WYPRODUKOWANE
**W UNII EUROPEJSKIEJ**
ROZWIJANE
**W POLSCE**

**4** MILIONY KLIENTÓW W POLSCE

# THREAT INTELLIGENCE

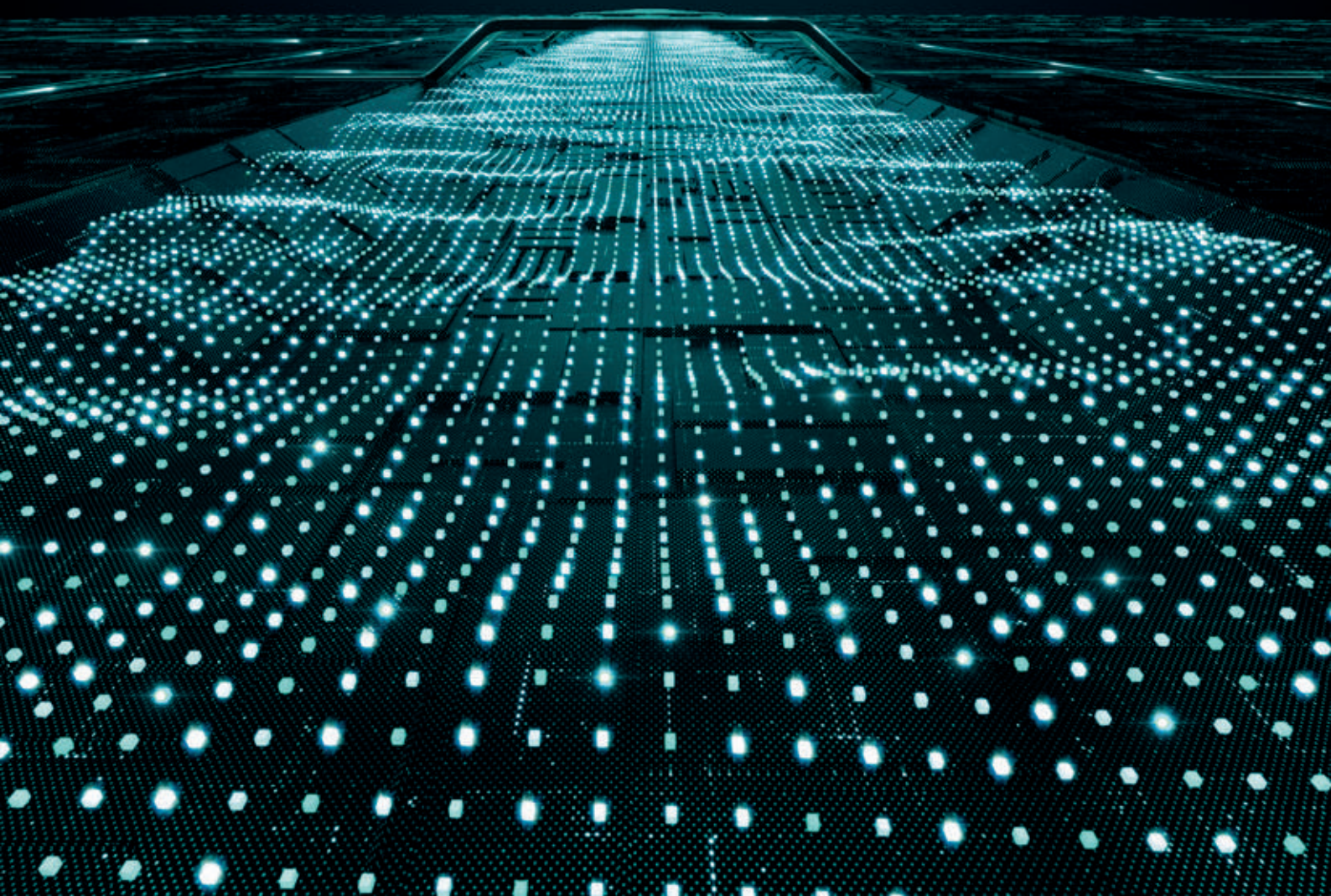
**Rozbuduj ochronę swojej sieci firmowej**
- wykorzystuj informacje z wnętrza sieci
i te pozyskane z globalnej cyberprzestrzeni.

