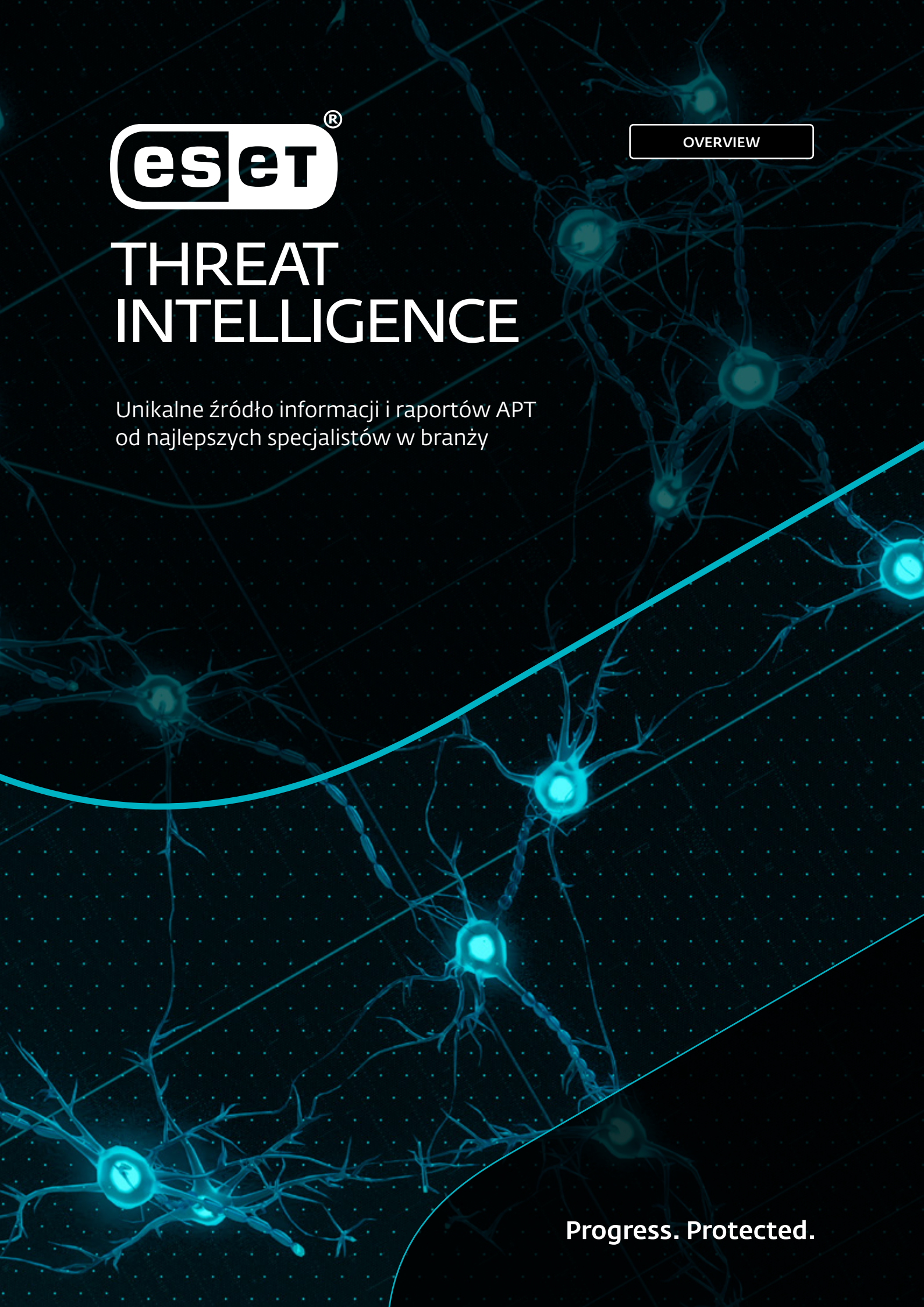
OVERVIEW

THREAT INTELLIGENCE

Unikalne źródło informacji i raportów APT
od najlepszych specjalistów w branży



Progress. Protected.

