

Operacje zabezpieczające oparte na sztucznej inteligencji

Szybsze wykrywanie i eliminowanie zagrożeń oraz zapobieganie zagrożeniom

Streszczenie

Metody włamań zmieniają się coraz szybciej, ale cel wdrażanych zabezpieczeń pozostaje ten sam. Aby ograniczyć ryzyko ataków, należy zapobiec jak największej liczbie cyberzagrożeń, wykrywając i eliminując włamania jak najszybciej, aby zminimalizować poniesione szkody i koszty.

W obliczu niedoboru personelu IT przedsiębiorstwa coraz częściej wdrażają na całej cyfrowej powierzchni ataku oraz w ramach całego cyklu życia cyberataku opracowane przez Fortinet mechanizmy sztucznej inteligencji (AI) oraz inne zaawansowane technologie, aby ograniczyć swoją podatność na cyberzagrożenia. Architektura Fortinet Security Fabric oferuje najbardziej wszechstronną, zintegrowaną i zautomatyzowaną w branży platformę chroniącą przed cyberatakami.

61% przedsiębiorstw twierdzi, że bez zastosowania mechanizmów sztucznej inteligencji nie jest w stanie wykryć prób naruszenia bezpieczeństwa¹.

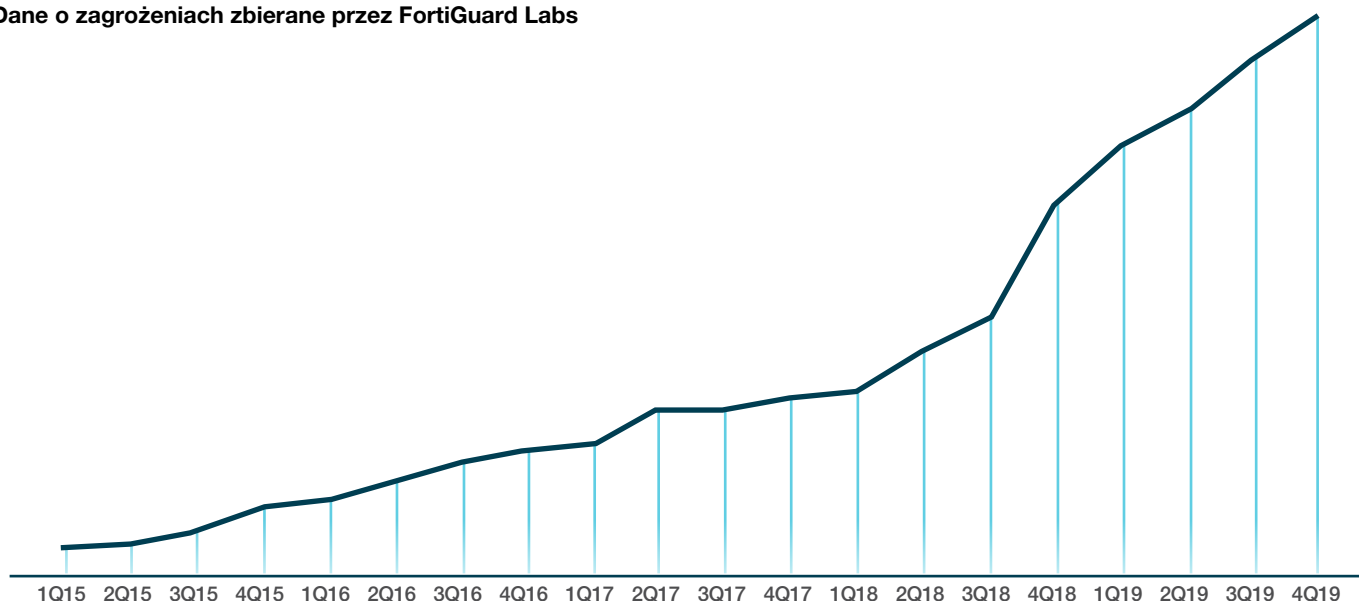
Zwiększenie liczby, dynamiki i złożoności metod włamań

W latach 2018 – 2019 łączna ilość otrzymanych przez FortiGuard Labs informacji o zagrożeniach, w tym o nowych plikach, stronach internetowych, programach wykorzystujących luki w zabezpieczeniach i innych niebezpieczeństwach, wzrosła o 34% do 940 TB. Nie ulega zatem wątpliwości, że liczba zagrożeń w cyberprzestrzeni nadal rośnie wraz z rosnącą cyfrową powierzchnią ataku w większości przedsiębiorstw.