ENJOY SAFER TECHNOLOGY™

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ESET jest globalnym dostawcą oprogramowania zabezpieczającego komputery firm oraz użytkowników indywidualnych, któremu zaufało **4 miliony Polaków i ponad 110 milionów użytkowników na świecie.**

Produkty ESET są rozwijane w kilku centrach badawczo-rozwojowych na świecie. **Pierwsze takie centrum powstało i działa do dzisiaj w Krakowie.** To, co od lat wyróżnia ESET na tle konkurencji, to metoda wykrywania wirusów i ataków oparta na **sztucznej inteligencji, tj. zaawansowanej heurystyce, która z czasem przerodziła się w uczenie maszynowe.** Rozwiązania ESET wyróżnia również niemal niezauważalne dla wydajności komputerów działanie, co wielokrotnie doceniły w testach niezależne ośrodki badawcze, m.in. AV-Test, czy AV-Comparatives.



# Czym jest usługa **ESET Threat Intelligence?**

**Usługa ESET Threat Intelligence dostarcza administratorowi informacji o identyfikowanych w globalnej cyberprzestrzeni atakach ukierunkowanych, zaawansowanych zagrożeniach (APT) i zero-day oraz informacji nt. aktywności botnetów, wymierzonych w sieć firmową.**

Wykrycie wspomnianych zagrożeń jest trudne, jeśli administrator ma dostęp wyłącznie do informacji zbieranych w sieci lokalnej.

# Dlaczego warto wybrać usługę **ESET Threat Intelligence?**

ESET Threat Intelligence pomaga filtrować informacje nt. ataków i zagrożeń ukierunkowanych na działanie w danej sieć firmowej, identyfikując i dostarczając informacje najistotniejsze z punktu widzenia danej organizacji.

## NADMIAR DANYCH SZKODZI

Zagrożenia zero-day, ataki ukierunkowane (APT) i botnety są problemem wielu firm na całym świecie. Ze względu na olbrzymią liczbę tego typu zagrożeń, organizacje te nie są w stanie łatwo identyfikować, które proaktywne mechanizmy obronne i jakie środki zaradcze powinny uruchomić w swoich firmach. To prowadzi do sytuacji, w której administrator gubi się, próbując znaleźć niezbędne informacje w oparciu o ograniczone dane - pochodzące z własnej sieci lub z olbrzymich zbiorów danych firm trzecich. Usługa ESET Threat Intelligence pomaga filtrować informacje nt. ataków i zagrożeń ukierunkowanych na działanie w danej sieć firmowej, identyfikując i dostarczając informacje najistotniejsze z punktu widzenia danej organizacji.

Umożliwia firmom szybkie i łatwe ustalanie priorytetów reakcji w odpowiedzi na pojawiające się zagrożenia, dając administratorom więcej czasu na wdrażanie nowych mechanizmów obronnych.

## OCHRONA PROAKTYWNA VS. REAKTYWNA

Współczesne cyberzagrożenia stale ewoluują - pojawiają się nowe metody ataków i nowe typy wirusów. Nic dziwnego, że kiedy dochodzi do ataku lub naruszenia danych organizacji, ta zwykle jest zaskoczona faktem, że ich mechanizmy obronne zawiodły oraz, że atak w ogóle miał miejsce. Dopiero po wykryciu incydentu, a więc reaktywnie, firmy wprowadzają zabezpieczenia, które mają ochronić je przed powtórką podobnego ataku. Takie podejście nie chroni jednak przedsiębiorstwa przed kolejnymi incydentami - cyberprzestępcy mogą bowiem wykorzystać nową podatność lub zastosować nowy sposób ataku.

ESET Threat Intelligence pozwala przygotować się na przyszłe i nieznane w danym momencie ataki i zagrożenia. Umożliwia organizacjom poprawę skuteczności działania posiadanych zabezpieczeń i wdrożenie nowych polityk bezpieczeństwa - takie proaktywne podejście pozwala wyprzedzać ewentualne ataki.

## REAKCJA NA INCYDENTY

Kiedy dochodzi do naruszenia danych, administratorzy zwykle muszą szybko dowiedzieć się, jak doszło do danego incydentu, a także określić, których urządzeń on dotyczył. Proces ten przebiega zwykle stosunkowo długo. Wszystko dlatego, że administratorzy muszą zwykle w tym celu ręcznie przeszukiwać swoją sieć, próbując odnaleźć elementy nietypowe.

ESET Threat Intelligence pozwala zespołom odpowiedzialnym za bezpieczeństwo sieci firmowej w pełni zrozumieć dany incydent i szybko reagować na naruszenia danych. Dostarczając informacji na temat źródła zagrożenia, zachowania szkodliwego oprogramowania, wektorów ataków oraz tzw. wskaźników kompromisu (IoC), administratorzy nie tylko lepiej rozumieją genezę i skutki ataku, ale przede wszystkim mogą szybciej reagować na kolejne incydenty.

