding into new markets as a result of how the overall situation with cyber threats is evolving. The expansion has reached such markets as SOAR, CM, XDR, external service management, and third-party risk management. The reason for this come from the necessity of addressing the need to keep up with highly sophisticated threats where the risks and consequences of cyber attacks are now higher than ever before. This fact gives you an opportunity to reflect on your own situation and assess your prospective needs.

The cyber TI market is constantly evolving and, therefore, understanding it and selecting the right solution can be challenging. However, by keeping in mind the emerging intelligence categories, the need for multiple TI services, the value and nature of IOC feeds, the expanding use cases and personas that TI can support, and the expansion of TIP and TI vendors into new markets, organizations can better assess their own situation and needs, the overall situation in which TI is practiced, and thereby make the right decision.

Even though the TI market is nowadays expanding in many ways, there are some challenges that TI vendors need to deal with in order to provide a solution that organizations can rely on. ESET can comprehensively address them thanks to its advanced capabilities and expertise. These challenges include the following:

1 OVERWHELMING AMOUNT OF DATA

ESET offers only curated intelligence that is wrapped up in comprehensive private APT reports. We can also provide an additional attribution to the data feeds.

2 LACK OF EXPERTISE TO INTERPRET

ESET only offers contextual intelligence; it

is supported by MITRE ATTACK; tagging respective TTPs and providing details on targeted business verticals, sometimes even a country or region.

3 HIGH COSTS/LEVEL OF EXPANSES


Although usually quite a subjective matter, ESET has a competitive offering consisting of a positive cost versus benefit ratio, especially when taking the overall market costs into consideration.

4 LACK OF DIFFERENTIATION IN SOURCES

ESET offers a unique proprietary intelligence supported by ESET's own research teams providing real-time expertise in targeting attacks, APT actors, Zero Days threats, or botnet activities; ESET's threat intelligence is based on a unique telemetry, and it utilizes ESET's multilayered technologies.

5 POOR OPERATIONALIZATION

ESET offers aggregated MRTI (machine-learning threat intelligence) feeds and comprehensive attribution details, including the timeline of an attack, MITRE attack technique, or some other attribution details that organizations are interested in.



Even though the TI market is nowadays expanding in many ways, there are some challenges that TI vendors need to deal with in order to provide a solution that organizations can rely on.

ESET Threat Intelligence

3.1 What is ESET Threat Intelligence (ETI)?

[ESET Threat Intelligence](#) is defined by its **preventive approach to cybersecurity that aims at providing quick reaction capabilities, better preparedness, and proactive measures** to various kinds of cyber threats.

It is, therefore, a comprehensive and advanced intelligence service that enables customers to detect, analyze, and respond to cyber threats in a timely and efficient manner. It offers a range of intelligence-gathering techniques and resources, such as malware analysis, threat intelligence feeds, and a list of suspicious URLs and domains in order to provide customers with actionable insights and a deep understanding of the emerging threats

One of the key benefits of ETI is that it enables customers to quickly identify and respond to cyber threats. ETI also provides customers with a better understanding of their own security posture and helps them to improve it over time. Moreover, ESET Threat Intelligence can be a great solution for organizations that never had ESET solutions and products in their environments because it provides them with a holistic and fully tailored approach

to their security policies.

ETI gives organizations the advantage of having a **unique geographical coverage** that is something that has proven to be crucial in recent years due to unseen shifts in cybersecurity challenges, including more sophisticated as well as more targeted and localized attacks, and specific compliance requirements, but also due to significant changes in [geopolitics](#). Nation-state actors and APT groups play a crucial role in improving the damaging potential of cyber threats. These actors are attacking not only public organizations, but more often private ones as well, as they might have strategic importance. Therefore, investing in threat intelligence capacities is becoming a new norm for private organizations of all sizes.

Thanks to ETI, ESET repeatedly performed as one of the best providers of intel on cyberwarfare during the Russian aggression against Ukraine. Our researchers and experts are mapping a wide range of APT groups, often most notoriously operating from Russia, China, North Korea, and Iran. Unique geographical coverage enables organizations to identify which tools and

techniques adversaries in other countries use and thereby anticipate the potential attacks in a specific region and that makes them more resilient.

