OVERVIEW

THREAT INTELLIGENCE

Unikalne źródła informacji i raportów
od najlepszych specjalistów w branży

Progress. Protected.

Dlaczego warto dodać ESET do swojego CTI?

Zrozumienie obecnego krajobrazu zagrożeń oraz taktyk stosowanych przez cyberprzestępców zapewnia kluczową przewagę informacyjną. **Wiedza ta umożliwia organizacjom skuteczne wzmacnianie wewnętrznych systemów ochrony.** Fundamentem każdej solidnej strategii Cyber Threat Intelligence (CTI) są wysokiej jakości dane wywiadowcze.

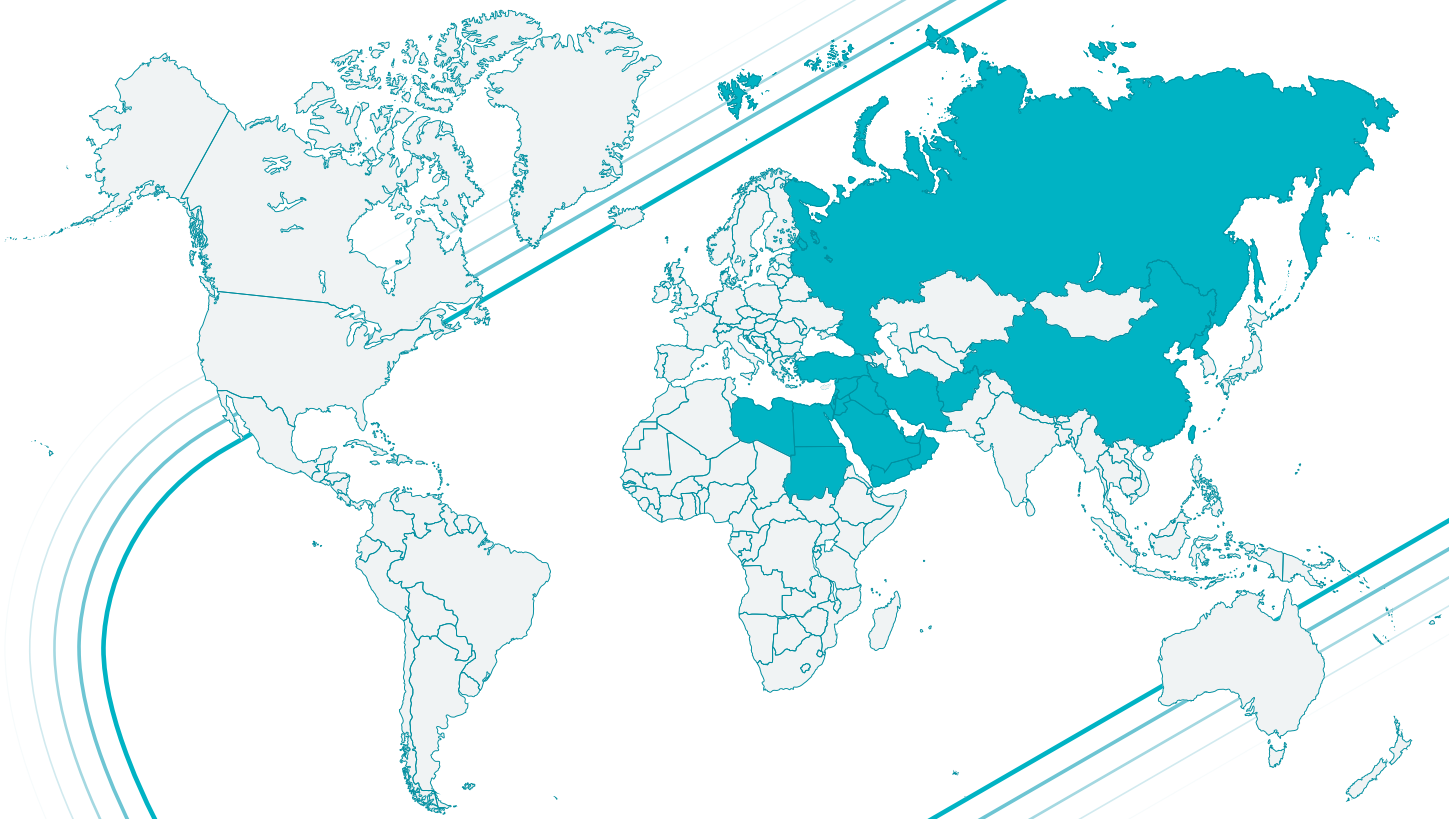
ESET od ponad 35 lat nieustannie rozwija technologię cyberochrony. Nasz sukces opiera się na podejściu „prevention-first" – strategii zapobiegania wspieranej przez sztuczną inteligencję i wzmacnianej wiedzą ekspertów. Trzonem naszych działań jest **unikalna technologia Threat Intelligence, oparta na rozbudowanej sieci R&D, kierowanej przez uznanych na świecie badaczy.**

Poświęcamy czas, aby dobrze zrozumieć pojawiające się cyberzagrożenia, dlatego potrafimy skutecznie się przed nimi bronić.