Kiedy dochodzi do ataku lub naruszenia bezpieczeństwa danych, organizacje są zwykle zaskoczone, że ich mechanizmy obronne zawiodły oraz, że atak w ogóle miał miejsce.

Dostarczając informacji na temat źródła zagrożenia, zachowania szkodliwego oprogramowania, wektorów ataków oraz tzw. wskaźników kompromisu (IoC), administratorzy nie tylko lepiej rozumieją genezę i skutki ataku, ale przede wszystkim mogą szybciej reagować na kolejne incydenty.

# Poczuj różnicę z ESET

## WIEDZA EKSPERTÓW WSPARTA UCZENIEM MASZYNOWYM

Wykorzystanie zaawansowanych algorytmów uczenia maszynowego do automatyzowania decyzji i oceny zagrożeń stanowi integralną część naszego podejścia do ochrony użytkownika i sieci firmy. Siła i skuteczność tego rozwiązania zależy od wiedzy i umiejętności ludzi, którzy ją tworzyli. W ESET pracują światowej klasy eksperci i to dzięki ich wiedzy możliwe jest stosowanie wyjątkowo precyzyjnych i inteligentnych algorytmów identyfikujących zagrożenia.

## SYSTEM REPUTACJI

Rozwiązania ESET są wyposażone w chmurowy system wczesnego ostrzegania przed złośliwym oprogramowaniem oparty na reputacji plików – ESET LiveGrid®. System ten zbiera dane od 110 milionów użytkowników z całego świata, które są weryfikowane przez centra badawczo-rozwojowe (R&D) ESET. Zdobyte informacje ESET LiveGrid® udostępnia użytkownikom rozwiązań ESET, zapewniając im w ten sposób najwyższy możliwy poziom ochrony przed zagrożeniami i cyberatakami.

## ESET MARKĄ GLOBALNĄ

Rozwiązania ESET są obecne w ponad 200 krajach świata, w tym w Polsce. Firma posiada 13 laboratoriów badawczo-rozwojowych. Pierwsze z nich powstało w Krakowie, gdzie działa do dzisiaj. Firma posiada 22 biura rozlokowane na całym świecie. Globalna obecność firmy ESET pomaga w skutecznej walce z zagrożeniami rozprzestrzeniającymi się w różnych częściach świata, a także w opracowywaniu technologii wykrywania nowych zagrożeń i podatności.

Wiedza ekspertów ESET wspierana jest przez mechanizmy uczenia maszynowego. Ochronę rozbudowuje chmurowy system wczesnego ostrzegania LiveGrid®, oceniający reputację plików, gromadzący informację od 110 mln użytkowników z całego świata. Zbierane w ten sposób informacje są dodatkowo weryfikowane przez centra badawczo-rozwojowe ESET.

# Zastosowanie

## Proaktywne zapobieganie zagrożeniom

Firmy nie chcą, aby ich sieć była infiltrowana przez niepowołane osoby z wewnątrz organizacji oraz spoza niej.

### ROZWIĄZANIE

- ✓ ESET Threat Intelligence aktywnie powiadamia administratorów o najnowszych atakach ukierunkowanych oraz o serwerach C&C, które pojawiły się na całym świecie.
- ✓ Usługa, dzięki możliwości zintegrowania z systemami SIEM lub z UTM, pozwala zatrzymać łączność ze złośliwym oprogramowaniem lub zapobiec wyciekom danych.
- ✓ Firmy wprowadzają reguły bezpieczeństwa i odpowiednie środki, które mają zapobiegać atakom ransomware w ich organizacji.

### REKOMENDOWANE DODATKOWE ROZWIĄZANIA ESET

- ✓ **ESET Endpoint Security**

## Zwiększ efektywność reakcji na incydenty bezpieczeństwa

Po wystąpieniu infekcji firmy muszą upewnić się, że zostały zidentyfikowane i usunięte wszystkie zagrożenia wewnątrz sieci korporacyjnej.

### ROZWIĄZANIE

- ✓ Zredukuj ilość gromadzonych danych i czas jaki poświęcasz na dochodzenie przyczyn incydentów, przesyłając i analizując zagrożenia za pomocą narzędzia ESET Threat Intelligence. Dzięki temu możesz uzyskać niezbędne informacje na temat ich aktywności.
- ✓ Wyszukuj i usuwaj infekcje wykryte w sieciach korporacyjnych, korzystając z danych dostarczanych przez usługę ESET Threat Intelligence.