3.1.1 WHAT CAN ETI PROVIDE?

ETI is designed to provide knowledge and expertise to help organizations mitigate cybersecurity risks. It contains various data feeds, metadata, curated feeds, and it is focused on quality instead of quantity while providing highly relevant and market-leading information. One of the most important features of ETI is real-time feeds that provide up-to-the-minute information on the latest threats.

Thanks to ETI, your organization can investigate incidents, test hypotheses, and improve threat-hunting capabilities. ETI also provides a lot of metadata that can give you contextual information on threats, such as the source, type, and severity of the threat. This metadata is updated frequently, ensuring that organizations always have access to the latest information.

“ESET has gained well-earned notoriety and experienced increased demand by governments, Ukraine-based organizations, and global organizations for ESET’s threat intelligence services and security products.”

Source: IDC, *Worldwide Modern Endpoint Security Market Shares, July 2021–June 2022: Currency Exchange Rates Slightly Trimmed Accelerating Growth, Doc # US49982022, January 2023.*

By having ESET's APT reports at hand, you can gain comprehensive knowledge of the threat landscape, including an analysis of the threat actors, their compromise methods and behavior, specific technical details, activity summaries, and more. These reports are designed to be used by security analysts, incident responders, and other cybersecurity professionals.

ETI allows organizations to take advantage of checking the levels of confidence when it comes to assessing the collected data inputs. This is particularly important because it enables organizations to define the reliability of the data that they are using and, therefore, make better-informed decisions. Thanks to testing hypothesis, customers can improve their overall threat-hunting capabilities. This is crucial when aiming at becoming more proactive instead of just waiting passively until an attack occurs.

The main benefits of ETI that can strengthen your cybersecurity posture include:

- **Human expertise** based on the experience of ESET's threat intel analysts
- **Understanding** risks and thereby **predicting threats, mitigating** incidents, and **reducing** exposure to the currently prevailing threats
- Improving **threat hunting** and **remediation**

- Gathering TI from a **unique range of sources**
- Enabling you to spot potential compromises by **scanning systems** via Yara or checking networks
- **Monitoring APT groups** and gaining a profound understanding of their tactics, methods, or even motives
- **Saving resources** due to low maintenance requirements thanks to curated content
- Enabling you to make **faster, more useful, and better decisions** in both short- (block IP ranges, hashes, etc.) and long-term periods (intelligence and cybersecurity strategy)
- Constant seeking of threats, across **multiple layers**, from pre-boot to the resting state

ESET provides a type of TI that is easy to use and maintain. It features:

- **Curated and highly actionable expert intelligence**
- **Robust telemetry**
- **Automation across multiple layers** with the emphasis on seeking and detecting threats from pro-boot to a restful state
- **Integration of feeds** into your current architecture (SIEM/SOAR/TIP) supported by ESET's guidelines

- Extended integration options such as compatibility with TAXII 2
- **Frequent updates** of feeds (every 5-10 minutes) and **filtering the IOCs based on their severity and prevalence**

3.1.2 ETI DATA FEEDS

As mentioned hereinabove, ETI provides organizations with [unique feeds](#). These are streams of data covering potential or actual threats to an organization's security as well as providing information in a comprehensive, actionable, and timely manner. ETI data feeds are curated from a pool of around 110 million sensors, ESET LiveGrid®, and an automated botnet tracking system ensuring the lowest possible number of false positives.



MALICIOUS FILES FEED

This feed provides real-time information on the currently prevalent malware samples as well as their characteristics and IOCs. The feed helps you understand which malicious files are being seen in the wild and enables you to proactively block them before they can cause any harm. It features the assessment of shared hashes of malicious executable files and associated data. The feed is updated frequently, and it comes with filtering so that customers only obtain relevant data with low levels of redundancy.



APT FEED

As the name suggests, this feed covers APTs from the research point of

view, focusing mainly on IOCs associated with APT groups' attacks. The feed allows you to conduct precise and reliable detection and response, prevent data exfiltration, and protect critical assets. It is based on data collected and produced directly by ESET research, and it comes as an export from the ESET internal MISP server. All of the information is shared as part of a detailed APT report in which they are presented in context and comprehensively explained, but the feed can also be purchased separately.



