



ENJOY SAFER TECHNOLOGY™

ESET THREAT INTELLIGENCE

Rozszerz wiedzę o bezpieczeństwie Twojej firmowej sieci o informację z globalnej cyberprzestrzeni

Dla dużych firm sektora bankowego, energetycznego lub wojskowego, kluczowe jest, by wiedzieć o wszystkich możliwych wektorach ataku na swoją sieć i uzyskać te informacje nie tylko ze swoich źródeł. Wszystko po to, by móc stosownie odpowiadać na stale zmieniającą się charakterystykę bezpieczeństwa swojego środowiska sieciowego. Ataki ukierunkowane, zagrożenia APT, exploity 0-day oraz działanie botnetów są trudne do wykrycia przez inżynierów posiadających dostęp wyłącznie do informacji z wnętrza sieci firmowej.

ESET Threat Intelligence wypełnia lukę pomiędzy informacjami uzyskanymi przez inżynierów z wnętrza sieci firmowej, a danymi zbieranymi przez system ESET z całego świata. ESET Threat Intelligence wykorzystuje informacje gromadzone przez ponad 100 milionów stacji roboczych na całym świecie, które wysyłają zebrane informacje do chmurowego systemu reputacyjnego ESET LiveGrid®. Następnie dane te są przesyłane do centrów Research & Development, zlokalizowanych na całym świecie, gdzie eksperci zajmują się dogłębną analizą otrzymanych danych. Dzięki temu ESET Threat Intelligence dostarcza klientom ESET unikatową wiedzę, która pomaga zrozumieć i zarządzać ryzykiem ataku na swoją sieć firmową, umożliwiając równocześnie poprawę skuteczności działania swoich zabezpieczeń.

Raport dotyczący zagrożeń ukierunkowanych

Informuje o potencjalnych atakach, które znajdują się dopiero w fazie opracowywania lub o trwających właśnie atakach ukierunkowanych przeciwko Twojej organizacji. Reguły wyszukiwania mogą być ustalone przy użyciu języka YARA – w ten sposób uzyskasz dokładnie te informacje, których szukasz. Bazując na raporcie, otrzymasz istotne informacje nt. potencjalnych lub trwających właśnie ataków, w tym m.in. częstotliwości takich ataków, adresach URL zawierających złośliwy kod, danych dotyczących późniejszej aktywności zagrożeń w systemie, miejscach, w których zostały one wykryte i wiele więcej.

System ochrony oparty na chmurze

System ochrony przed złośliwym oprogramowaniem ESET jest jedną z kilku technologii ESET, opartych na chmurowym systemie reputacji plików ESET LiveGrid. Potencjalnie niebezpieczne pliki i programy są monitorowane i zgłaszane do laboratorium ESET za pośrednictwem ESET LiveGrid. Następnie podejrzana zawartość jest automatycznie weryfikowana m.in. w procesach sandboxingu i analizy behawioralnej.



Podejrzana i nieznaną dotąd aplikacja czy zagrożenie są monitorowane i przesyłane do ESET za pomocą ESET LiveGrid.



Zebrane próbki są poddawane sandboxingowi i analizie behawioralnej, a pozytywne zidentyfikowanie złośliwej zawartości lub aktywności skutkuje automatyczną detekcją i blokadą pliku lub aplikacji przez programy ESET na całym świecie.



Klienci uzyskują informację o detekcji za pomocą systemu ESET LiveGrid bez konieczności czekania na kolejną aktualizację.

Reputacja plików

Podczas sprawdzania pliku lub adresu URL, rozwiązanie ESET najpierw sprawdza lokalną pamięć dla znanych zagrożeń i białą listę plików, co poprawia wydajność skanowania. Następnie rozwiązanie ESET wysyła zapytanie o reputację pliku do ESET LiveGrid.



System ESET LiveGrid zbiera informacje o zagrożeniach od milionów użytkowników ESET na całym świecie, ustalając m.in. datę utworzenia pliku i powszechność jego występowania.



Nieznanne zagrożenia są przysyłane do laboratoriów ESET w celu dalszej analizy.



System automatycznie ocenia dane i zapewnia szybką reakcję, wykorzystując do tego celu białe i czarne listy plików.

Raport aktywności botnetów

Regularne raporty dostarczają dane ilościowe o zidentyfikowanych rodzinach złośliwego oprogramowania i zagrożeniach, których celem jest przyłączenie kolejnych urządzeń do sieci botnet. Klasyfikacja odbywa się według typu zagrożenia. Raport zawiera listę znanych serwerów C&C, zarządzających botnetami, jak również listę celów danego zagrożenia.