### REKOMENDOWANE DODATKOWE ROZWIĄZANIA ESET

- ✓ **ESET Endpoint Security**

*„Jak mówi się u nas w szpitalu: zapobieganie jest lepsze niż leczenie."*

— Jos Savelkoul, kierownik zespołu ds. technologii informatycznych
Zuyderland Hospital, Holandia (licencja dla 10 000 stanowisk)

# Zapobieganie zagrożeniom

Większość firm tylko usuwa bieżące zagrożenia. Nie wprowadza żadnych środków zaradczych, by zapobiegać przedostawaniu się do organizacji nowych zagrożeń.

## ROZWIĄZANIE

- ✓ Podejrzany plik można przesłać do systemu automatycznej analizy ESET.
- ✓ Analizowana próbka dostarcza przydatnych informacji o tym, w jaki sposób działa złośliwe oprogramowanie.
- ✓ Organizacje wprowadzają zmiany w celu uniknięcia podobnego ataku w przyszłości.

## REKOMENDOWANE DODATKOWE ROZWIĄZANIA ESET

- ✓ **ESET Endpoint Security**
- ✓ **ESET Mail Security**
- ✓ **ESET Dynamic Threat Defense**

*„Rozwiązania ESET chronią i ostrzegają dział IT Primoris w przypadku poważnych zagrożeń i infekcji oraz ataków ransomware."*

— Joshua Collins, data center operations manager w Primoris Services Corporation, Stany Zjednoczone (licencja dla 4 000 stanowisk)

# Funkcje ESET Threat Intelligence

## STRUMIEŃ DANYCH - DANE Z CHMURY W CZASIE RZECZYWISTYM

ESET Threat Intelligence dostarcza danych w znanych formatach STIX/TAXII, które ułatwiają integrację z istniejącymi systemami SIEM. Taka integracja pozwala rozbudować informacje dostarczane przez tego typu rozwiązania, dzięki czemu możliwe jest zapobieżenie atakom cyberzagrożeń zanim uderzą one w sieć firmową. ESET Threat Intelligence udostępnia trzy główne typy danych nt. botnetów, złośliwych plików oraz informacje dotyczące domen. Każdy wspomniany strumień danych jest odświeżany co 5 minut.

## RAPORTY WCZESNEGO OSTRZEGANIA

Narzędzie udostępnia raporty generowane w oparciu o reguły YARA, określając program, działanie lub powiązaną konfigurację, które zostały przygotowane do ataku, albo już wykorzystane w ataku na konkretną organizację lub klienta.

## AUTOMATYCZNA ANALIZA PRÓBEK

ESET Threat Intelligence pozwala tworzyć niestandardowe raporty, na podstawie przesłanego pliku lub jego hasha. Sam raport dostarcza wielu wartościowych informacji, które mogą pomóc w zmianie dotychczasowych polityk bezpieczeństwa firmy lub w analizie konkretnych incydentów.

## ANALIZA PRÓBEK ZAGROŻEŃ DLA ANDROIDA

ESET Threat intelligence umożliwia weryfikację, czy złośliwe oprogramowanie wymierzone w urządzenia z Androidem, może wpływać na aplikację mobilną danej organizacji. To szczególnie ważne dla banków i branż, które udostępniają klientom własne aplikacje mobilne. Dodatkowo narzędzie pozwala na analizę dowolnej aplikacji dla systemu Android - wystarczy zaimportować do ESET Threat Intelligence stosowny plik (.apk).

## REGUŁY YARA

Reguły YARA umożliwiają administratorom tworzenie niestandardowych zapytań i uzyskiwanie informacji charakterystycznych tylko dla konkretnej firmy. Takie dane zawsze interesują administratorów bezpieczeństwa sieci. Raport poinformuje m.in. o potencjalnych lub trwających właśnie atakach, w tym o częstotliwości takich ataków, adresach URL zawierających złośliwy kod, danych dotyczących późniejszej aktywności zagrożeń w systemie, miejscach, w których zostały one wykryte itp.

## INTERFEJS API

ESET Threat Intelligence udostępnia pełny interfejs API, który pozwala automatyzować raporty. Reguły YARA i inne funkcjonalności umożliwią integrację rozwiązania ESET z innymi systemami używanymi w danej organizacji.