Rośnie również dynamika cyberataków. W 2019 r. średni cykl życia danego zagrożenia (od początkowego pojawienia się, poprzez szczytowe rozpowszechnienie, aż do pojawienia się nowego wariantu lub ataku) wynosił zazwyczaj nie więcej niż jeden miesiąc. Obecnie daje się zaobserwować istnienie dojrzałego cyberprzestępczego ekosystemu, w którym narzędzia takie jak zestawy programów wykorzystujących luki w zabezpieczeniach (eksploity), usługi MaaS (Malware-as-a-Service, złośliwe oprogramowanie jako usługa) lub boty do wynajęcia, drastycznie skróciły czas wdrożenia przez cyberprzestępców nowej metody ataku. Można wręcz stwierdzić, że zasadniczo ta cyberprzestępcza branża weszła w fazę elastycznego rozwoju i produkcji.

Jednocześnie wzrósł również stopień złożoności cyberataków, które nie ograniczają się już do ukierunkowanych ataków na infrastruktury całych krajów. Złośliwe działania podejmowane są we wszystkich aspektach obejmujących inżynierię społeczną, mechanizmy włamań oparte na otwartym kodzie źródłowym i różne inne innowacje, co prowadzi do pojawiania się zagrożeń, które coraz łatwiej mylą czujność użytkowników końcowych i są coraz trudniejsze do wykrycia przez tradycyjne zabezpieczenia.

Dane o zagrożeniach zbierane przez FortiGuard Labs



Rysunek 1: Liczba cyberzagrożeń w okresie od 1 kw. 2015 r. do 4 kw. 2019 r.

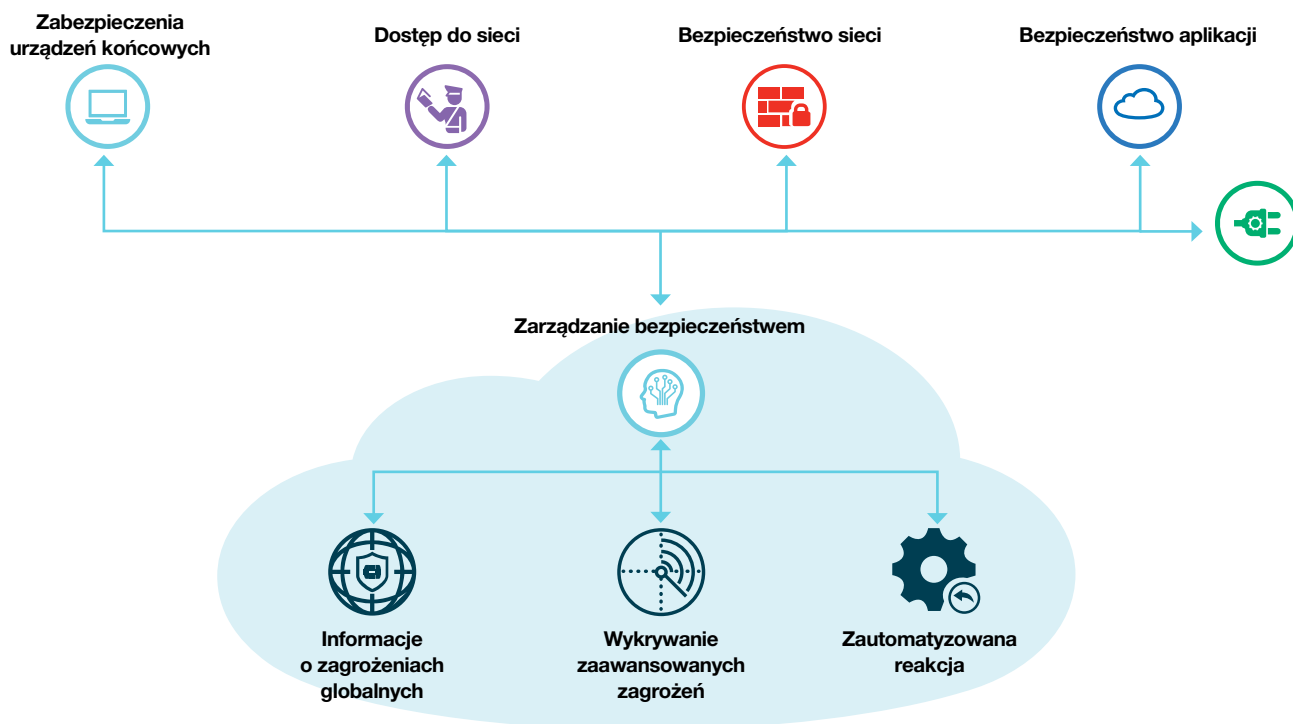
Moc obliczeniowa i sztuczna inteligencja pozwolą dotrzymać tempa zagrożeniom

