ESET®

THREAT INTELLIGENCE

Extend your security intelligence from local network to global cyberspace

CYBERSECURITY
EXPERTS ON YOUR SIDE

What is a **Threat Intelligence solution?**

ESET's Threat Intelligence service provides global knowledge on targeted attacks, advanced persistent threats (APTs), zero-days and botnet activities.

These items are traditionally difficult for security engineers to discover, who can only access information within their local network.

Why **Threat Intelligence?**

Threat Intelligence services help sift through the information overload and provide the most relevant information for specific organizations.

INFORMATION OVERLOAD

Zero-days, advanced persistent threats, targeted attacks and botnets are all concerns for industries across the world. The problem is, due to the amount 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 quickly and easily prioritize emerging threats, which leaves them more time to proactively implement new defenses against them.

PROACTIVE VS. REACTIVE

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 this attack from being repeated. However, this does not protect them from the next attack that may use another brand new vector.

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

INCIDENT RESPONSE SUPPORT

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 typically a very long and manual process as engineers sift through their network searching for abnormalities which may indicate a compromise occurred.

Threat Intelligence services allow incident response teams to fully understand and quickly respond to data breaches. By providing information on the threat actor, malware behaviour, 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.

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.

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.

The ESET difference

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, due to the threat actors being intelligent opponents.
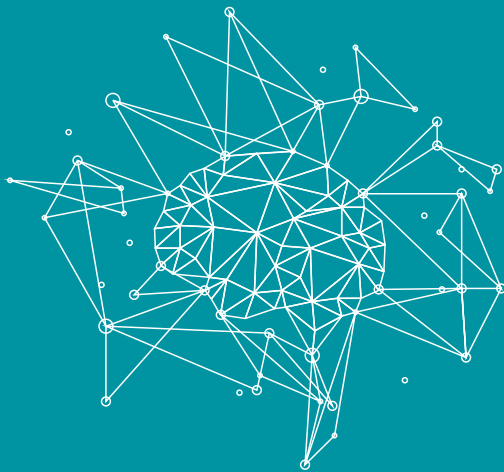
REPUTATION SYSTEM

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, and verified by our R&D centers, which gives customers the highest level of confidence when viewing information and reports within their console.

WORLDWIDE PRESENCE

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 worldwide perspective on all the most recent trends and threats.

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.

Use cases

Proactive Threat Prevention

Businesses want to prevent infiltrations from being able to communicate in or out of their network.

SOLUTION

✓ Threat intelligence proactively notifies security teams of the most recent targeted attacks and command and control (C&C) servers that have occurred around the globe.

✓ Threat intelligence provides data feeds which can be integrated with SIEM tools or UTM devices to stop connectivity to or from malicious actors, thus preventing data leaks or damages.

✓ Businesses input rules and mitigations to prevent the intrusion of ransomware into their organization.

RECOMMENDED ADDITIONAL ESET SOLUTIONS

✓ **ESET Endpoint Security**

✓ **ESET Enterprise Inspector**

Increase efficiency of incident response and investigations

Once an infection occurs, businesses need to make sure that they identify and remove all incidence of the infection across their network.

SOLUTION

✓ Reduce data gathering and investigation time by uploading and analyzing threats via ESET Threat Intelligence to provide information on how the threat functions.

✓ Search and remediate infections found within organizations using data provided by threat intelligence service.

RECOMMENDED ADDITIONAL ESET SOLUTIONS

✓ **ESET Endpoint Security**

✓ **ESET Enterprise Inspector**

"As we say at the hospital, prevention is better than healing."

— Jos Savelkoul, team leader ICT-Department, Zuyderland Hospital, Netherlands. 10.000+ Seats

Threat mitigation

Most businesses simply remediate threats and do not input mitigations to prevent new infections from infiltrating their organizations.

SOLUTION

✓ After a malware infection, a file can be submitted to ESET's automated sample analysis.

✓ The sample analysis provides actionable data on how the malware behaves.

✓ The organization inputs mitigations to prevent future infections from exploiting the same threat vectors.

RECOMMENDED ADDITIONAL ESET SOLUTIONS

✓ **ESET Endpoint Security**

✓ **ESET Mail Security**

✓ **ESET Enterprise Inspector**

✓ **ESET Dynamic Threat Defense**

"ESET security solutions have protected and alerted Primoris IT department on numerous occasions to serious threats and infections, most importantly ransomware."

