Prevention first:

Leveraging Cyber Threat Intelligence for Proactive Defense

Digital Security
Progress. Protected.

Table of Contents

Why Prevention Truly Matters

There is no doubt that cyber threat prevention is paramount. With organizations becoming increasingly dependent on digital operations, the risk of cyber threats grows accordingly. Everyone should be aware of that. But are they?

In the last few years, we've seen some wake-up calls showing us how important actionable preventive measures are in cybersecurity. Such cases can shed light on why skimping on prevention is a risky move. We're talking major **hits to the wallet**, a **tarnished reputation** that can take years to rebuild, and even **legal repercussions** that hardly anyone wants to deal with. These are the big-ticket consequences that cyber threats can bring to the table when ignoring proactive prevention.

> **"When preventive technologies are undermined, quick detection and response is the only thing standing between you and a costly and likely very public data breach."**

Source: *Forrester: The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q3 2023.*

H. Mullins and Team. July 21, 2023.

By prioritizing a prevention-first approach, organizations can safeguard their systems and data, and therefore reduce the risk of being compromised. Even if an attack occurs, proactive prevention minimizes the time that security teams have to spend on incident response and remediation. This not only ensures the continuity of organizations' operations but also builds trust with their stakeholders.

Even though a prevention-first approach is crucial for businesses of all sizes, there are certain **aspects** that are **particularly important** for **large organizations** and enterprises.

Breaches at organizations with Threat Intelligence in place had an average cost that was

$197 thousand less

than the 2023 mean cost of a data breach of $4.45 million.

Source: *IBM, Cost of a Data Breach Report 2023*.

These aspects include:

SCALE OF OPERATIONS

Enterprises typically have a large scale of operations. They are complex and intricate. This means that they have more data and systems to protect, making them a bigger target for cybercriminals and increasing the potential impact of cyber-attacks.

REGULATORY COMPLIANCE

Many organizations and enterprises operate in sectors that are subject to strict regulatory requirements for data protection. Failure to prevent cyber-attacks can lead to noncompliance, resulting in hefty fines and legal consequences. The golden rule here is: It is **better to invest in prevention** than spend on restoration.

$243 thousand

was the mitigated average data breach costs with Threat Intelligence in place in 2024.

Source: *IBM, Cost of a Data Breach Report 2024*.

COMPLEX INFRASTRUCTURE AND INTEGRATION REQUIREMENTS

Enterprises often have more complex IT infrastructures, including multiple networks, applications, and systems. Managing cybersecurity across these vectors can be challenging and it requires sophisticated threat intelligence solutions that are put to good use across the entire protection stack. Ideally, advanced **CTI encompasses** both reliable **technology** and **human expertise.**

$4.45 million

was the average cost of a data breach in 2023.

Source: *IBM, Cost of a Data Breach Report 2023*.

REPUTATION

Many such organizations have substantial clientele and a recognized reputation. A cyber-attack can inflict considerable harm on their overall image, erode stakeholder confidence, and negatively impact their standing in the market or community. This might seem trivial at first glance, but the reality may be much more dramatic after such harm happens.

One **effective way to adopt a prevention-first approach** that mitigates such potential harm is through the use of **cyber threat intelligence solutions**. These solutions provide real-time insights into potential threats, enabling organizations to identify and mitigate risks before they cause harm and, therefore, stay one step ahead of cybercriminals.

This paper gives a firsthand look at the challenges of prevention and how closely prevention is intertwined with cyber threat intelligence. If you are uncertain or feeling lost in how to approach this issue, then you will find in this paper an explanation of the possible pain points that you might have with implementing preventive measures and adopting cyber threat intelligence.

What Can You Actually Struggle with?

ADVANCED (ZERO-DAY) THREATS

As is commonly known, a zero-day threat refers to **malicious code** that is used by attackers before a patch or fix is available. These vulnerabilities are "zero-day" because there are zero days between the discovery of the flaw and the availability of a patch.

Such threats can bypass traditional security measures. The direct and quite nasty impacts of this are that organizations face the risk of **undetected attacks**, **data breaches**, and **subsequent financial losses**.

One of the best solutions to this problem is the adoption of cyber threat intelligence that helps identify and mitigate zero-day threats by providing reliable and actionable information on emerging vulnerabilities and the most commonly seen attack techniques, such as obfuscation of files or information, accessing credentials from password stores, phishing, and exfiltration over command and control channels.

