Unique intelligence feeds and APT reports from the industry's top professionals
OVERCOME INFORMATION OVERLOAD
Ransomware, zero-days, advanced persistent threats, targeted attacks and botnets are all concerns for businesses around the world. The problem is that, due to the volume of different threats, organizations are unable to easily understand which proactive defenses and mitigations are the most important.

This ultimately leads to organizations scrambling to try and find meaningful information among limited data sets, such as their own networks, or the extremely large datasets that they find via external sources. Threat intelligence services help sift through the information overload and provide the most relevant information for specific organizations.

Threat intelligence services allow organizations to prioritize emerging threats quickly and easily, which leaves them more time to proactively implement new defenses against them.

FIGHT THREATS PROACTIVELY
Today’s cybersecurity landscape is constantly evolving with new attack methods and never before seen threats. When an attack or data breach occurs, organizations are typically surprised that their defenses were compromised, or are completely unaware that the attack even happened. After the attack is finally discovered, organizations rush to reactively implement mitigations to stop the attack from being repeated. However, this does not protect them from the next attack that might use a brand new vector.

Threat intelligence services provide insight on future business risks and unknown threats, which allows organizations to improve the effectiveness of their defenses and implement a proactive cybersecurity posture.

Stop information overload and get data relevant to your organization

Why threat intelligence?

By providing information on the threat actor, attack vectors and indicators of compromise, security teams can reduce incident response time by getting the full picture of the attack and what to look for.

ACCELERATE INCIDENT RESPONSE
When a data breach occurs, security teams typically need to figure out how the incident happened, as well as identify which devices were affected. This process is usually a very long and manual process as engineers sift through their network searching for abnormalities which might indicate that the network was compromised.

Threat intelligence services allow incident response teams to fully understand and quickly respond to data breaches. By providing information on the threat actor, attack vectors and indicators of compromise, security teams can reduce incident response time by understanding the full picture of the attack as well as what to look for.

ACCELERATE INCIDENT RESPONSE

Why threat intelligence?

By providing information on the threat actor, attack vectors and indicators of compromise, security teams can reduce incident response time by getting the full picture of the attack and what to look for.

ACCELERATE INCIDENT RESPONSE

When a data breach occurs, security teams typically need to figure out how the incident happened, as well as identify which devices were affected. This process is usually a very long and manual process as engineers sift through their network searching for abnormalities which might indicate that the network was compromised.

Threat intelligence services allow incident response teams to fully understand and quickly respond to data breaches. By providing information on the threat actor, attack vectors and indicators of compromise, security teams can reduce incident response time by understanding the full picture of the attack as well as what to look for.

ACCELERATE INCIDENT RESPONSE

Why threat intelligence?

By providing information on the threat actor, attack vectors and indicators of compromise, security teams can reduce incident response time by getting the full picture of the attack and what to look for.
The ESET advantage

Human expertise backed by machine learning. Our reputation system, LiveGrid® is made up of 110 million sensors worldwide, and verified by our R&D centers.

1 HUMAN EXPERTISE BACKED BY MACHINE LEARNING

The use of machine learning to automate decisions and evaluate possible threats is a vital part of our approach. But it is only as strong as the people who stand behind the system. Human expertise is paramount in providing the most accurate threat intelligence possible, because threat actors can be intelligent opponents.

2 STRONG REPUTATION SYSTEM — LIVEGRID®

ESET Endpoint products contain a cloud reputation system which feeds relevant information about the most recent threats and benign files. Our reputation system, LiveGrid® is made up of 110 million sensors worldwide, the output of which is verified by our R&D centers. This gives customers the highest level of confidence when viewing information and reports within their console.

3 EU ORIGINS, WORLDWIDE PRESENCE

Based in the European Union, ESET has been in the security industry for over 30 years, has 22 offices worldwide, 13 R&D facilities and a presence in over 200 countries and territories. This helps to provide our customers with a global perspective on all the most recent trends and threats.

The ESET advantage

GET UNIQUE INSIGHTS

ESET gathers threat intelligence from a unique range of sources and has unparalleled in-the-field experience that helps you fight increasingly sophisticated cybersecurity attacks.