Niezależnie od poziomu zaawansowania Twoich obecnych rozwiązań CTI, integracja **ESET wnosi realną wartość dodaną**. Nasze kompleksowe źródła danych o zagrożeniach, raporty APT i raporty dotyczące cyberprzestępczości pozwalają wyprzedzać zagrożenia i wzmacniają Twoją ochronę dzięki praktycznym spostrzeżeniom i najnowszym badaniom.

Wykorzystaj unikalną telemetrię ESET

Globalna obecność ESET, budowana przez dekady, zapewnia nam bogatą i zróżnicowaną bazę danych wywiadowczych, pochodzącą z milionów źródeł. W przeciwieństwie do konkurentów, nasza telemetria jest szczególnie silna w regionach uznawanych za „bardziej interesujące" z geopolitycznego punktu widzenia w kontekście obrony cybernetycznej. To unikalne pokrycie przekłada się bezpośrednio na wyższej jakości dane wywiadowcze. Korzystając z telemetrii ESET, zyskujesz dostęp do wartościowych, praktycznych informacji, które zwiększają skuteczność wykrywania zagrożeń i reagowania na incydenty.

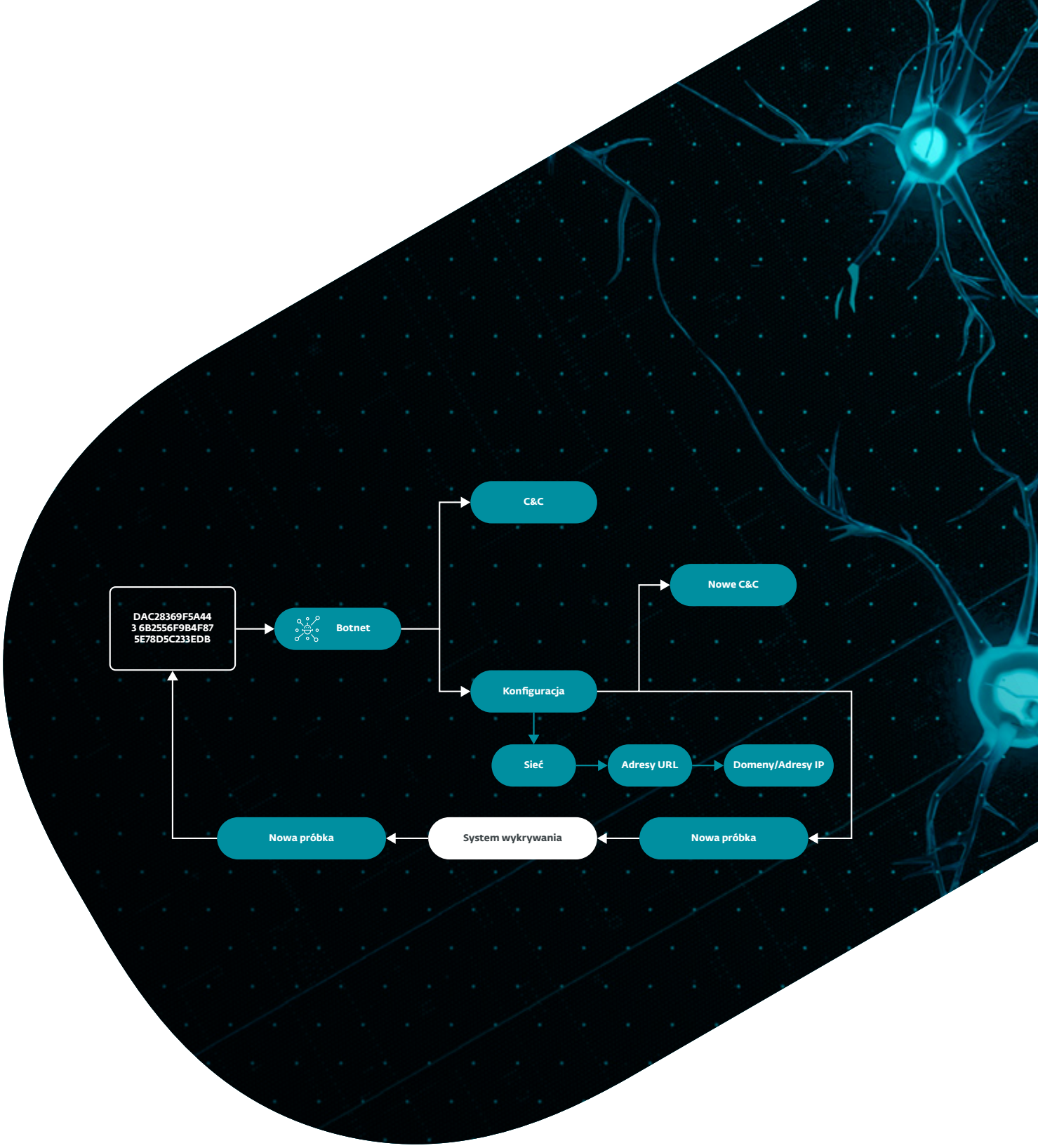


eset Cybersecurity
Progress. Protected.

Unikalne, wzbogacone dane wywiadowcze dostarczające praktycznych informacji

Threat intelligence to nie tylko zbieranie wskaźników i ich prezentacja — ESET idzie znacznie dalej. Wykorzystujemy zaawansowane technologie i szeroką wiedzę specjalistyczną, aby przetwarzać i wzbogacać nasze dane wywiadowcze, zapewniając, że przynoszą one realną wartość dla Twojej organizacji.

1. **Kompleksowa telemetria:** Nasze działania rozpoczynają się od szerokiego zakresu danych telemetrycznych generowanych przez ESET LiveSense -naszą wielowarstwową technologię zabezpieczeń zintegrowaną z platformą ESET PROTECT. Zapewnia to szeroką i dogłębną kolekcję danych z różnorodnych źródeł.