Panel kontrolny
ESET Threat Intelligence

# Raporty z systemu wczesnego wykrywania

## Raporty

### RAPORTY NT. ATAKÓW TARGETOWANYCH

Informują użytkownika o bieżących atakach wymierzonych w organizację oraz o potencjalnych zagrożeniach wymierzonych w firmę, będących dopiero w trakcie przygotowania. Raporty te zawierają zestawy reguł YARA, informacje o reputacji zagrożeń, podobne do niego pliki binarne, szczegóły nt. plików, dane wyjściowe z obszaru testowego i wiele innych.

### RAPORT NT. AKTYWNOŚCI BOTNETÓW

Zawiera informacje dotyczące zidentyfikowanych rodzin złośliwego oprogramowania i zagrożeń tworzących sieć komputerów zombie, czyli tzw. botnetów. Raport zawiera przydatne dla administratorów informacje, które obejmują: serwery Command and Control (C&C) zaangażowane w zarządzanie botnetami, próbki botnetu, globalne tygodniowe statystyki oraz listę celów złośliwego oprogramowania.

### RAPORT NT. FAŁSZYWYCH CERTYFIKATÓW SSL

Generowany, gdy program ESET wykryje nowo wydany certyfikat SSL ze zbliżonymi parametrami do tego, jaki klient dostarczył podczas początkowej konfiguracji. Może ostrzegać przed zbliżającymi się kampaniami phishingowymi. Raport zawiera m.in. kluczowe atrybuty certyfikatu, jego dane i dopasowania YARA.

### RAPORT O ATAKACH PHISHINGOWYCH

Przedstawia dane dotyczące wszystkich działań phishingowych skierowanych do wybranej organizacji. Raport zawiera informacje o kampanii wyłudzającej informacje, w tym: jej rozmiar, liczbę klientów, zrzuty z adresów URL, podgląd wiadomości phishingowych, lokalizację serwerów i wiele więcej.

## Informacje

### INFORMACJE O BOTNETACH

ESET Threat Intelligence dostarcza trzy typy strumieni informacji, które przekazują informacje nt. ponad tysiąca celów dziennie, w tym dane na temat samych botnetów, zaangażowanych serwerów i ich celów. Obejmują takie elementy jak: wykrywanie zagrożeń, hash, ostatnią datę aktywności serwera, pobrane pliki, adresy IP, protokoły, cele itp.

### INFORMACJE O DOMENIE

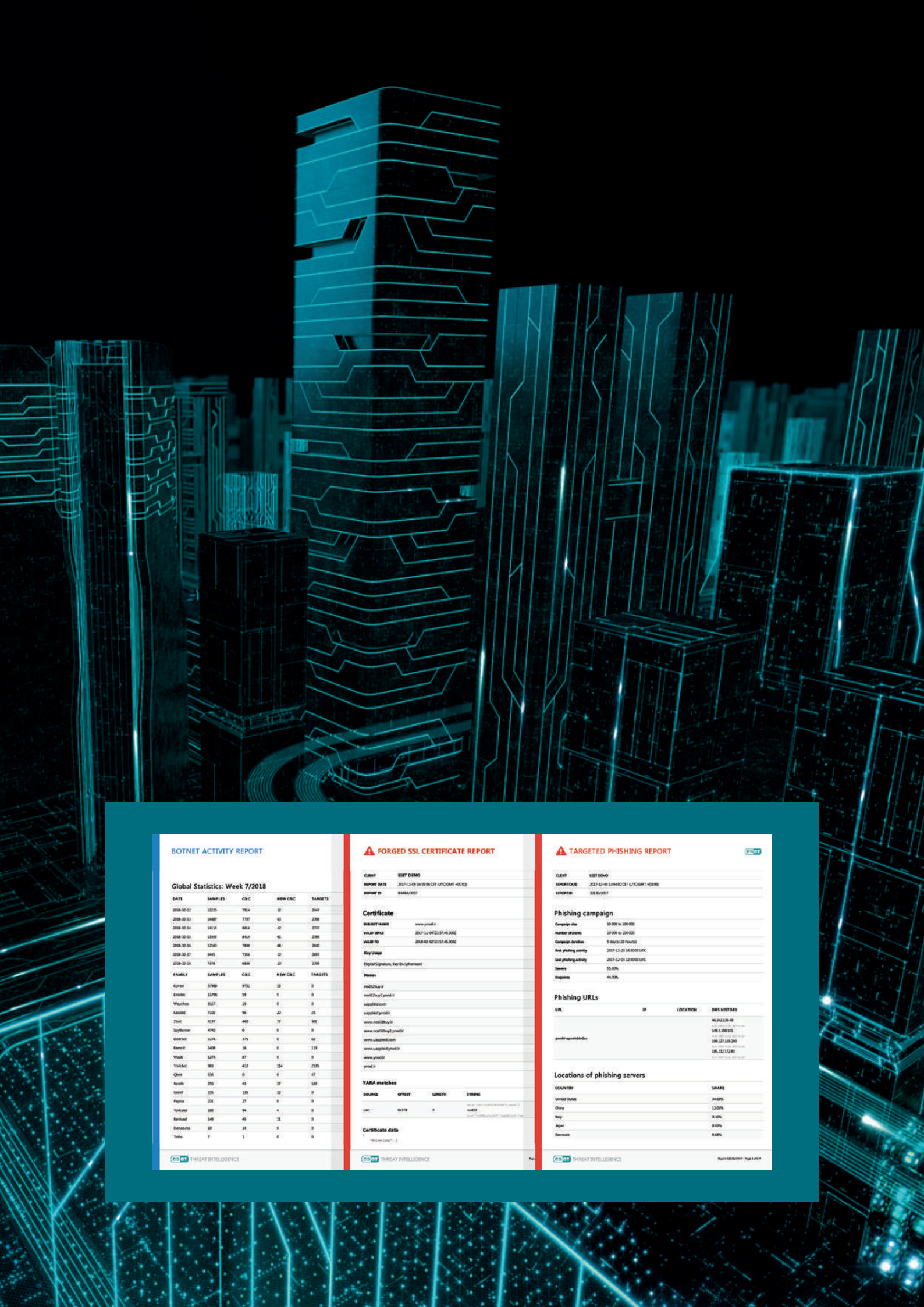
Usługa ESET Threat Intelligence udostępnia informacje o szkodliwych domenach i uwzględnia w szczególności: nazwę domeny, adres IP, wykrywanie pliku pobranego z adresu URL i detekcję pliku, który próbował uzyskać dostęp do adresu URL.