— Joshua Collins, Data Center Operations Manager, Primoris Services Corporation, USA. 4.000+ Seats

ESET Threat Intelligence technical features

REAL-TIME DATA FEEDS

ESET Threat Intelligence data feeds utilize widely supported STIX/TAXII format, which makes it easy to integrate with existing SIEM tools. This integration helps to strengthen service providers and deliver the latest information on the threat landscape to predict and prevent threats before they strike. Currently there are three main types of feeds available: Botnet, Malicious file and Domain Feed. All feeds containing new metadata are refreshed every 5 minutes.

EARLY WARNING REPORTS

Provides reports based on YARA rules matches about programs, activity or related configurations that are being either prepared or already utilized in an attack against a specific organization or its customer.

ROBUST API

ESET Threat Intelligence features a full API that is available for automation of reports, YARA rules and other functionalities to allow for integration with other systems used within organizations.

ANDROID SAMPLE SUBMISSION

With ESET Threat intelligence, it is possible to monitor whether Android malware is targeting a business's mobile application. This is especially important for banks and other industries that have their own mobile applications. In addition, at any point a business can upload an android application into ESET Threat intelligence for full analysis of an .apk file.

YARA RULES

Allows the business to set up custom rules to obtain company-specific information that security engineers are interested in. Once these rules are set up, organizations receive valuable details such as the number of times they have been seen worldwide, URLs containing malicious code, malware behavior on the system, where it was detected, and more.

AUTOMATED SAMPLE ANALYSIS

Creates a custom report based on the submitted file or hash, which provides valuable information for fact-based decisions and incident investigations.

ESET Threat Intelligence dashboard

Early warning reports and feeds

Reports

TARGETED MALWARE REPORT

Keeps user informed about a potential attack that is under preparation or an ongoing attack aimed specifically against his organization. This report includes YARA rule strings, reputation information, similar binaries, file details, sandbox output and more.

BOTNET ACTIVITY REPORT

Delivers regular and quantitative data about identified malware families and variants of botnet malware. The report provides actionable data that includes Command and Control (C&C) servers involved in botnet management, samples of botnet, global weekly statistics, and a list of targets of this malware.

FORGED SSL CERTIFICATE REPORT

Generated when ESET detects a newly released SSL certificate by a certificate authority which has a very similar asset to the one provided by the customer during initial setup. This may include things like upcoming phishing campaigns that are attempting to leverage this certificate. This report provides key attributes of the certificate, YARA matches and certificate data.

TARGETED PHISHING REPORT

Shows data about all phishing email activities targeted at the selected organization. The report provides phishing campaign information that includes campaign size, number of clients, URL screenshots, preview of phishing email, location of servers and much more.

Feeds

BOTNET FEED

Features three types of feeds that check over 1000+ targets per day including information on the botnet itself, servers involved and their targets. The data provided directly by these feeds include items such as detection, hash, date of server last seen active, files downloaded, IP addresses, protocols, targets, and much more.

DOMAIN FEED

Features domains which are considered malicious including domain name, IP address, detection of file downloaded from URL and detection of file which was trying to access the URL.

MALICIOUS FILE FEED

Features executables which are considered malicious and recognizes and shares information such as SHA1, MD5, SHA256, detection, size, and file format.

CUSTOM FEEDS

ESET can provide a completely new feed based on specific organization requirements. Moreover, all currently available feeds are adjustable according to the customers needs.

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

BOTNET ACTIVITY REPORT

Global Statistics: Week 7/2018

DATE	SAMPLES	C&C	NEW C&C	TARGETS
2018-02-12	12225	7914	32	2647
2018-02-13	14487	7737	63	2706
2018-02-14	14114	8016	42	2737
2018-02-15	13359	8414	61	2789
2018-02-16	12160	7830	68	2640
2018-02-17	9445	7356	12	2697
2018-02-18	7378	6834	20	1795

FAMILY	SAMPLES	C&C	NEW C&C	TARGETS
Kovter	37988	9751	13	0
Emotet	11798	59	5	0
Wauchos	8157	19	0	0
Kasidet	7102	96	20	23
Zbot	6137	460	77	301
SpyBanker	4743	0	0	0
Dorkbot	2274	375	0	62
Ramnit	1408	16	0	119
Waski	1274	87	0	0
TrickBot	983	412	114	2135
Qbot	636	0	0	47
Retefe	256	43	17	163
Uramif	235	135	32	0
Papras	231	27	0	0
Tovkater	166	94	4	0
Banload	148	45	11	0
Elenoocka	10	14	0	0
Tinba	7	1	0	0