2. **Zróżnicowane metody gromadzenia danych:** Oprócz LiveSense wykorzystujemy różnorodne metody zbierania i monitorowania informacji, w tym honeypot'y, sensory, zasoby OSINT, indeksowanie sieci (w tym także deep web) oraz śledzenie zagrożeń. W rezultacie uzyskujemy znaczną ilość wysokiej jakości danych.
3. **Zaawansowane przetwarzanie:** Po zebraniu wszystkie dane przetwarzane są za pomocą naszych systemów, które wykorzystują sztuczną inteligencję do klasyfikowania i analizowania informacji. Dzięki temu wyodrębniane są tylko najbardziej istotne i przydatne dane wywiadowcze.
4. **Ekspercka analiza:** Oprócz automatycznego przetwarzania, kluczową rolę odgrywa nasz zespół wykwalifikowanych analityków i badaczy ds. wywiadu zagrożeń. Nieustannie badają i analizują działania różnych grup zagrożeń, ich motywacje, taktyki, techniki i procedury (TTPs), a także wykorzystywane narzędzia. Ta ludzka weryfikacja pozwala nam osiągnąć dodatkową warstwę precyzji w naszych danych wywiadowczych, wykraczając poza możliwości samego uczenia maszynowego i automatyzacji.



Próbki, które otrzymujemy za pośrednictwem telemetrii, poddawane są dogłębnej analizie behawioralnej i strukturalnej. Proces ten dostarcza dodatkowych użytecznych wskaźników, co jeszcze bardziej wzbogaca nasze dane wywiadowcze o zagrożeniach. Poprzez skrupulatne badanie każdej próbki uzyskujemy cenne informacje, które podnoszą ogólną jakość i skuteczność naszego wywiadu, zapewniając bardziej kompleksowe zrozumienie krajobrazu zagrożeń.

Najwyższe bezpieczeństwo dzięki szczegółowym raportom APT

Nasze raporty APT, napisane zwięzłym i praktycznym językiem, pomagają wzmocnić bezpieczeństwo Twojej organizacji. Zawierają szczegółowe informacje o kampaniach malware, metodach dystrybucji i zaangażowanych grupach. Uzyskaj dostęp do naszego serwera MISP i narzędzia AI Advisor oraz zaplanuj sesje na żywo z najlepszymi ekspertami ds. wywiadu zagrożeń ESET, aby uzyskać kompleksowe, praktyczne informacje.