Zyskaj interesującą perspektywę na krajobraz zagrożeń i cyberbezpieczeństwa

ZYSKAJ DOSTĘP DO WYJĄTKOWEJ WIEDZY

ESET gromadzi informacje o zagrożeniach z unikalnej gamy źródeł i dysponuje niezrównanym doświadczeniem, które pomaga zwalczać coraz bardziej wyrafinowane ataki cybernetyczne.

WYPRZEDZAJ PRZECIWNIKÓW

ESET śledzi pieniądze, w szczególności monitorując kraje wykrycia grup APT atakujące zachodnie firmy, tj.: Rosję, Chiny, Koreę Północną, Iran. O nowych zagrożeniach dowiesz się jako pierwszy.

ZYSKAJ DODATKOWY CZAS NA REAKCJĘ

Przewiduj zagrożenia i podejmuj szybsze i lepsze decyzje dzięki kompleksowym raportom ESET i wyselekcjonowanym kanałom informacyjnym. Zmniejsz możliwość narażenia na dominujące zagrożenia, o których ostrzegą Cię eksperci.

POPRAW SWOJE BEZPIECZEŃSTWO

Na podstawie źródeł danych wywiadowczych ESET możesz zwiększyć możliwość wykrywania zagrożeń i ich usuwania, blokować ataki APT i oprogramowanie ransomware oraz ulepszać infrastrukturę cyberbezpieczeństwa.

AUTOMATYCZNE BADANIE ZAGROŻEŃ

Technologia ESET stale wyszukuje zagrożenia na wielu poziomach, od stanu przed uruchomieniem do stanu zakończenia. Skorzystaj z telemetrii we wszystkich krajach, w których ESET wykrywa podobne zagrożenia.

Zaleta ESET

Wiedza ekspertów poparta uczeniem maszynowym. Nasz system reputacji LiveGrid® składa się ze 110 milionów sond na całym świecie i jest weryfikowany w naszych centrach badawczo-rozwojowych.

WIEDZA EKSPERTÓW WSPIERANA 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.

SKUTECZNY SYSTEM REPUTACJI — LIVEGRID®

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 badawczorozwojowe (R&D) ESET. Zdobyte informacje ESET LiveGrid® udostępnia użytkownikom rozwiązań ESET, zapewniając im w ten sposób najwyższy możliwy poziom ochrony przed zagrożeniami i cyberatakami.

UNIJNE KORZENIE, ŚWIATOWY ZASIĘG

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.

eset® Digital Security **Progress. Protected.**

Raporty nt. zagrożeń APT (Advanced Persistent Threat)

NAJLEPSZE BADANIA NA WYCIĄGNIĘCIE RĘKI

Nasz zespół badawczy jest dobrze znany w branży cyberbezpieczeństwa dzięki naszemu wielokrotnie nagradzanemu blogowi We Live Security. Dostępne są tam podsumowania badań zespołu i działań APT, a także znacznie bardziej szczegółowe informacje. Klienci ESET otrzymują ekskluzywny wcześniejszy dostęp do całej zawartości We Live Security.

PRAKTYCZNE I DOPASOWANE DO TWOICH POTRZEB

Nasze sprawozdania są źródłem cennych informacji na temat najnowszych zagrożeń, przedstawiając również kontekst infekcji. Dzięki pracy naszych ekspertów uzyskane dane zyskują cenne komentarze, stając się w ten sposób bardziej przejrzyste i zrozumiałe. W ten sposób zyskujesz wiedzę, która z wyprzedzeniem pozwala przygotować się Tobie i Twojej firmie na ewentualne ataki.

SZYBKIE PODEJMOWANIE KLUCZOWYCH DECYZJI

Wszystko to pomaga organizacjom w podejmowaniu kluczowych decyzji i zapewnia strategiczną przewagę w walce z cyberprzestępczością – uzyskasz dostęp do informacji nt. nowych ataków, zyskasz ich kontekst, a dzięki temu będziesz mógł szybciej podejmować kluczowe dla bezpieczeństwa IT decyzje.