DOMAIN FEED

This feed blocks malicious domains to prevent users from visiting the sites and, therefore, stay protected against infections and data breaches. Such domains are usually part of the phishing campaigns, command-and-control (C2) infrastructure for malware, or a larger cyber attack. The feed covers the domain name, IP address, and the date associated with them and respective malicious activity. The feed ranks the domains based on their severity, which enables you to adjust the response accordingly, e.g., to only block high-severity domains. The feed also provides information on the level of confidence in the form of an assessment of which domain to block.

URL FEED



Information about current and prevalent malicious URLs and associated data. The feed is created from all URL sources every 5 minutes, deduplication happens every 24 hours

and the filtering in this case is a little bit stricter to make sure no sensitive information is being shared. Therefore, it is based on sharing URLs without parameters. Unlike the Domain feed, a URL feed is much smaller and more targeted in terms of allowing analysts to block specific malicious URLs instead of blocking entire domains.



IP FEED

This feed shares the current and prevalent malicious and abusive IPs and some data associated with them. The structure of the data is similar to that used for the domain and URL feeds. The main use-case is to understand which malicious IPs are currently prevalent in the wild, to block those with high severity and inspect the less severe based on additional data, and to see what harm has already been caused. Filtering in this case is very similar to that in the URL feed.



BOTNET FEED

Based on ESET's proprietary, automated botnet tracking system, this feed features two types of sub-feeds: C&C and targets. The data provided includes items such as detection, hash, last alive, files downloaded, IP addresses, protocols, targets, and other information. IOCs include MD5, SHA1, SHA256; C and Cs (URLs).

3.1.3 APT REPORTS

ESET's Advanced Persistent Threat (APT) Reports represent a [reliable source of cyber threat intelligence](#) that covers APT actors and their activities. The reports provide strategic, tactical, technical as well as operational intelligence that empowers organizations to improve their detection of threats and to develop a more proactive cyber security posture.

It helps them with threat hunting and investigating and mitigating active incidents. More importantly, it also helps

49%

increase of paid commercial threat intelligence feeds from 2021 to 2022.

Source: [The State Of Threat Intelligence](#), Forrester, April 13, 2023.

60%

increase of feeds from information sharing communities from 2021 to 2022.

Source: [The State Of Threat Intelligence](#), Forrester, April 13, 2023.

65%

increase of freely available threat intelligence feeds from 2021 to 2022.

Source: [The State Of Threat Intelligence](#), Forrester, April 13, 2023.

them to be proactive or even predictive instead of being reactive, and to make better and faster decisions on both the technical and management levels. Knowing the adversary helps security leaders to determine which potential threats are most likely to become actual threats to their organization, to decide where to invest, and what to focus on.

INTEGRATION WITH MISP

One highly convenient practice for organizations is to consolidate all the data from reports into a threat intelligence platform. ESET offers access to its internal MISP (Malware Information Sharing Platform), which comes pre-filled with all the relevant and valuable data. Customers can, therefore, easily synchronize them with their own systems, thereby resulting in a seamless integration.

This integration via MISP proves to be extremely helpful for a variety of experts, as it saves both time and resources, while enabling them to easily familiarize themselves with the pool of thorough data. Notably, customers gain the ability to create their own queries, establish specific connections, conduct in-depth analyses, and leverage the diverse range of data available within the MISP. The integration is part of the Premium purchase package and stands for a unique approach setting ESET apart from other vendors which typically do not offer such comprehensive integration capabilities.

DETAILED LOOK AT APT REPORTS PREMIUM

APT Reports are really not just about IOCs, but also about the contextual information and other relevant details. These reports come as a package of several types of outputs:

- Activity Summary Reports,
- Technical Analysis Reports,
- Monthly Overview Reports,
- Monthly Digest Reports,
- APT Data Feed,
- Access to APT MISP server (allows customers to consume data in a more automatic way),
- Access to threat intel analysts

Organizations also get pre-publication access to the technical blog posts that are published on WeLiveSecurity.