Automatyczna analiza próbek

Ważne, byś wiedział, co dzieje się w sieci firmowej – czy podejrzany plik jest rzeczywiście zagrożeniem, czy też nie – aby móc odpowiednio zareagować. Raport dotyczący przesłanego pliku lub jako hash, dostarcza cennych danych włącznie z liczbą detekcji na całym świecie, informacją kiedy próbka została zaobserwowana po raz pierwszy, identyfikacją geograficzną występowania, podpisem cyfrowym i innymi, pomagając w ten sposób podjąć kluczowe decyzje dotyczącej reakcji na dane zagrożenie.

Dodatkowa warstwa bezpieczeństwa, nawet jeśli nie jesteś klientem ESET

Eksperci ds. zabezpieczeń IT zalecają łączenie różnych metod i zabezpieczeń w celu zminimalizowania potencjalnego ryzyka infekcji lub ataku, które mogą wynikać z korzystania z rozwiązania zabezpieczającego jednego producenta.

ESET Threat Intelligence nie wymaga wdrożenia rozwiązań ESET w sieci firmowej. Oznacza to, że może on być stosowany przez klientów nie posiadających rozwiązań ESET jako dodatkowa warstwa zabezpieczeń, działająca jako system wczesnego ostrzeżenia przed nadciągającymi zagrożeniami czy atakami ukierunkowanymi, o których dostawca rozwiązań ochronnych, zastosowanych w danej firmie, może nie widzieć. Alternatywnie, system ten może być stosowany w celu uzyskania dodatkowych informacji nt. konkretnego ataku, który został już wykryty w sieci firmowej, by następnie umożliwić podjęcie odpowiedniej decyzji dotyczącej ochrony sieci.

Sygnatury DNA

To kompletna informacja nt. złośliwego zachowania pliku i jego charakterystyki. Chociaż złośliwy kod zagrożenia może zostać łatwo zmodyfikowany lub ukryty, jego zachowanie z pewnością nie ulegnie drastycznej zmianie. W ten sposób ESET identyfikuje nieznaną do tej pory zagrożenie, które zawierają „geny” charakteryzujące wykryte wcześniej zagrożenia.



Zaawansowana heurystyka proaktywnie wykrywa niezidentyfikowane do tej pory zagrożenia.

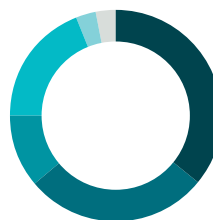


ESET wykrywa zagrożenia w oparciu o ich zachowanie, demaskując je na podstawie podejmowanej przez nie aktywności.



Zaawansowane techniki, w tym sygnatury DNA, identyfikują zagrożenia w oparciu o strukturę ich kodu.

64% klientów ESET odnotowało zwrot z inwestycji (wdrożenia ESET) w mniej niż 6 miesięcy, a 75% klientów w ciągu 9 miesięcy

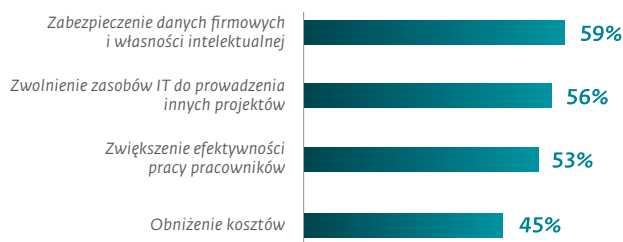


0 - 3 miesiące:	36%
4 - 6 miesięcy:	28%
7 - 9 miesięcy:	11%
10 - 12 miesięcy:	19%
13 - 18 miesięcy:	3%
18 miesięcy lub dłużej:	3%



Ankieta przeprowadzona przez TechValidate wśród 522 użytkowników rozwiązań ESET, którym zostało zadane pytanie: „Proszę określić jak długo trwał zwrot z inwestycji zakupu rozwiązania bezpieczeństwa ESET?”.

Jakie korzyści zauważyli klienci po wdrożeniu rozwiązań ESET?



Ankieta przeprowadzona przez TechValidate wśród 1213 użytkowników rozwiązań zabezpiecz ESET.



ESET otrzymał najwięcej wyróżnień „Advanced+” wygrywając w testach ochrony proaktywnej AV-Comparatives



ESET otrzymał wyróżnienie „Advanced+” wygrywając w teście ochrony w czasie rzeczywistym organizacji AV-Comparatives



ESET 13 lat nieprzerwanie zdobywa nagrody VB100 i jest producentem, który posiada rekordową liczbę 100 wyróżnień VB100, przyznanych w testach zrealizowanych przez niezależną organizację badawczą Virus Bulletin



ESET uzyskuje najwyższe oceny w testach wykrywających spam organizowanych przez Virus Bulletin