TALENT SHORTAGE

The cybersecurity industry faces a shortage of skilled professionals. Organizations struggle to find and retain experts in threat intelligence and analysis, profoundly impacting their defensive capabilities to address gaps in threat detection and response.

These gaps might include minimal monitoring by organizations that are not capable of maintaining 24/7 surveillance, poor analysis of alerts, logs, and other IoCs, or a slow incident response that could otherwise better mitigate any damage. **Investing in training**, **automation**, and collaboration with **external threat intelligence providers** can alleviate the talent shortage and, therefore, allow you to be more resilient.

COMPLEXITY OF USED TOOLS

Organizations often use multiple security tools, each with their own interface, data format, and configuration. Integrating these tools can be a quite complex and tricky task and can consume a lot of time. The possible negative impacts include **decreased efficiency**, **misconfigurations**, and **slowed incident response**.

Speaking about managing diverse tools, security teams often need to switch between multiple interfaces, leading to wasted time and causing potential errors. The challenge for integration is complexity, which increases the risk of misconfiguration, such as incorrect data mappings or missed updates. This is also a challenge for smooth information flow, and when tools don't seamlessly exchange information, incident response times unnecessarily increase.

Adopting unified threat intelligence platforms that streamline and automate data aggregation, normalization, and sharing across tools is a first step to addressing these problems. Such platforms serve as a central hub for intel and, therefore, significantly reduce complexity. The use of **standardized formats** like JSON and STIX via TAXII is also highly important because it ensures compatibility and ease of implementation.

Last but not least, **automation** empowers security teams and helps them take advantage of current threat intelligence to better protect networks. Automated orchestration of data flows between tools minimizes manual intervention and can reduce human error.

COMPLIANCE GAPS AND LACK OF PRACTICAL KNOWLEDGE

Less mature organizations can struggle to translate threat intelligence into actionable steps. There might be a gap between theoretical knowledge and practical application, or compliance requirements may not align with security practices. These tend to result in an **ineffective implementation** of threat intelligence, **noncompliance with the regulations**, or even missed opportunities.

Ineffective implementation is when organizations collect threat data but fail to operationalize it effectively. Being noncompliant with the regulations means your organization is failing to align with current threat intel practices and standards which—as mentioned above—can have legal consequences. However, there is also the aspect of

By deploying AI extensively across prevention workflows, organizations averaged

$2.2 million less

in breach costs compared to those with no AI use in prevention workflows.

Source: *IBM, Cost of a Data Breach Report 2024*.

missed opportunities that mainly deals with how the lack of practical knowledge prevents organizations from fully leveraging threat intelligence for proactive and preventive defense strategies.

What can you do about it? **Educate security teams** on practical threat intelligence usage, **align compliance efforts with security goals**, and prioritize actionable insights. Regularly train security teams on practical threat intelligence usage and bridge the gap between theory and hands-on application.

Provide threat intelligence in a context that aligns with specific compliance requirements and highlights actionable insights. Finally, prioritize threat intelligence efforts based on risk assessments and compliance needs.

What is Cyber Threat Intelligence?

Cyber threat intelligence informs your thinking and actions. You are not just passively waiting for and making guesses about the threats that you are facing, but rather **actively anticipating real threats** and seeking opportunities to create stronger defenses against them. This helps build your short- to long-term plans, ensures stability and preparedness, builds resilience, and enables progress.

In cybersecurity, such an approach shifts the threat protection paradigm and shapes the decision-making process. Active utilization of cyber threat intelligence is a practical method of dealing with cyber threats, allowing organizations to establish and support the right course of action and, therefore, let the business thrive.

Cyber threat intelligence is about **gathering**, **analyzing**, and **contextualizing information** about potential and ongoing threats to an organization's information technology systems. More than anything else, it is this proactive approach that enables organizations to identify, assess, and mitigate the risks posed by cyber threats.

> **Threat intelligence has evolved significantly over the past decade, allowing organizations to proactively identify and mitigate cyberthreats. In addition to this, by leveraging threat intelligence data, they can better understand their risk profile and develop comprehensive security strategies that protect against malicious actors.**

Source: *IDC: The Strategic, Operational, and Tactical Dimensions of Threat Intelligence: A Vendor Perspective*, Doc # US51451823, December 29, 2023, M. Soltysik and Ch. Kissel.