DOSTĘPNOŚĆ ANALITYKA ESET

Każdy klient zamawiający pakiet APT Reports Premium będzie miał także aż do 4 godzin miesięcznie dostępu do analityka ESET. Daje to możliwość bardziej szczegółowego omówienia problemów i otrzymania pomocy w rozwiązaniu wszelkich nierozstrzygniętych kwestii.

DZIĘKI APT REPORTS OTRZYMASZ

Dostęp do prywatnej, szczegółowej analizy technicznej	Miesięczne podsumowanie dla kadry kierowniczej najwyższego szczebla	Bezpośredni dostęp do specjalisty ds. cyberbezpieczeństwa ESET	Raport podsumowujący działanie APT	Dostęp do serwisu MISP

SZCZEGÓŁOWA ANALIZA

Pakiet zawiera miesięczne szczegółowe raporty zawierające analizę techniczną opisujące ostatnie kampanie, nowe zestawy narzędzi i powiązane tematy. Co dwa tygodnie będziesz także otrzymywać raport z podsumowaniem działań, który opisuje najnowsze kampanie APT, które badacze ESET śledzili, zawierające powiązanych aktorów, ich cele i oczywiście wskaźniki kompromitacji (IoC). Przegląd miesięczny łączy informacje ze wszystkich raportów, analiz technicznym i podsumowań działań opublikowanych w poprzednim miesiącu.

Dostępność sprawozdań i źródeł danych ESET Threat Intelligence jest uzależniona od kraju. Aby uzyskać więcej informacji, należy skontaktować się z lokalnym przedstawicielem firmy ESET.

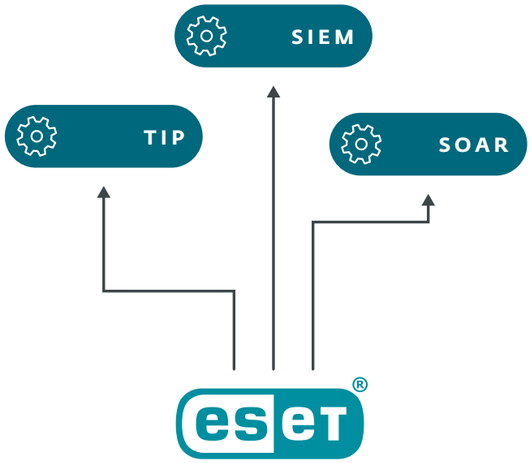
Zintegruj rozwiązanie ESET Threat Intelligence ze swoimi systemami

Integracja telemetrii ESET jest prosta i wzbogaci Twój **TIP**, **SIEM** lub **SOAR.**

Posiadamy **kompleksowe API z pełną dokumentacją.**

Dostarczamy dane w **standardowych formatach** – takich jak JSON i STIX poprzez TAXII – dzięki czemu możliwa jest integracja z dowolnym narzędziem.

Dla IBM QRadar, Anomali, ThreatQuotient i Logpoint posiadamy **instrukcje integracji umożliwiające szybką i łatwą implementację** i stale dodajemy kolejne rozwiązania do listy.



Jak powstaje nasza wiedza o zagrożeniach? **Cykl życia rozwiązania ESET Threat Intelligence**

Tworzenie naszego wywiadu jest w rzeczywistości cyklem samowzmacniania.

Wykorzystuje szeroką gamę danych telemetrycznych generowanych przez ESET LiveSense, naszą wielowarstwową technologię zabezpieczeń wbudowaną w platformę ESET PROTECT.

Zebraną telemetrię uzupełniają różne dodatkowe źródła, takie jak Honeypot czy OSINT.

Następnie dane są przetwarzane w naszych systemach badania złośliwego oprogramowania wspomaganych sztuczną inteligencją. Systemy te sa w stanie odkryć i dodać wiele informacji kontekstowych w celu wzbogacenia danych wywiadowczych.

Najważniejszym elementem elementów jest dbałość ekspertów do spraw zagrożeń o końcowy produkt, aby był najlepiej dostosowany do najnowszych dostępnych danych, które pomogą Ci podejmować lepsze i szybsze decyzje.