MAKE CRUCIAL DECISIONS, FASTER

Anticipate threats and make faster, better decisions thanks to comprehensive ESET reports and curated feeds. Reduce your exposure to prevailing threats, forecasted by experts.

AUTOMATE THREAT INVESTIGATION

ESET technology searches for threats constantly, across multiple layers, from pre-boot to resting state. Benefit from telemetry on all countries where ESET detects emerging threats.

STAY AHEAD OF ADVERSARIES

ESET follows the money, specifically monitoring those places where we have detected APT groups that target tax-exempt companies: Russia, China, North Korea, Iran. You’ll know about new threats first.

IMPROVE YOUR SECURITY POSTURE

Informed by ESET intelligence feeds, enhance your threat hunting and remediation capabilities. Block APTs and ransomware, and improve your cybersecurity architecture.
Advanced Persistent Threat (APT) Reports

PUTTING OUR BEST RESEARCH AT YOUR FINGERTIPS

Our research team is well known in the digital security industry, thanks to our award-winning We Live Security blog. The team's excellent research and APT activity summaries are available, along with much more detailed information. ESET customers get an exclusive early preview of all We Live Security content.

MAKE CRUCIAL DECISIONS FAST

All this helps organizations make crucial decisions and provides a strategic advantage in the fight against digital crime. It brings an understanding of what is happening on the 'bad side of the internet' and provides crucial context, so that your organization can make internal preparations quickly.

ACTIONABLE, CURATED CONTENT

Reports provide a great deal of context for what is going on and why. Thanks to this, organizations can prepare in advance for what might be coming. Importantly, our experts make sure the content is easy to understand.

ACCESS TO ESET ANALYST

Every customer ordering the APT Reports PREMIUM package will also have access to an ESET analyst for up to four hours each month. This provides the opportunity to discuss topics in greater detail and help resolve any outstanding issues.

IN-DEPTH ANALYSIS

The package includes monthly in-depth technical analysis reports describing recent campaigns, new tricks, and related subjects. You'll also get an activity summary report every two weeks that describes the latest APT campaigns ESET researchers have been tracking from various threat actors, as well as their targets and, of course, the associated Indicators of Compromise (IoCs). A monthly overview combines information from all Technical Analysis and Activity Summary reports released in the previous month into a shorter and more digestible form.

WITH APT REPORTS, YOU GET

| Access to private, in-depth technical analysis | APT activity summary reports | A monthly summary for your C-level executives | Direct access to an ESET Cybersecurity professional | Access to our MISP server |

Availability of ESET Threat Intelligence reports and feeds vary by country. Please contact local ESET representative for more information.
Integrate ESET Threat Intelligence into your system

Integrating ESET telemetry is simple and will enrich your **TIP, SIEM**, or **SOAR**

We have a comprehensive API with full documentation

We supply data in standardized formats - such as JSON and STIX feeds via TAXII – so that integration into any tool is possible.

For IBM QRadar, Anomali, and Logpoint we have step-by-step integration manuals for fast and easy implementation – and we’re continually adding others.
Enrich your view of the worldwide threat landscape based on unique telemetry. ESET feeds come from our research centers around the globe, providing a holistic picture and enabling you to quickly block IoCs in your environment. Feeds are in the formats: • JSON • STIX 2.0

**ESET proprietary intelligence feeds**

**MALICIOUS FILES FEED**
Understand which malicious files are being seen in the wild. The feed features domains which are considered malicious, including domain name, IP address, detection of file handled from URL, and detection of the file which was trying to access the URL. This feed consists of shared hashes of malicious executable files and associated data.

**DOMAIN FEED**
Block domains which are considered malicious. The feed includes domain names, IP addresses, and the dates associated with them. The feed ranks domains based on their severity, which lets you adjust your response accordingly. For example, to only block high severity domains.