Such an intelligence capability can be obtained from various sources, such as open-source intelligence, commercial intelligence services, government intelligence agencies, and in-house threat intelligence teams. If cyber threat intelligence—a prevention-first approach in its very essence—is to be done correctly, it must be based on comprehensive knowledge. This basically means that organizations should rely on **the combination** of reliable **technology** that is right for your organization and **professional human intelligence** capacities.

When designed and conducted professionally, such capability not only provides proactive prevention but also reduces complexity. This is becoming more than just a nice to have thing. With the rising complexity of the threat landscape, it is a highly recommended must.

Cyber threat intelligence can help you with:

- Taking proactive measures to prevent or mitigate cyber-attacks.
- Prioritizing where to focus limited resources when trying to mitigate the biggest risks.
- Triaging events and reducing the damage from potential attacks.
- Minimizing the overall negative impact once you are attacked.
- Responding effectively to security incidents.

Practically speaking, there are many real-time situations where this capability can be helpful. Cyber threat intelligence is highly useful for **keeping track of IPs** associated with malicious infrastructure, the most commonly seen **TTPs**, **compromised credentials**, or **web injects** inserting HTML or JavaScript.

Gathering, **contextualization**, **interpretation**, and **targeted actions** – these four are the best outcomes an organization can benefit from when using cyber threat intelligence.

ESET Threat Intelligence and Its Key Benefits

ESET Threat Intelligence (**ETI**) is defined by its preventive approach to cybersecurity, aiming to provide quick reaction capabilities, better preparedness, and proactive measures against various kinds of cyber threats.

> **"As for our threat intelligence sources, the quality of ESET's threat intelligence is among the top two, if not the number one."**

A government organization, October 2023.

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

HIGHLY CURATED AND ACTIONABLE

- Low false positives
- Quality over quantity
- In human-readable format

UNIQUE GEOGRAPHICAL COVERAGE

- Coverage from ESET's own telemetry
- Unique range of sources
- Unparallel in-the-field experience

TRUSTED THREAT INTELLIGENCE PARTNER

- 30+ years in the industry
- Based in Europe
- Privately owned

> **ESET's visibility into a unique set of data is what makes them attractive in the CTI world.**

A defense organization, August 2023.

Some other benefits are:

HUMAN EXPERTISE

Even though sophisticated, custom systems are used to gather and process cyber threat data, human expertise remains crucial. The reason is that **contextualization** and **interpretation** are **still best done by humans**. Threat intel analysts also oversee the processes and explore and suggest improvements.

UNDERSTANDING RISKS

Understanding means predicting threats, mitigating incidents, and reducing exposure to prevailing threats.

IMPROVING THREAT HUNTING AND REMEDIATION

Proactively searching for cyber threats that may have evaded initial security defenses along with the eradication of persistent threats, thereby enhancing your security posture.

SPOTTING POTENTIAL COMPROMISES

This enables you to spot potential compromises by **using YARA rules to scan systems** and checking networks.

MONITORING APT GROUPS

This allows you to gain a profound **understanding of APT groups**' tactics, methods, or even motives. Knowing this can give you an advantage.

SAVING RESOURCES

Low maintenance requirements thanks to curated content, thereby enabling you to save valuable resources.

AGILITY

This enables you to make faster, more useful, and better decisions over the short- and long-term periods. In the former case, it can offer **highly relevant IoCs** in a timely fashion. In the latter case, it can **buttress your intelligence** and cybersecurity strategy.

ETI is a **comprehensive offering** consisting of many tools that provide value to ensure a high level of cyber protection. ETI can be consumed as a complex service, providing insights thanks to **data feeds**, **APT reports**, **ESET AI Advisor**, and direct **access to analysts** with comprehensive knowledge of threats.

ESET Threat Intelligence Data Feeds

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

There are six well-known ETI feeds; together, these provide a holistic picture and enable your organization to quickly block IoCs. These are the **Malicious Files Feed**, **APT Feed**, **Domain Feed**, **URL Feed**, **IP Feed**, and **Botnet Feed**. You can learn more about them in our buyer's guide on cyber threat intelligence.

Nine new feeds enhance ESET's original intel capabilities even more. Each one of these feeds is created in near real time, and deduplication happens every 24 hours.

SMS SCAM FEED

You can think of an SMS scam as a fraudulent text message. This feed contains targeted information about the current and prevalent SMS scam domains, URLs, and associated data. The feed is created from all ESET domain and URL sources.