1. Activity Summary Reports

These reports are issued within a timeframe of two weeks and describe the latest APT campaigns ESET researchers have been tracking from various threat actors as well as their targets and associated IOCs. These reports allow defenders to keep track of the most advanced threat actors out there and give them context about their current activities. The data can be used by **network defenders** to protect their networks by

blocking these IOCs. They also allow **researchers** and **incident response handlers** to improve their understanding of APT groups targeting their organizations by knowing their most up-to-date Tactics, Techniques, and Procedures (TTPs).

2. Technical Analysis Reports

To some extent, Technical Analysis Reports are similar to white papers that are published on WeLiveSecurity. These reports fall under the realm of tactical threat intelligence, and describe the recent campaigns, new toolsets, and related subjects. They contain actionable data such as YARA rules, Snort rules, pivoting queries such as Shodan and Censys, MITRE ATT&CK[®] mappings, recommendations on how to protect your network, and remediation advice where applicable. When complex malware frameworks are described, ESET also provides tools to help customers' analysts, such as de-obfuscation or decryption scripts. The reports are useful for **defenders** looking to protect their networks against the latest threats. They are also helpful for **researchers** and **incident responders** that must analyze and report on threats that might potentially target their

3. Monthly Overview Reports

Monthly Overview Reports combine information from all Technical Analysis and Activity Summary reports released in the previous month into a shorter and more digestible form. They focus on strategic, tactical, and operational threat intelligence, and cover updates on the activities of various threat actors including their targeted regions and business verticals. The reports are, therefore, suitable even for non-cybersecurity **C-level personnel, managers, and decision-makers**, or as monthly summary reports for researchers and incident responders. Monthly Overviews are automatically sent to customers who subscribe to ESET APT Reports PREMIUM. However, they aim to be self-standing and can be offered as a more accessible tier of reports to customers that subscribe to no other product or service offered by ESET. Monthly Overviews Reports do not contain any IOCs, as those are included in Technical Analysis and Activity Summary reports, where technical threat intelligence is enclosed.

4. Monthly Digest Reports

These are way less technical and provide critical facts from the Monthly Overview Reports in a brief, comprehensive, and digestible format. They are released regularly—one report per month

(12 per year in total) — and they include valuable information on targeted verticals, countries, and regions, and key and actionable facts every **threat defender, executive manager, CISO, or any other decision maker** can benefit from. The reports come in a concise one-pager format that makes them exceptionally practical.

ESET offers pre-publication access to a range of reports that have proven to be of high value for organizations and their preparedness. This includes the Threat Reports that are published on WeLiveSecurity twice a year. Subscribers gain exclusive access to these reports approximately 6-7 days before they are made available to the public.

The same applies to APT Activity Reports that mirror the release schedule of Threat Reports. In addition, subscribers can also benefit from pre-publication access to our technical blog posts that are published at least once per month. These blog posts become accessible approximately 2-3 days before their regular publication.

One of the advantages is that those few days of pre-publication could be crucial for threat hunters and defenders to scan systems as adversaries tracking our research could change their behavior and adapt to the new situation stemming from exposing the details of their activities. Pre-publications, therefore, simply help organizations stay ahead of time.