Zastrzeżone źródła danych wywiadowczych

Wzbogać swój podgląd na światowy krajobraz cyberbezpieczeństwa w oparciu o unikalną telemetrię. Kanały ESET pochodzą z naszych ośrodków badawczych na całym świecie, zapewniając kompletny obraz i umożliwiając szybkie blokowanie IoC w Twoim środowisku. Kanały informacyjne są dostępne w formatach • JSON • STIX 2.1

POCHODZENIE SZKODLIWYCH PLIKÓW

Kanał informacyjny w czasie rzeczywistym dostarczający dane o nowo odkrytych próbkach złośliwego oprogramowania, ich charakterystyce i IoC. Pomaga zrozumieć, które złośliwe pliki są obecnie często spotykane i umożliwia proaktywne ich blokowanie zanim spowodują jakiekolwiek szkody. Kanał zawiera listę złośliwych domen, w tym skróty plików, oznaczenie czasu, wykryty typ zagrożenia i inne szczegółowe informacje.

INFORMACJE O DOMENACH

Tego kanału można używać do blokowania domen uznawanych za złośliwe. Obejmuje nazwy domen, adresy IP i powiązane z nimi daty. Kanał klasyfikuje domeny na podstawie ich ważności, co umożliwia odpowiednie dostosowanie odpowiedzi, na przykład w celu blokowania tylko domen o wysokim stopniu istotności.

INFORMACJE O ADRESACH IP

Kanał udostępnia adresy IP uważane za złośliwe i powiązane z nimi dane. Struktura danych jest bardzo podobna do stosowanej w przypadku domen i adresów URL. Głównym przykładowym zastosowaniem jest tutaj przedstawienie, które adresy IP są obecnie powszechne, zablokowanie tych adresów IP, które są bardzo ważne, wykrycie tych mniej istotnych i dalsza weryfikacja.

INFORMACJE O ADRESACH URL

Podobnie jak w przypadku kanału informacyjnego dla domen, kanał URL sprawdza określone adresy. Zawiera szczegółowe informacje o danych związanych z adresem URL, a także informacje o domenach, które je hostują. Wszystkie informacje są filtrowane, aby wyświetlić tylko wyniki o wysokim stopniu wiarygodności.

KANAŁ INFORMACYJNY BOTNET

Bazując na autorskiej sieci śledzenia botnetów firmy ESET, kanał Botnet Feed zawiera trzy typy kanałów podrzędnych – botnet, C&C i cele. Dostarczane dane obejmują takie elementy, jak wykrywanie, hash, ostry żywy, pobrane pliki, adresy IP, protokoły, cele i inne informacje.

KANAŁ INFORMACYJNY APT

Ten kanał zawiera informacje APT opracowane w ramach badań firmy ESET. Ogólnie rzecz biorąc, plik danych jest eksportem z wewnętrznego serwera MISP firmy ESET. Wszystkie udostępniane dane są również szczegółowo wyjaśnione w raportach APT. Kanał informacyjny o APT jest również częścią raportów APT, ale można go zakupić osobno.

Dzięki kanałom informacyjnym ESET zyskujesz

- ✓ INFORMACJE O NOWINKACH Z BRANŻY
- ✓ AKTYWNĄ TREŚĆ
- ✓ NISKĄ ILOŚĆ FAŁSZYWYCH ALARMÓW
- ✓ CZĘSTE AKTUALIZACJE
- ✓ KOMPLEKSOWE AP

Dostępność sprawozdań i źródeł danych ESET Threat Intelligence jest uzależniona od kraju. Aby uzyskać więcej informacji, należy skontaktować się z lokalnym przedstawicielem firmy ESET.

eset® Digital Security
Progress. Protected.

O firmie ESET

Nowa generacja cyberochrony dla firm

Podczas gdy tradycyjne rozwiązania zabezpieczające skupiają się na reagowaniu na zagrożenia dopiero po ich wykonaniu, ESET oferuje niezrównane podejście do zapobiegania oparte o sztuczną inteligencję, ekspertyzę uznanych analityków, technologię Threat Intelligence i rozległą sieć ośrodków badawczo – rozwojowych prowadzonych przez uznanych w branży ekspertów.