SMISHING FEED

The Smishing Feed works exactly the same as the SMS Scam Feed except that the fraudulent activity utilizes smishing – a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information, or sending money to cybercriminals.

The feed can be used for unique threat intelligence, targeted incident response, further research, employee awareness, and system protection.

CRYPTOSCAM FEED

Crypto scams refer to any fraudulent practice in the cryptocurrency realm aimed at tricking individuals into bad investments or giving away assets or sensitive information.

You can imagine this feed as a subset of scam domains and URLs that contain targeted information about the current and prevalent crypto scam domains, URLs, and associated data. The feed is created from all ESET domain and URL sources.

→ PHISHING URL FEED

Phishing URLs direct recipients to fake websites and attempt to entice them into divulging sensitive data such as login credentials or financial information. The website usually looks deceptively familiar and legit, but it misuses your trust by "fishing" for personal information.

The Phishing URL feed collects raw data from multiple sources. Organizations can integrate this feed into their security solutions, including XDR/EDR, SIEM, SOAR, and firewalls to proactively defend against cyber threats.

SCAM URL FEED

Scam URLs pose a serious threat that is particularly prone to be effective due to human error. Such URLs look real and trustworthy but are actually malicious. This feed covers fraudulent electronic shops, investment scams, dating scams, and it also helps you detect scam URLs at the network level.

Users can integrate it with their network security controls or other analytical tools, such as TIPs, SIEM systems, and SOAR solutions to protect employees from scams.

"ESET's intelligence focuses on part of the world where many recent ransomware attacks emanate from and has been proven to be both operationally timely and uniquely identifying these threats."

Jess Parnell, VP of Security Operations Centripetal, October 2023.

→ MALICIOUS EMAIL ATTACHMENT FEED

The primary purpose of this feed is to protect users and organizations from potential threats posed by email attachments. Malicious email attachments are files sent via email with the intent to compromise or damage the recipient's computer system or exfiltrate sensitive information.

These harmful payloads often masquerade as seemingly innocuous items, such as documents, PDFs, images, or audio files. When unsuspecting users open these attachments, they inadvertently

➜ unleash malware, such as ransomware, spyware, and trojans. The attachments often mimic legitimate communications from reputable sources, increasing the likelihood of users opening them.

The feed is updated daily to keep pace with emerging threats and is created from ESET telemetry sources focused on email scanning (on both the client and server sides) in near real time. Users can access this information via TAXII and STIX, and through various security tools.

RANSOMWARE MALICIOUS FILES FEED

This feed provides real-time information on currently prevalent ransomware samples as well as on their characteristics and IoCs. The feed helps you understand which ransomware families are being seen in the wild and enables you to proactively block them before they can cause any harm.

It includes hashes of ransomware samples and associated data. The feed is updated in real time and it is filtered so that you only obtain relevant data with low redundancy.

ANDROID THREATS FEED

An Android threat refers to any malware or malicious activity targeting Android devices, including smartphones, tablets, and other devices running the Android OS. These threats are designed to exploit vulnerabilities, steal personal information, spy on user activities, display unwanted ads, or even lock the device for ransom. By utilizing the Android threats feed, you can stay informed about these evolving dangers and protect your devices from potential attacks.

The feed provides real-time information on currently prevalent Android threats as well as on their characteristics and IoCs. The feed helps you understand which Android threats are being seen in the wild and enables you to proactively block them before they can cause any harm.

ANDROID INFOSTEALER FEED

This feed contains targeted information about current and prevalent Android infostealer samples and associated data. Infostealers often target banking information on Android devices and once they are installed, they can compromise the security and privacy of individuals and organizations, leading to identity theft, financial loss, and other severe consequences.

The data that this feed provides helps you understand which Android infostealer families are being seen in the wild and enables you to proactively block them.

Integrations

Integrations are vital for enhancing organizational cybersecurity. By connecting our threat intelligence data with platforms like Elastic, Microsoft Sentinel, OpenCTI, and ThreatQuotient, ESET enables easy access to critical information. Such integrations **optimize threat detection and response**, providing **real-time data feeds** to help organizations stay ahead of cyber threats, while also supporting a **prevention-first approach**.

ESET ensures compatibility through using standards like TAXII 2.1 and STIX 2.1, which make our threat intelligence data easily consumable across various SIEM and SOAR platforms. This approach provides organizations with curated, accurate data in common formats so that organizations can enhance their security measures with minimal effort and maximum efficiency.