**IP FEED**
This feed shares IPs considered to be malicious and the data associated with them. The structure of the data is very similar to that used for the Domain and URL feeds. The main use-case here is to understand which malicious IPs are currently prevalent in the wild, block those IPs which are of high severity, spot those that are less severe, and investigate further based on additional data, to see if they have already caused harm.

**URL FEED**
Similar to Domain Feed, the URL Feed looks at specific addresses. It includes detailed information on data related to the URL, as well as information about the domains and IP associated with them. The information is filtered to show only high confidence results and includes easy to understand information on why the URL was flagged.

**BOTNET FEED**
Based on ESET’s proprietary botnet tracker network. Botnet feed features three types of sub-feeds—botnet, C&C and targets. Data provided includes items such as detection, hash, last alive, files downloaded, IP addresses, protocols, targets, and other information.

**APT FEED**
This feed consists of APT information produced by ESET research. In general, the feed is an export from the ESET internal MISP server. All the data that is shared is also explained in greater detail in APT reports. The APT Feed is also part of APT reports offering, but the feed can also be purchased separately.
About ESET

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.

ESET IN NUMBERS

- 1bn+ internet users protected
- 400k+ business customers
- 200+ countries & territories
- 13 global R&D centers

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.

About ESET

SOME OF OUR CUSTOMERS

- Canon: protecting by ESET since 2007, more than 32,000 endpoints
- MITTISHI MOTORS: protecting by ESET since 2007, more than 6,000 endpoints
- Allianz Suisse: protecting by ESET since 2006, 2 million customer base
- T-Systems: IT security partner since 2006

SOME OF OUR TOP AWARDS

ISO SECURITY CERTIFIED

ESET is ISO/IEC 27001:2013 certified, an internationally recognized and applicable security standard in implementing and managing information security. The certification is granted by the third-party accredited certification body SGS and demonstrates ESET’s full compliance with industry leading best practices.

Why choose ESET?

INDUSTRY RECOGNITION

- Recognized as Established Vendor in 2021 Gartner® Peer Insights™ ‘Voice of the Customer’ EPP Report
- ISO SECURITY CERTIFIED

ISO SECURITY CERTIFIED

ESET is ISO/IEC 27001:2013 certified, an internationally recognized and applicable security standard in implementing and managing information security. The certification is granted by the third-party accredited certification body SGS and demonstrates ESET’s full compliance with industry leading best practices.

SOME OF OUR TOP AWARDS

- Canon: giving back to the community with a 2021 Tech Cares Award from TrustRadius
- MITTISHI MOTORS: recognized for industry leading best practices
- ESET recognized for industry leading best practices
Why choose ESET?

**ANALYST RECOGNITION**

ESET has been recognized as a Major Player in endpoint security in the IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2021 and and IDC MarketScape Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment.

**IDC**

ESET has been recognized as a "Top Player" for the fourth year in a row in Radicati's Advanced Persistent Threat (APT) Protection - Market Quadrant 2021.

**Radicati Group Inc.**

The rigorous MITRE ATT&CK Evaluation demonstrated the undeniable qualities of ESET EDR technology and validated the strong vision for ESET Inspect’s future.

**MITRE ATT&CK.**

"The implementation was very straightforward. In cooperation with ESET’s well-trained technical staff, we were up and running our new ESET security solution in a few hours."

IT Manager, Ol Milton’s Motors LLC, Greece, 6,000+ seats

"We were most impressed with the support and assistance we received. In addition to being a great product, the excellent care and support we got was what really led us to move all of Primoris’ systems to ESET as a whole."

Joshua Collins, Data Center Operations Manager, Primoris Services Corporation, USA, 4,000+ seats

"Why choose ESET?"

The implementation was very straightforward. In cooperation with ESET’s well-trained technical staff, we were up and running our new ESET security solution in a few hours.

IT Manager, Ol Milton’s Motors LLC, Greece, 6,000+ seats

We were most impressed with the support and assistance we received. In addition to being a great product, the excellent care and support we got was what really led us to move all of Primoris’ systems to ESET as a whole.

Joshua Collins, Data Center Operations Manager, Primoris Services Corporation, USA, 4,000+ seats