NAJLEPSZE WYNIKI NASZYCH BADAŃ NA WYCIĄGNIĘCIE RĘKI

Nasz zespół badawczy jest dobrze znany w branży bezpieczeństwa cyfrowego, m.in. dzięki nagradzanemu blogowi WeLiveSecurity. Na blogu dostępne są zarówno znakomite analizy, jak i podsumowania aktywności APT z dużo bardziej szczegółowymi informacjami. Klienci ESET otrzymują ekskluzywny, wcześniejszy dostęp do wszystkich treści publikowanych na WeLiveSecurity.

PRAKTYCZNE, WYSELEKCJONOWANE TREŚCI

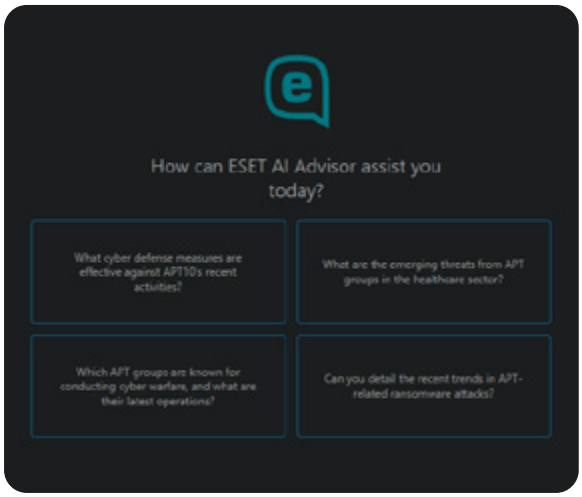
Raporty dostarczają szerokiego kontekstu dotyczącego bieżących wydarzeń i ich przyczyn. Dzięki temu organizacje mogą z wyprzedzeniem przygotować się na potencjalne zagrożenia. Co istotne, nasi eksperci dbają o to, aby treści były napisane w sposób zrozumiały i przystępny.

KLUCZOWE DECYZJE PODEJMUJ SZYBKO

Wszystko to pomaga organizacjom podejmować kluczowe decyzje i zapewnia strategiczną przewagę w walce z cyberprzestępczością. Zapewnia lepsze zrozumienie tego, co dzieje się po „ciemnej stronie Internetu", oraz dostarcza istotnego kontekstu umożliwiając szybką wewnętrzną reakcję w Twojej organizacji.