ELASTIC SIEM

Elastic users can benefit from ESET Threat Intelligence feeds to monitor botnets, malicious domains, files, URLs, and IPs, which reveal hidden cybercriminal activities and APT operations. This integration enhances Elastic's SIEM product, providing security operators with global threat data, reduced false positives, and valuable context. Customers gain real-time data from ESET feeds, comprehensive coverage of threats, and highly curated information based on ESET's proprietary research, delivered through native Elastic integration.

MICROSOFT SENTINEL

ESET's integration with Microsoft Sentinel enhances threat detection and response by combining ESET's threat intelligence data feeds with Sentinel's SIEM and SOAR capabilities. SOC analysts can leverage Sentinel's TAXII client to access curated data on APTs, malicious files, botnets, domains, URLs, and IPs. This collaboration aims to improve threat detection and response times, and is supported by ESET's reputable research, contributions to MITRE ATT&CK, and cooperation with CISA, EUROPOL, and the FBI.

OpenCTI

OpenCTI offers a collaborative platform for analyzing, enriching, and sharing threat data. Integrating ESET Threat Intelligence enhances threat insights and detection. The integration can use either ESET's native OpenCTI Connector or the OpenCTI TAXII2 Connector to ingest ESET data feeds, automating the import of STIX 2 Bundles without conversion. Even if you do not use our native connector or plugin to the platform, the integration is surprisingly easy.

OpenCTI's CSV Feeds allow for the automatic generation of a CSV file, which is updated at user-defined intervals, making it easy to integrate with systems that can ingest CSV files. The platform's TAXII Collections are implemented as part of a TAXII 2.1 server, enabling the creation of as many TAXII Collections as needed, which is particularly useful for integrating with modern cybersecurity systems. Lastly, OpenCTI's Live Streams feature enhances real-time data sharing by serving STIX 2.1 Bundles as TAXII Collections with advanced capabilities, providing richer context for the shared data.

THREATQUOTIENT

Integrating ThreatQuotient with ESET Threat Intelligence enhances threat detection and response. After logging into the ThreatQ Marketplace, you can download the integration file and configure API keys in your ThreatQ instance. The integration uses the ESET Threat Intelligence TAXII service to access specific feeds, including Botnet, Domain, Malicious Files, and URL feeds. These feeds provide STIX Bundles containing indicators, malware, identities, and relationships.

APT Reports

ESET's **Advanced Persistent Threat** (**APT**) Reports represent a reliable source of cyber threat intelligence that covers APT groups and their activities. The reports provide strategic, tactical, technical, and operational intelligence.

They help organizations with **threat hunting** as well as **investigating** and **mitigating active incidents** and, therefore, assist organizations to become proactive and predictive instead of reactive. 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.

> **"ESET offers a unique perspective on threat actors' activity, and provides a technical and profound analysis of malware, infrastructure and TTPs. ESET's team has become a critical component in our ability to cope with the various threat actors operating in our region, and we are grateful for the collaboration with them."**

An intelligence agency, September 2023.

One highly convenient practice for organizations is to consolidate all of the data from the reports into their threat intelligence platform. ESET offers access to its internal MISP (Malware Information Sharing Platform) server, which comes pre-filled with all the relevant and valuable data. Therefore, customers can easily synchronize it with their systems.

The APT reports offer contextual information and other relevant details. These reports come as a package with several types of outputs: **Activity Summary reports**, **Technical Analysis reports**, **Monthly Overview reports**, **Monthly Digest reports**, **APT Data Feeds**, access to the MISP server, and access to threat intel analysts.

ESET AI Advisor

ESET AI Advisor is the perfect addition to the security analyst's toolkit, offering a smooth and intuitive experience that melds effortlessly with daily workflows. Drawing from ESET's rich twenty-year history in **pioneering AI-powered endpoint protection**, this tool not only delivers **granular incident insights** but also provides **strategic guidance** tailored to SOC teams. It stands as a transformative asset for businesses, especially those with constrained IT capabilities, eager to harness the power of insightful threat intelligence.

> **"The ESET AI Advisor module represents a significant leap forward in our mission to close the cybersecurity skills gap and empower organizations to safeguard their digital assets effectively."**

Juraj Malcho, ESET Chief Technology Officer.

Whether your organization is equipped with less experienced security professionals or you've been in the game for a while supported by skilled and reliable expert personnel, ESET AI Advisor is your go-to for a **hassle-free way to spot**, **analyze**, and **tackle security risks**. It's all laid out in a way that's a breeze to get so that you can jump right into action.