### INFORMACJE O ZŁOŚLIWYCH PLIKACH

ESET Threat Intelligence zawiera informacje o zainfekowanych plikach, rozpoznaje i udostępnia dane dotyczące m.in. SHA1, MD5, SHA256, podaje detekcję, rozmiar i format pliku.

### INFORMACJE ZGODNE Z POTRZEBAMI FIRM

Usługa ESET może dostosować źródła informacji do określonych wymagań organizacji.



BOTNET ACTIVITY REPORT

Global Statistics: Week 7/2018

| DATE | SAMPLES | C&C | NEW C&C | TARGETS |
|---|---|---|---|---|
| 2018-02-12 | 12225 | 7914 | 32 | 2047 |
| 2018-02-13 | 14487 | 7737 | 43 | 2706 |
| 2018-02-14 | 14114 | 8454 | 42 | 2737 |
| 2018-02-15 | 13059 | 8414 | 41 | 2789 |
| 2018-02-16 | 12160 | 7838 | 48 | 2640 |
| 2018-02-17 | 9445 | 7356 | 12 | 2497 |
| 2018-02-18 | 7378 | 6834 | 20 | 1795 |

| FAMILY | SAMPLES | C&C | NEW C&C | TARGETS |
|---|---|---|---|---|
| Kovter | 57988 | 9751 | 19 | 0 |
| Emotet | 11798 | 59 | 5 | 0 |
| Wauchos | 8317 | 19 | 0 | 0 |
| Gamblet | 7102 | 96 | 20 | 23 |
| Zbot | 6137 | 460 | 77 | 901 |
| SpyBanker | 4745 | 0 | 0 | 0 |
| Dorkbot | 2274 | 375 | 0 | 92 |
| Ramnit | 1408 | 16 | 0 | 159 |
| Neshi | 1274 | 87 | 0 | 0 |
| Trickbot | 980 | 412 | 114 | 2135 |
| Qhost | 636 | 0 | 0 | 47 |
| Nemim | 256 | 45 | 17 | 169 |
| Unruf | 235 | 135 | 12 | 0 |
| Pepms | 231 | 27 | 0 | 0 |
| Tovkater | 166 | 94 | 4 | 0 |
| Banload | 148 | 45 | 11 | 0 |
| Elenooka | 10 | 14 | 0 | 0 |
| Tinba | 7 | 1 | 0 | 0 |

ESET THREAT INTELLIGENCE

FORGED SSL CERTIFICATE REPORT

| | |
|---|---|
| CLIENT | ESET DEMO |
| REPORT DATE | 2017-12-09 16:59:09 CET (UTC/GMT +01:00) |
| REPORT ID | 89A8A/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