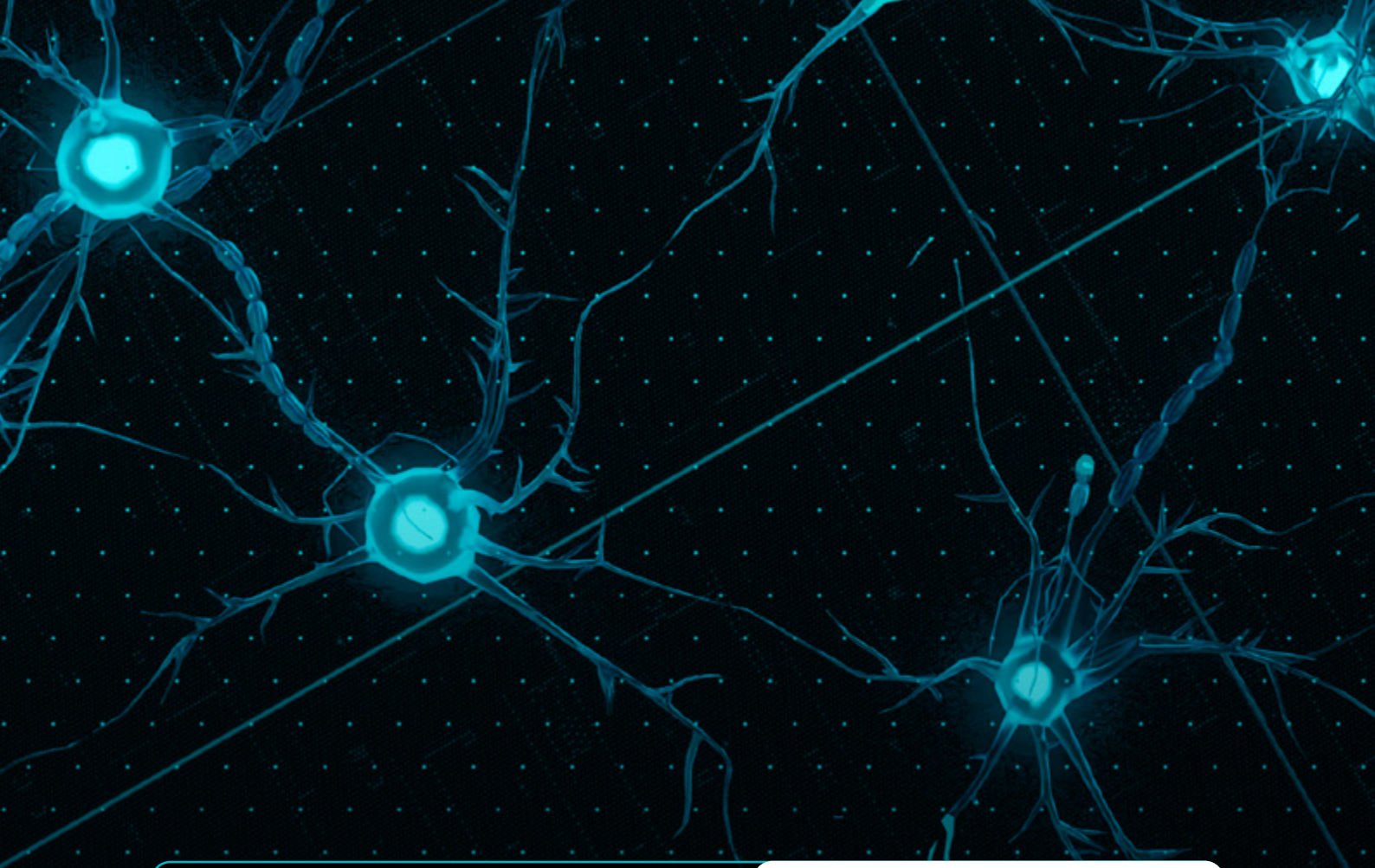
DOSTĘP DO ANALITYKA ESET

Każdy klient, który zamówi pakiet APT Reports Premium, otrzymuje również dostęp do analityka ESET przez maksymalnie cztery godziny miesięcznie. To okazja do pogłębionej analizy wybranych tematów i wsparcia w rozwiązywaniu ewentualnych problemów.



ESET AI ADVISOR

ESET AI Advisor wykorzystuje zaawansowaną wiedzę specjalistyczną z zakresu AI i APT, aby na żądanie dostarczać informacje i środki ochrony przed cyberatakami. ESET AI Advisor jest dostępny w formie chatbota, który odpowiada na pytania dotyczące bezpieczeństwa, udostępnia podsumowania działań grup APT, kompiluje wskaźniki kompromitacji (IoC) i techniki, taktyki oraz procedury (TTP), a także generuje reguły YARA w celu szybkiego zrozumienia i zapobiegania zagrożeniom.



		APT Reports	APT Reports Advanced	APT Reports Ultimate
Podsumowania dwutygodniowej aktywności	Raporty podsumowujące aktywność wszystkich objętych monitoringiem grup APT – dwa razy w miesiącu	✓	✓	✓
Raporty analizy zagrożeń	Regularne lub spersonalizowane analizy techniczne dominujących zagrożeń (~30 raportów rocznie)	✓	✓	✓
Przegląd miesięczny	Miesięczne zestawienie informacji z przeglądem zagrożeń	✓	✓	✓
Miesięczny skrót	Indeks i skrót najważniejszych raportów i wydarzeń z danego miesiąca	✓	✓	✓
Wstępny dostęp do WeLiveSecurity	Wczesny dostęp do raportów zagrożeń i wybranych artykułów z WeLiveSecurity	✓	✓	✓
APT IOC Feed	Pełny dostęp do STIX/TAXII zawierającego IOC z raportów APT	✓	✓	✓
Dostęp do serwera MISP	Pełny dostęp do serwera ESET MISP zawierającego wszystkie informacje dostępne w raportach	✗	✓	✓
ESET AI Advisor	Dostęp do narzędzia ESET AI Advisor zapewniającego wgląd i podsumowania dostępnych raportów APT	✗	✓	✓
Dostęp analityka	Dostęp analityka za pośrednictwem różnych platform, takich jak MS Teams i poczta e-mail, ograniczony do czterech godzin miesięcznie (czas nie przechodzi na kolejny miesiąc i obejmuje również przygotowanie)	✗	✗	✓

Od wskaźników do wywiadu: przechytrz cyberprzestępców

Raporty ESET Threat Intelligence eCrime dostarczają dogłębnych informacji na temat oprogramowania ransomware i szeroko pojętej cyberprzestępczości. Dzięki nim zyskasz wgląd w narzędzia, infrastrukturę i strategie monetyzacji stosowane przez atakujących, poparte globalnymi badaniami i telemetrią ESET. Wyjdź poza wskaźniki IoC i zyskaj dostęp do informacji kontekstowych, które wzmacniają proaktywną obronę i strategiczne podejmowanie decyzji.