The interface is user-friendly, turning complex threat information into something that you can actually **use immediately** regardless of your experience level.

Organizations with extensive use of security AI identified and contained a data breach

108

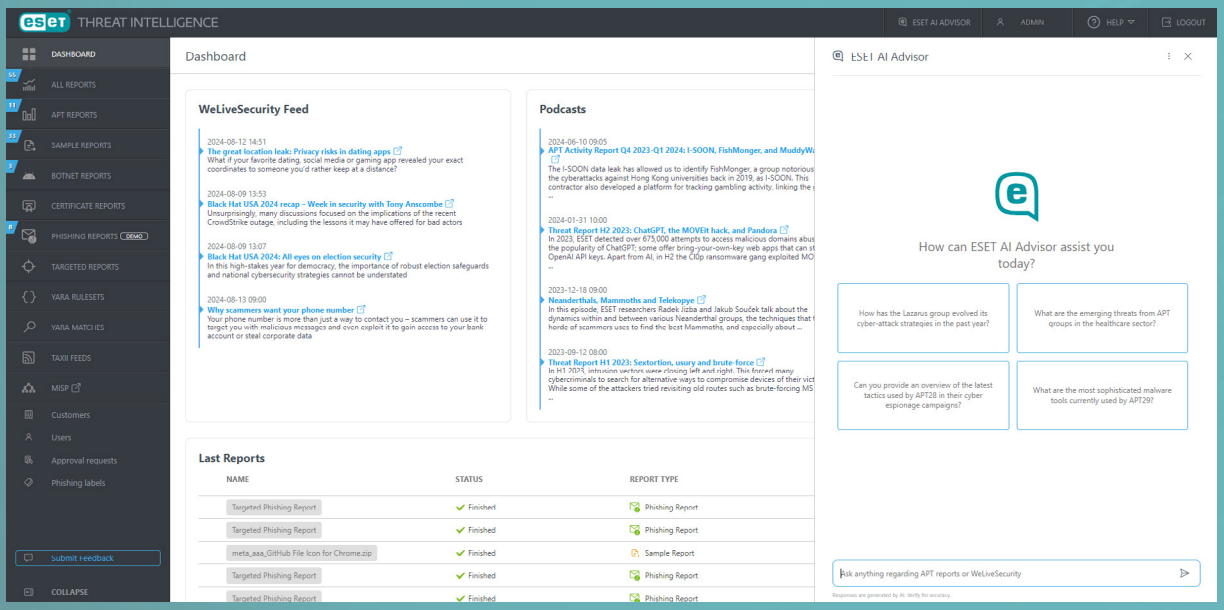
days faster

than organizations with no use of AI.

Source: *IBM, Cost of a Data Breach Report 2023*.

ESET AI Advisor plays a crucial role in expediting decision-making during critical incidents. Security analysts can effortlessly consult ESET AI Advisor to gain insights into the specific threats within their environment.

ESET AI Advisor is available in the ESET Threat Intelligence console along with the APT Reports.



Picture 1: *Integration of ESET AI Advisor in the ESET Threat Intelligence console.*

Conclusion

Leveraging cyber threat intelligence (CTI) is essential for effective prevention in the current cybersecurity landscape. It is better for organizations of all sizes to **prioritize preventive measures** because this saves resources, protects business continuity, and keeps the business free of potential legal repercussions due to noncompliance.

Adversaries, along with their tools and practices, are simply too sophisticated to stay reactive nowadays. Organizations might face significant challenges in adopting preventive measures, including resource constraints and the complexity of integrating CTI. Our experts contend that **understanding CTI** together with knowing what

valuable data it provides—and how it can be utilized in prevention—is one of the key steps for overcoming these obstacles and becoming resilient.

ESET offers advanced threat intelligence capabilities that are based on **robust data feeds** and **detailed reports** that are accompanied by **ESET AI Advisor**, which assists with processing and evaluating vast amounts of data. Seamless integrations are part of the service as well. Even though there is no single miracle solution to adopting a preventive approach in cybersecurity, the comprehensiveness of CTI supported by other defense measures can reliably skyrocket organizations' operational resilience.

Explore your use case for ETI and gain access to ESET APT reports, ETI data feeds, and a comprehensive toolset for an ESET-powered prevention-first approach.

LEARN MORE

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

LEARN MORE

eset
Digital Security
Progress. Protected.