{
"Version": 2


ESET THREAT INTELLIGENCE

TARGETED PHISHING REPORT

| | |
|---|---|
| CLIENT | ESET DEMO |
| REPORT DATE | 2017-12-09 13:44:00 CET (UTC/GMT +01:00) |
| REPORT ID | 53E3D/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 | 2017-11-28 14:30:00 UTC |
| last phishing activity | 2017-12-09 12:30:00 UTC |
| Servers | 55.30% |
| Endpoints | 44.70% |

Phishing URLs

| URL | IP | LOCATION | DNS HISTORY |
|---|---|---|---|
| | | | 46.262.130.49<br>149.5.168.101<br>188.127.159.200<br>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% |

ESET THREAT INTELLIGENCE

# O ESET

**ESET jest globalnym dostawcą oprogra-
-mowania zabezpieczającego komputery firm oraz użytkowników indywidualnych, któremu zaufało 4 miliony Polaków i ponad 110 milionów osób na świecie. Producent został uznany jedynym Challengerem w raporcie Gartner Magic Quadrant dla platform Endpoint Protection 2018[1].**

Od 30 lat ESET w swoich centrach badawczo-
-rozwojowych, m.in. od ponad dekady w Krakowie, rozwija najlepsze w branży oprogramowanie i usługi bezpieczeństwa informatycznego, dostarczając firmom i użytkownikom indywidualnym kompleksowe rozwiązania do ochrony przed stale ewoluującymi zagrożeniami.

ESET jest firmą o wysokiej płynności finansowej, od początku pozostającą w rękach prywatnych przedsiębiorców. Dzięki temu ESET ma pełną swobodę działania i może zapewnić najlepszą ochronę wszystkim swoim klientom.

Produkty ESET dostępne są w ponad 200 krajach świata. W Polsce za dystrybucję rozwiązań ESET odpowiada firma DAGMA.

## ESET W LICZBACH

**110 mln+**
użytkowników na całym świecie

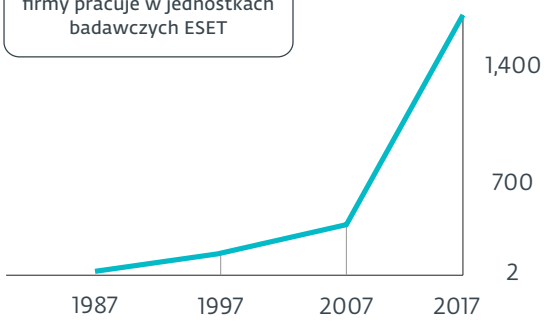
**4 mln+**
użytkowników w Polsce

**400 tys.+**
klientów biznesowych

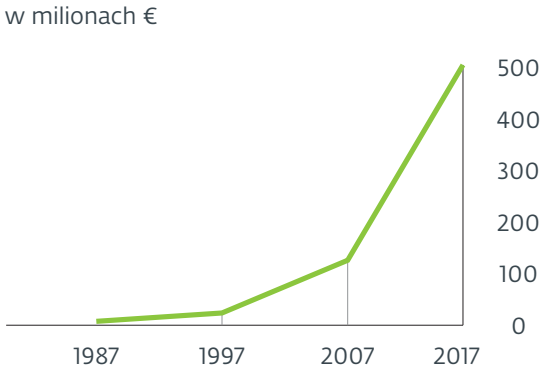
**13**
centrów badawczo-
-rozwojowych

## PRACOWNICY ESET

Więcej niż 1/3 pracowników firmy pracuje w jednostkach badawczych ESET




## PRZYCHODY ESET




[1] Gartner nie promuje żadnego sprzedawcy, produktu ani usług przedstawionych w publikacjach badawczych. Publikacje badawcze Gartnera zawierają opinie organizacji badawczej Gartnera i nie powinny być interpretowane jako stwierdzenia faktów. Gartner zrzeka się wszelkich gwarancji wyrażonych lub domniemanych, w odniesieniu do tych badań, w tym wszelkich gwarancji przydatności handlowej lub jakości do określonego celu.

## WYBRANI KLIENCI

HONDA

Od 2011 roku chroniona przez ESET.
Licencje w tym okresie zostały trzykrotnie przedłużone, a ich liczba podwojona.

GREENPEACE

Od 2008 roku chroniony przez ESET.
Licencje w tym okresie zostały przedłużone dziesięciokrotnie.

Canon

Od 2016 roku ESET chroni ponad 14 tysięcy stanowisk.

T-Mobile jest partnerem ISP od 2008 roku.
W swojej bazie posiada 2 mln klientów.