Co wyróżnia raporty ESET eCrime

PROAKTYWNA OBRONA

Zdobądź informacje nie tylko o grupach cyberprzestępczych, ale także o podmiotach powiązanych, które faktycznie przeprowadzają ataki. Zobacz, jak działają, i przewiduj ich kolejne posunięcia, aby zawsze być o krok przed nimi.

EFEKTYWNOŚĆ OPERACYJNA

Wykorzystaj jasne, wyselekcjonowane informacje z rzeczywistych incydentów i przebij się przez szum informacyjny. Zapewnij swojemu zespołowi łatwiejsze wykrywanie zagrożeń, szybsze reagowanie i skupienie się na tym, co najważniejsze.

WYJĄTKOWA WIDOCZNOŚĆ

Wyjdź poza publiczne źródła informacji o zagrożeniach. Zyskaj wgląd w taktyki monetyzacji, infrastrukturę i zachowania podmiotów powiązanych w praktyce – wszystko to poparte globalną telemetrią i badaniami ESET.

		Raporty eCrime	Raporty eCrime Advanced
Podsumowanie działalności CO MIESIĄC	○ Najnowsze kampanie ransomware i infostealer w postaci przejrzystych, strategicznych informacji ○ Kto jest celem, jak przebiegają ataki, co poszło nie tak ○ Kluczowe wnioski, wskaźniki IOC i wytyczne dotyczące wzmocnienia odporności	✓	✓
Analiza techniczna CO MIESIĄC	○ Dogłębna analiza konkretnych podmiotów stanowiących zagrożenie (np. FIN7) ○ Pełny łańcuch ataku: od początkowego dostępu do kradzieży danych ○ Taktyki atakujących, narzędzia, infrastruktura, mapowanie MITRE ATT&CK®, wskaźniki IOC	✓	✓
Miesięczny przegląd CYKLICZNIE	○ Przegląd ostatnich działań ransomware/infostealerów przygotowany dla kadry kierowniczej ○ Kluczowe trendy, godne uwagi incydenty, pojawiające się zagrożenia ○ Pomoc kierownictwu przy ustalaniu ryzyks i ustalaniu priorytetów bez technicznej złożoności	✓	✓
eCrime Feed	○ Najświeższe i wyselekcjonowane wskaźniki IOC dotyczące gangów ransomware, ich podmiotów stowarzyszonych i kampanii infostealerów ○ Dostępne w standardowym formacie STIX/TAXII	✓	✓
ESET AI Advisor	○ Wykorzystanie informacji eCrime do udzielania odpowiedzi na pytania związane z zagrożeniami ○ Pomoc w interpretacji incydentów i zachowań atakujących ○ Natychmiastowy dostęp do informacji o zagrożeniach dla zespołów i decydentów	✗	✓
Dostęp do serwera MISP	○ Bezpośrednia integracja z wyselekcjonowanymi informacjami o zagrożeniach ○ Automatyczne pobieranie wskaźników IOC w celu wzbogacenia zabezpieczeń ○ Usprawnienie przepływu pracy, szybsze wykrywanie i wsparcie w reagowaniu na incydenty	✗	✓

Przejrzyste i zwięzłe źródła danych

Zyskaj szerszy wgląd w krajobraz zagrożeń dzięki unikalnej telemetrii ESET. Oferujemy starannie wyselekcjonowane kanały danych w formatach JSON i STIX 2.1, które łatwo integrują się z narzędziami SIEM, TIP i SOAR. W przeciwieństwie do wielu dostawców TI, przywiązujemy ogromną wagę do jakości – nasze kanały są dokładnie filtrowane i oceniane pod kątem trafności. Dzięki temu możliwe są automatyczne działania systemów zabezpieczeń oraz pełny obraz zagrożeń dla analityków wywiadu.

- Bogate w metadane, szczegółowe i selekcjonowane dane o bardzo niskim poziomie fałszywych alarmów
- Mała objętość danych, wysoka trafność, brak duplikatów, ocena wiarygodności
- Wynik zaawansowanego filtrowania z wnioskami badaczy ESET
- Lider rynku zakresie danych botnetowych
- Zautomatyzowane procesy i integracje oszczędzają czas pracy analityków
- Kanały w czasie rzeczywistym – wyłącznie aktualne i istotne wskaźniki zagrożeń (IOC)

MALICIOUS DATA FEED

Informacje w czasie rzeczywistym na temat nowo wykrytych próbek złośliwego oprogramowania, ich cech charakterystycznych i wskaźników IoC. Kanał zawiera sygnatury plików, sygnatury czasowe i typy zagrożeń, które pomagają blokować złośliwe pliki, zanim spowodują one jakiekolwiek szkody.