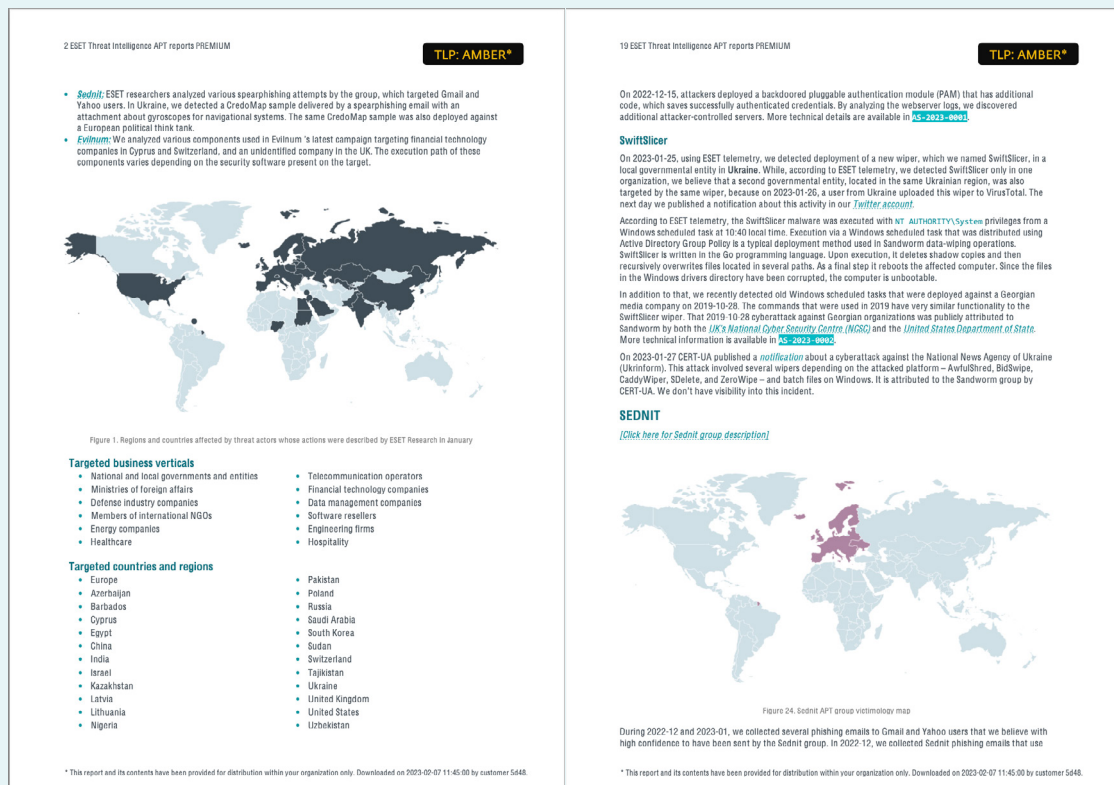


Figure 2. Excerpt from the ESET Monthly Overview Report. As displayed, these reports include information about targeted countries and business verticals, and feature various maps and timeline infographics.

Conclusion

Understanding threat intelligence might help you realize how important the contextual perspective on the threat landscape is.


Addressing your organization's needs is a crucial aspect when designing your defense strategy, and although threat intelligence is not always considered a top priority among some organizations, both practical experience and a detailed market overview suggest that it is becoming a critical capability.

This guide explained what threat intelligence is, provided tips on what to look for when choosing a TI provider, dove into the TI market and how organizations consume this service, and introduced ESET's solution. All of this together is motivated by the fact that being ahead of adversaries always requires well-informed expert knowledge that can be trusted.

Those who realize the potential of TI often consume it from more than fifty vendors. That does not necessarily have

to be the best choice as the quality of data and information rank higher than the quantity itself. There is an extensive amount of data that could be gathered and relying on that with no real curation and no integration with your systems can hardly improve your resilience and posture.

That is where ESET might be of help as it provides the complex capabilities of cyber threat intelligence that is based on technology, knowledge, human expertise, and a tailored approach. The service provides curated, relevant, reliable, and frequently updated data that come with MISP integration so that you can investigate incidents as well as test hypotheses and improve threat-hunting capabilities.



ESET has complex cyber threat intelligence capabilities that are based on technology, knowledge, human expertise, and a tailored approach.

We advocate that the only viable approach to effectively protect your organization's data is to have multiple layers of protection in place.

About ESET

When technology enables **progress**, ESET is here to **protect it**.

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.



protected by ESET since 2016
more than 32,000 endpoints



ISP security partner since 2008
2 million customer base



protected by ESET since 2016
more than 4,000 mailboxes



**MITSUBISHI
MOTORS**

Drive your Ambition

protected by ESET since 2017
more than 9,000 endpoints

30+

years of expertise

1bn+

internet users protected

400k+

business customers

195

countries & territories

13

global R&D centers



30+ years of continuous innovation



Leading European Union vendor



Always focused on technology



Growing YoY since its inception