## WYBRANE NAGRODY

CRN

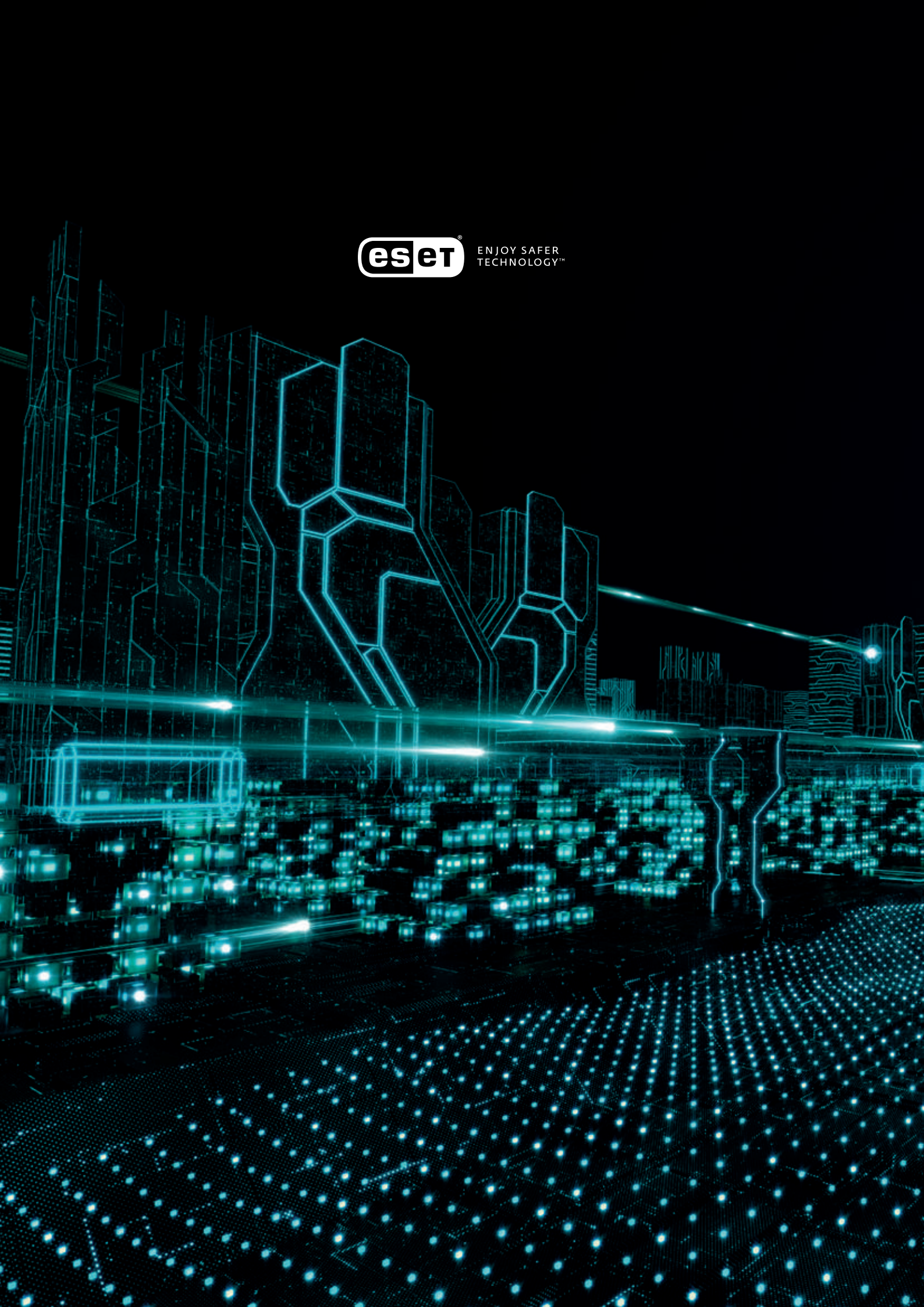
SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

AV comparatives Approved Business Product 2017

PRODUKT ROKU 2017 WYBÓR CZYTELNIKÓW IT professional

*„Biorąc pod uwagę cechy produktu, zarówno w zakresie ochrony przed złośliwym oprogramowaniem, możliwościami zarządzania, jak również w zakresie globalnego zasięgu klientów i wsparcia technicznego, ESET powinien być brany pod uwagę w zapytaniach ofertowych i przetargach dotyczących wdrożenia rozwiązań antywirusowych."*

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


ENJOY SAFER
TECHNOLOGY™