Poznaj bliżej niezwykle skuteczną ochronę przed oprogramowaniem ransomware, atakami typu phishing, zagrożeniami zero - day i atakami ukierunkowanymi. A wszystko to dzięki naszej wielokrotnie nagradzanej, chmurowej platformie XDR, która łączy w sobie mechanizmy zapobiegania, proaktywnego wykrywania i neutralizowania zagrożeń. Nasze rozwiązania oferują niespotykane na rynku możliwości konfiguracji. Zainwestuj w ochronę ESET. Zmniejsz koszty wdrożenia i zarządzania cyberochroną, zyskaj skuteczne zabezpieczenie dla firmy, zapewniając jej ciągłość działania, przy minimalnym wpływie na wydajność chronionych stacji roboczych.

Technologia umożliwia postęp, ESET ją zabezpiecza.

ESET W LICZBACH

1 mld+
użytkowników na świecie

400k+
klientów biznesowych

195
krajów i terytoriów

13
globalnych ośrodków badań i rozwoju

UZNANIE W BRANŻY

Gartner Peer Insights. Customer First

ESET jest doceniany dzięki ponad 700 recenzjom zebranym w serwisie Gartner Peer Insights

TrustRadius Tech Cares 2023

ESET został także doceniony za wsparcie dla społeczności nagrodą Tech Cares Award 2023 od TrustRadius

UZNANIE ANALITYKÓW

IDC ANALYZE THE FUTURE

W 2023 r firma IDC umieściła ESET wśród 5 największych dostawców analizy zagrożeń i podkreśliła profil rozwiązania ESET Threat Intelligence.

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

Firma ESET została uznana za „Top Player" czwarty rok z rzędu w raporcie Redicati Advanced Persistent Threat Market Quadrant 2023.

MITRE ATT&CK™

ESET jest największym niezależnym dostawcom oprogramowania z zakresu cyberbezpieczeństwa i w pierwszej dziesiątce z 354 autorów tworzących platformę MITRE ATT&CK.

CERTYFIKAT BEZPIECZEŃSTWA ISO

ESET jest zgodny z normą ISO/IEC 27001:2013, uznaną na całym świecie i mającą zastosowanie normą bezpieczeństwa dotyczącą wdrażania i zarządzania bezpieczeństwem informacji. Certyfikat jest przyznawany przez zewnętrzną akredytowaną jednostkę certyfikacyjną SGS i potwierdza pełną zgodność ESET z najlepszymi praktykami w branży.

NASI KLIENCI

zabezpieczamy ponad 9 tyś stacji roboczych od 2017 roku

zabezpieczamy ponad 4 tyś skrzynek pocztowych od 2016 roku

ochraniamy ponad 32 tyś stacji roboczych od 2016 roku

Partner ISP security od 2008 roku z około 2 milionową bazą klientów

NIEKTÓRE Z NASZYCH NAJLEPSZYCH NAGRÓD

"REALIZACJA BYŁA BARDZO PROSTA. WSPÓŁPRACUJĄC Z DOBRZE WYSZKOLONYM PRACOWNIKIEM TECHNICZNYM ESET, W KILKA GODZIN URUCHOMILIŚMY W PEŁNI ROZWIĄZANIE ZABEZPIECZAJĄCE."

Menedżer IT, Diamantis Masoutis S.A.,
Grecja, ponad 6 000 stanowisk

"BYLIŚMY POD WRAŻENIEM WSPARCIA I POMOCY, JAKĄ OTRZYMALIŚMY. OPRÓCZ TEGO, ŻE JEST TO ŚWIETNY PRODUKT, DOSKONAŁA OPIEKA I WSPARCIE, JAKIE OTRZYMALIŚMY, BYŁY TYM, CO TAK NAPRAWDĘ DOPROWADZIŁO DO ZABEZPIECZENIA WSZYSTKICH SYSTEMÓW PRIMORIS."

Joshua Collins, kierownik operacyjny centrum danych
Primoris Services Corporation, USA
ponad 4000 stanowisk