⚠ FORGED SSL CERTIFICATE REPORT

CLIENT	ESET DEMO
REPORT DATE	2017-11-09 16:55:06 CET (UTC/GMT +01:00)
REPORT ID	B9AB8/2017

Certificate

SUBJECT NAME	www.ynod.ir
VALID SINCE	2017-11-04T23:57:46.000Z
VALID TO	2018-02-02T23:57:46.000Z

Key Usage

Digital Signature, Key Encipherment

Names

nod32buy.ir
nod32buy2.ynod.ir
uappleid.com
uappleid.ynod.ir
www.nod32buy.ir
www.nod32buy2.ynod.ir
www.uappleid.com
www.uappleid.ynod.ir
www.ynod.ir
ynod.ir

YARA matches

SOURCE	OFFSET	LENGTH	STRING
cert	0x378	5	nod32

Certificate data

```
{
  "timestamp": {
```

⚠ TARGETED PHISHING REPORT   ⓔⓢⓔⓣ

CLIENT	ESET DEMO
REPORT DATE	2017-12-03 13:44:00 CET (UTC/GMT +01:00)
REPORT ID	32E30/2017

Phishing campaign

Campaign size	10 000 to 100 000
Number of clients	10 000 to 100 000
Campaign duration	9 day(s) 22 hour(s)
First phishing activity	2017-11-23 14:00:00 UTC
Last phishing activity	2017-12-03 12:00:00 UTC
Servers	55.30%
Endpoints	44.70%

Phishing URLs

URL	IP	LOCATION	DNS HISTORY
gooddrugssale(dot)su			46.242.139.49
			149.5.188.101
			199.127.103.200
			185.212.172.83

Locations of phishing servers

COUNTRY	SHARE
United States	34.69%
China	12.03%
Italy	9.10%
Japan	8.83%
Denmark	8.68%

About ESET

ESET – a global leader in information security – has been named as a Challenger in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms* two years in a row.

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

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.
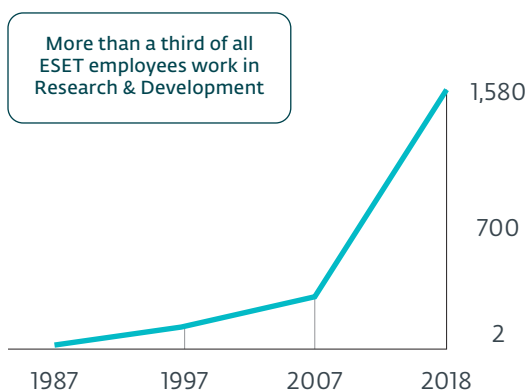
ESET IN NUMBERS

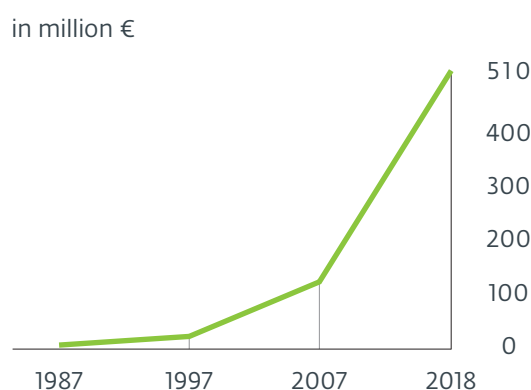**110m+**
users worldwide

400k+
business customers

200+
countries & territories

13
global R&D centers

ESET EMPLOYEES

More than a third of all ESET employees work in Research & Development

1,580
700
2

1987   1997   2007   2018

ESET REVENUE

in million €

510
400
300
200
100
0

1987   1997   2007   2018

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017
more than 14,000 endpoints

Canon
Canon Marketing Japan Group

protected by ESET since 2016
more than 9.000 endpoints

Allianz ⑪
Suisse

protected by ESET since 2016
more than 4,000 mailboxes

T·· ·

ISP security partner since 2008
2 million customer base

SOME OF OUR TOP AWARDS

AV TEST
APPROVED
CORPORATE
ENDPOINT
PROTECTION
av-test.org 10/2019
WINDOWS

G2
Leader
FALL
2019

THE CHANNEL CO.
CRN
★★★★★
PARTNER
PROGRAM
GUIDE
WINNER
2 0 1 9

AV
comparatives
APPROVED
Business Security
JUL 2019

SC
MEDIA
RECOMMENDED

"Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the shortlist for consideration in enterprise RFPs for anti-malware solutions."

KuppingerCole Leadership Compass
Enterprise Endpoint Security: Anti-Malware Solutions, 2018