OVERVIEW

THREAT INTELLIGENCE

Unique intelligence feeds and APT reports
from the industry's top professionals

Progress. Protected.

Get a unique perspective on the threat landscape

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.

STAY AHEAD OF ADVERSARIES

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

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, forewarned by experts.

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.

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.

The ESET advantage

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

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.

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 centres. This gives customers the highest level of confidence when viewing information and reports within their console.

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.

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.

ACTIONABLE, CURATED CONTENT

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

MAKE CRUCIAL DECISIONS FAST

All this helps organisations 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 organisation can make internal preparations quickly.

ACCESS TO AN ESET ANALYST

Every customer ordering the APT Reports Premium package will have also 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.

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

IN-DEPTH ANALYSIS

The package includes monthly in-depth technical analysis reports describing recent campaigns, new toolsets 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.

Availability of ESET Threat Intelligence reports and feeds varies by country. Please contact your local ESET representative for more information.

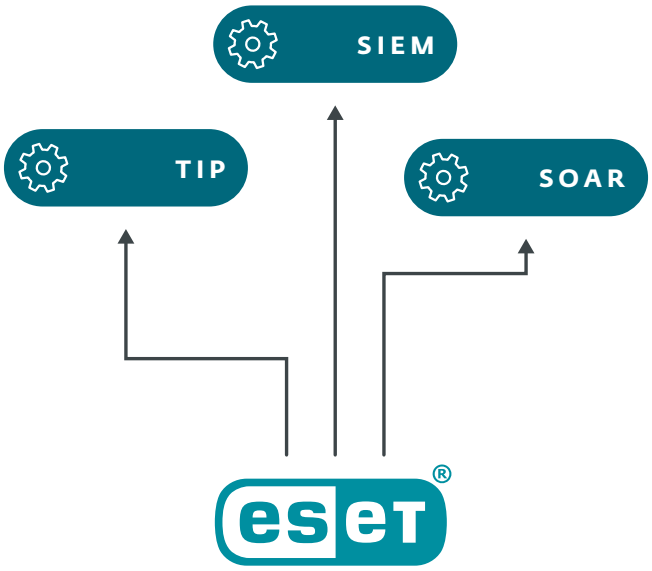
Integrate ESET Threat Intelligence into your system

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 **standardised formats** - such as JSON and STIX feeds via TAXII – so that integration into any tool is possible

For IBM QRadar, Anomali, ThreatQuotient, and Logpoint we have **step-by-step integration manuals** for fast and easy implementation – and we're continually adding others



How does our threat intelligence come to life? **ESET Threat Inteligence lifecycle**

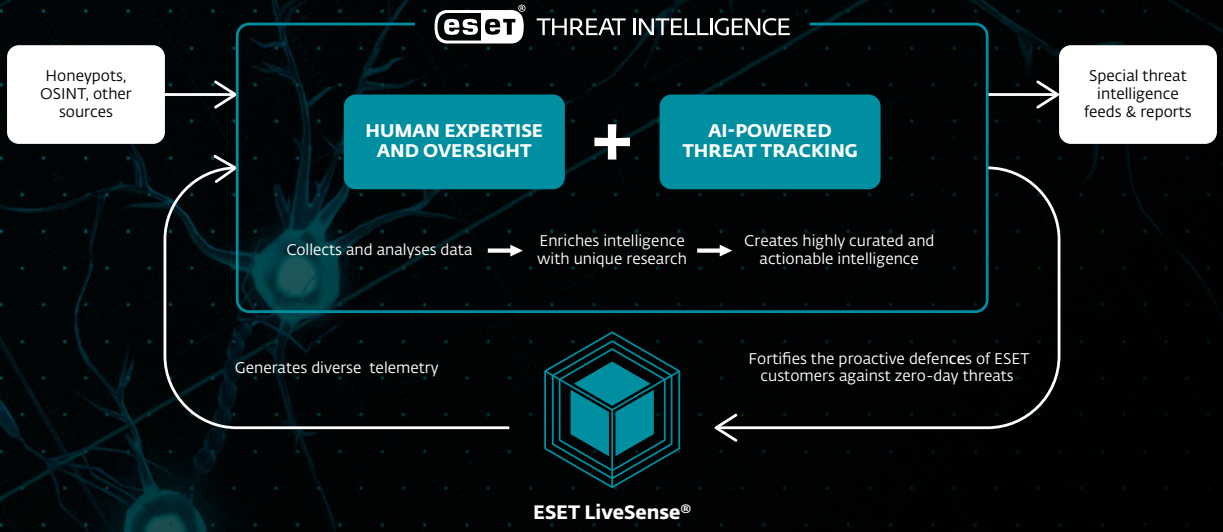
The creation of our intel is in fact a self-strengthening cycle.