RANSOMWARE FEED

Dane w czasie rzeczywistym dotyczące aktywnych rodzin oprogramowania ransomware i najczęściej występujących próbek. Umożliwiają proaktywne blokowanie, aby zapobiegać naruszeniom bezpieczeństwa i kosztownym zakłóceniom.

BOTNET FEED

Kanał obsługiwany jest przez narzędzie ESET do śledzenia botnetów. Zawiera on trzy podkanały: botnet, C&C i cele. Prezentuje szczegóły wykrywania, skróty plików, znaczniki czasu ostatniej komunikacji, pobrane pliki, adresy IP, protokoły i informacje docelowe.

APT IOC FEED

Wgląd w zaawansowane, trwałe zagrożenia na podstawie badań ESET. Eksportowane z wewnętrznego serwera MISP firmy ESET i dostosowane do raportów APT. Dostępne jako część raportów lub jako samodzielny feed.

PUA ADWARE FEED

ESET ma ponad 20 lat doświadczenia w klasyfikowaniu PUA (potencjalnie niechcianych aplikacji), dzięki czemu charakteryzuje się niezrównaną głębią i precyzją. Kanały Adware dostarczają w czasie rzeczywistym informacje o aktywnym adware i podobnych zagrożeniach. Pozwala to na proaktywne blokowanie przed wystąpieniem skutków.

PUA DUAL-USE APP FEED

Kanał śledzi legalne narzędzia (np. RMM) wykorzystywane w niewłaściwy sposób przez atakujących, co pomaga wyprzedzać nadużycia i jednocześnie zredukować szum dzięki dostosowanym, niskoredundantnym danym.

DOMAIN FEED

Kanał dostarcza dane dotyczące złośliwych domen, w tym nazwę domeny, adres IP i powiązaną datę. Domeny są klasyfikowane według stopnia zagrożenia, co pozwala nadać priorytet takim działaniom, jak blokowanie domen wysokiego ryzyka.

URL FEED

Wyselekcjonowany kanał zawierający konkretne adresy URL wraz ze szczegółowymi informacjami o konkretnych adresach i domenach je hostujących. Zawiera wyłącznie wyniki o wysokim stopniu pewności, poparte jasnymi, zrozumiałymi wyjaśnieniami dotyczącymi oznaczonych adresów URL.

IP FEED

Otrzymuj przydatne dane o złośliwych adresach IP. Struktura odzwierciedla kanały domen i adresów URL. Wykorzystaj ją do identyfikacji typowych zagrożeń, blokowania adresów IP o wysokim stopniu zagrożenia, monitorowania adresów o niższym ryzyku i dalszego badania przy użyciu dodatkowych danych w celu oceny potencjalnych szkód.

ANDROID THREATS FEED

Ten kanał dostarcza informacji w czasie rzeczywistym o powszechnych zagrożeniach Androida i ich wskaźnikach IoC , umożliwiając proaktywne blokowanie. Stworzony na podstawie telemetrii ESET, aktualizuje się w czasie niemal rzeczywistym z codzienną deduplikacją.

ANDROID INFOSTEALER FEED

Specjalistyczny kanał informacyjny poświęcony zagrożeniom dla Androida, zawierający szczegółowe informacje na temat aktualnych próbek programów do kradzieży danych oraz powiązanych danych. Zyskaj wgląd w aktywne rodziny programów i proaktywnie blokuj je, zanim wyrządzą szkody.

SCAM URL FEED

Chroń się przed oszustwami dzięki danym w czasie rzeczywistym o fałszywych stronach. Nasz kanał obejmuje sklepy elektroniczne, oszustwa inwestycyjne, oszustwa randkowe i kryptowalutowe. Dane z wszystkich źródeł URL ESET, aktualizowane niemal w czasie rzeczywistym i deduplikowane co 24 godziny.

CRYPTOSCAM FEED

Bądź o krok przed oszustwami kryptowalutowymi – dane w czasie rzeczywistym o domenach, adresach URL i powiązanych informacjach. Źródłem są dane telemetryczne ESET, które pomogą Ci proaktywnie blokować zagrożenia i chronić Twoje zasoby.

MALICIOUS EMAIL ATTACHMENTS FEED

E-mail to jeden z głównych wektorów ataku. Nasz kanał dostarcza danych w czasie rzeczywistym na temat złośliwych załączników e-mail pochodzących z rozległej telemetrii skanowania e-maili ESET.