It uses the wide range of telemetry generated by ESET LiveSense, our multilayered security technology which sits within ESET PROTECT Platform.

The gathered telemetry is complemented by various additional sources, such as honeypots, or OSINT.

Then, it is processed in our robust AI-augmented malware tracking and processing systems. These systems are capable of uncovering and adding a lot of contextual information to enrich the intelligence data.

As the crucial element, our threat intel experts oversee the final product and ensure it is curated to always contain fresh data to help you make better and faster decisions.



ESET proprietary intelligence feeds

Enrich your view of the worldwide threat landscape based on unique telemetry. ESET feeds come from our research centres around the globe, providing a holistic picture and enabling you to quickly block IoCs in your environment. Feeds are in the formats • JSON • STIX 2.1

MALICIOUS FILES FEED

This feed provides real-time information on newly discovered malware samples, their characteristics, and IoCs. It 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. The feed features malicious domains, including file hashes, timestamps, threat type detected, and other detailed information.

DOMAIN FEED

This feed can be used to block domains which are considered malicious. It 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.

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 which host them. All the information is filtered to show only high confidence results.

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 include 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. APT Feed is also part of APT Reports, but can be purchased separately.

With ESET feeds, you get

- ✓ HIGHLY CURATED DATA
- ✓ ACTIONABLE CONTENT
- ✓ LOW FALSE POSITIVES
- ✓ FREQUENT UPDATES
- ✓ COMPREHENSIVE API

The availability of ESET Threat Intelligence reports and feeds varies by country. Please contact your local ESET representative for more information.

About ESET

Next-gen digital security for business

WE DON'T JUST STOP BREACHES—WE PREVENT THEM

Unlike conventional solutions that focus on reacting to threats after they've been executed, ESET offers an unmatched AI-powered prevention-first approach backed by human expertise, renowned global Threat Intelligence, and an extensive R&D network led by industry-acclaimed researchers—all for the continuous innovation of our multilayered security technology.

Experience unparalleled protection from ransomware, phishing, zero-day threats and targeted attacks with our award-winning, cloud-first XDR cybersecurity platform that combines next-gen prevention, detection, and proactive threat hunting capabilities. Our highly customisable solutions include hyperlocal support. They offer minimal impact on endpoint performance, identify and neutralise emerging threats before they can be executed, ensure business continuity, and reduce the cost of implementation and management.

In a world where technology enables progress, protect your business with ESET.

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

200
countries and territories

13
global R&D centres

INDUSTRY RECOGNITION

Gartner Peer Insights. Customer First

ESET is recognized for over 700 reviews collected on Gartner Peer Insights

TrustRadius Tech Cares 2023

ESET recognized for giving back to the community with a 2023 Tech Cares Award from TrustRadius

ANALYST RECOGNITION

IDC ANALYZE THE FUTURE

In 2023, IDC placed ESET among the top 5 threat intelligence vendors and highlighted the profile of ESET Threat Intelligence.

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

ESET has been recognised as a 'Top Player' – for the fourth year in a row – in Radicati's Advanced Persistent Threat (APT) Protection Market Quadrant 2023.

MITRE ATT&CK™

ESET is the top independent cybersecurity software company contributor, and among the top 10 out of 354 contributors, to the MITRE ATT&CK framework.

ISO SECURITY CERTIFIED

ESET is compliant with ISO/IEC 27001:2013, an internationally recognised 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 CUSTOMERS

protected by ESET since 2017
more than 9,000 endpoints

protected by ESET since 2016
more than 4,000 mailboxes

protected by ESET since 2016
more than 32,000 endpoints

ISP security partner since 2008
2 million customer base

SOME OF OUR TOP AWARDS

"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, Diamantis Masoutis S.A., 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 Centre Operations Manager, Primoris Services Corporation, USA, 4,000+ seats