PHISHING URL FEED

Informacje w czasie rzeczywistym o aktywnych phishingowych adresach URL z dedykowanej bazy danych ESET. Kanał ten jest ciągle aktualizowany i codziennie deduplikowany, co pomaga wykrywać i blokować fałszywe strony internetowe, zanim naruszą one poufne dane.

SMISHING FEED

Zapewnia aktualne informacje na temat phishingu SMS-owego (smishing), w tym domen, adresów URL i powiązanych wskaźników. Dane pochodzą z obszernego systemu telemetrycznego ESET i są aktualizowane niemal w czasie rzeczywistym z codzienną deduplikacją.

SMS SCAM FEED

Chroń się przed oszustwami SMS dzięki danym o złośliwych domenach i URL-ach. Kanał jest aktualizowany niemal w czasie rzeczywistym i codziennie deduplikowany – pozwala identyfikować i blokować zaawansowane zagrożenia.

ECRIME FEED

Uzyskaj jasne, przydatne dane dotyczące cyberprzestępczości, również tej opartej na złośliwym oprogramowaniu. Monitoruj wszystko – od gangów ransomware i ich powiązanych podmiotów po kampanie infostealerów. Niech Twój zespół przejdzie od reagowania do proaktywnej ochrony organizacji.

Poznaj moc ESET Threat Intelligence

Umów się na prezentację i zobacz, jaką wartość ESET Threat Intelligence może wnieść do Twojej organizacji. 100% wskaźnik odnowień to dowód skuteczności naszych rozwiązań. Pokażemy Ci, jak możemy wzmocnić Twoje cyberbezpieczeństwo.

Nie jesteś jeszcze gotowy na prezentację?

Zacznij od utworzenia konta podglądowego w portalu ESET Threat Intelligence i zapoznaj się z kanałami danych i raportami APT.

ESET Cybersecurity
Progress. Protected.

To jest ESET

Proaktywna ochrona. Minimalizuj ryzyko dzięki podejściu prewencyjnemu.

Bądź o krok przed znanymi i pojawiającymi się cyberzagrożeniami, takimi jak ukierunkowane ataki, zagrożenia typu zero-day, oprogramowanie ransomware, phishing i inne. To możliwe, dzięki naszemu podejściu opartemu na sztucznej inteligencji, które stawia na pierwszym miejscu zapobieganie. ESET łączy sztuczną inteligencję i ludzką wiedzę specjalistyczną, aby zapewnić łatwą i skuteczną ochronę.

Skorzystaj z najlepszych w swojej klasie, opartych na badaniach naukowych zabezpieczeniach, popartych ponad 30-letnim doświadczeniem w zakresie globalnej analizy cyberzagrożeń. Rozległa sieć badawczo-rozwojowa, kierowana przez uznanych w branży naukowców, stanowi podstawę naszej wielokrotnie nagradzanej platformy cyberbezpieczeństwa opartej na chmurze.

Rozwiązania ESET są wysoce konfigurowalne, obejmują lokalne wsparcie techniczne i mają minimalny wpływ na wydajność.

ESET chroni Twój biznes, dzięki czemu możesz w pełni wykorzystać możliwości nowoczesnych technologii.

ESET W LICZBACH

1 mld+
chronionych użytkowników Internetu

500 tys.+
klientów biznesowych

176
krajów i terytoriów

11
globalnych centrów badawczo-rozwojowych

WYBRANI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

chroniony przez ESET od 2017 roku
ponad 9 500 stacji roboczych

Canon
Canon Marketing Japan Group

chroniony przez ESET od 2016 roku
ponad 23 000 stacji roboczych

T . .

Partner ISP w zakresie bezpieczeństwa od 2008 r.
2 miliony klientów

WYRÓŻNIENIA

SE LABS ®
AWARDS
Enterprise Endpoint (Windows)
WINNER 2025

Zwycięzca nagród SE LABS Awards 2025 w kategorii **najlepszego rozwiązania dla przedsiębiorstw i najlepszego rozwiązania dla małych firm**.

Gartner
Peer Insights
Customers' Choice 2026

Wyróżniony jako **Wybór Konsumentów** w serwisie Gartner® Peer Insights™. **„Voice of the Customer" Endpoint Protection Platforms** report 2026

FROST & SULLIVAN

Uznany za **lidera** we Frost Radar: Endpoint Security 2025, wykazując się doskonałością w zakresie wzrostu i innowacji