Na szczęście postępy w zakresie sztucznej inteligencji i mocy obliczeniowej pozwalają (po przygotowaniu i wdrożeniu odpowiednich rozwiązań) dotrzymać kroku cyberprzestępcom. Niezależnie od tego, czy chodzi o zapewnienie aktualnych informacji o globalnych zagrożeniach, wykrywanie w przedsiębiorstwie incydentów dotyczących bezpieczeństwa, zanim staną się one naruszeniami, czy wdrożenie działań prewencyjnych w czasie rzeczywistym w ramach całej infrastruktury zabezpieczeń, mechanizmy sztucznej inteligencji mogą być i rzeczywiście są pomocne.

Operacje zabezpieczające oparte na sztucznej inteligencji

Fortinet stosuje i oferuje szereg zaawansowanych technologii, w tym mechanizmy sztucznej inteligencji, aby pomóc przedsiębiorstwom w wykrywaniu i szybkim reagowaniu na stale zmieniające się metody cyberwłamań oraz zapobieganiu takim włamaniom. Niektóre z tych technologii pomagają generować informacje o zagrożeniu, które są następnie przesyłane do wdrożonych przez klientów zabezpieczeń chroniących urządzenia końcowe, sieci, aplikacje i ścieżki ataku w chmurze. Inne technologie są natomiast wdrażane w przedsiębiorstwach w celu dalszego poszukiwania zagrożeń ewentualnie niewykrytych przez wdrożone zabezpieczenia oraz szybszego reagowania na zaistniałe incydenty. Wiele technologii można też wdrożyć w całym przedsiębiorstwie, często w trybie blokowania, aby zapobiegać atakom w czasie rzeczywistym.

Powyższe rozwiązania można stosować w różnych kombinacjach, aby przygotować skoordynowaną obronę przed cyberprzestępcami w całym cyklu życia cyberataku. Taka kompleksowa ochrona zapewnia przedsiębiorstwom wiele możliwości powstrzymania cyberzagrożeń na różnych etapach, zanim dojdzie do naruszenia bezpieczeństwa danych lub innego znaczącego narażenia na szwank działalności operacyjnej.



Rysunek 2. Mechanizmy sztucznej inteligencji obsługują wiele funkcji Fortinet w zakresie wykrywania i eliminowania zagrożeń oraz zapobiegania zagrożeniom.

Sztuczna inteligencja a zapobieganie zagrożeniom

Rozwiązania Fortinet zapewniają niezależnie i niezmiennie najlepszą ochronę urządzeń końcowych, sieci, aplikacji i chmury i obejmują platformę zabezpieczającą urządzenia końcowe FortiClient (EPP), zaporę następnej generacji FortiGate (NGFW), bezpieczną bramę poczty e-mail FortiMail (SEG) oraz zaporę aplikacji WWW FortiWeb (WAF).

Wszystkie te produkty korzystają z danych o zagrożeniach przekazywanych przez FortiGuard Labs — globalną, multidyscyplinarną grupę badającą zagrożenia. W kontekście ponad dziesięciu różnych obszarów cyberbezpieczeństwa FortiGuard Labs dysponuje kompleksowym przeglądem sytuacji w zakresie cyberzagrożeń opartym na proaktywnie zbieranych we własnym zakresie informacjach o zagrożeniach, informacjach pochodzących od ponad dwustu międzybranżowych partnerów oraz danych z globalnej sieci sond obejmującej ponad 5 mln urządzeń³.

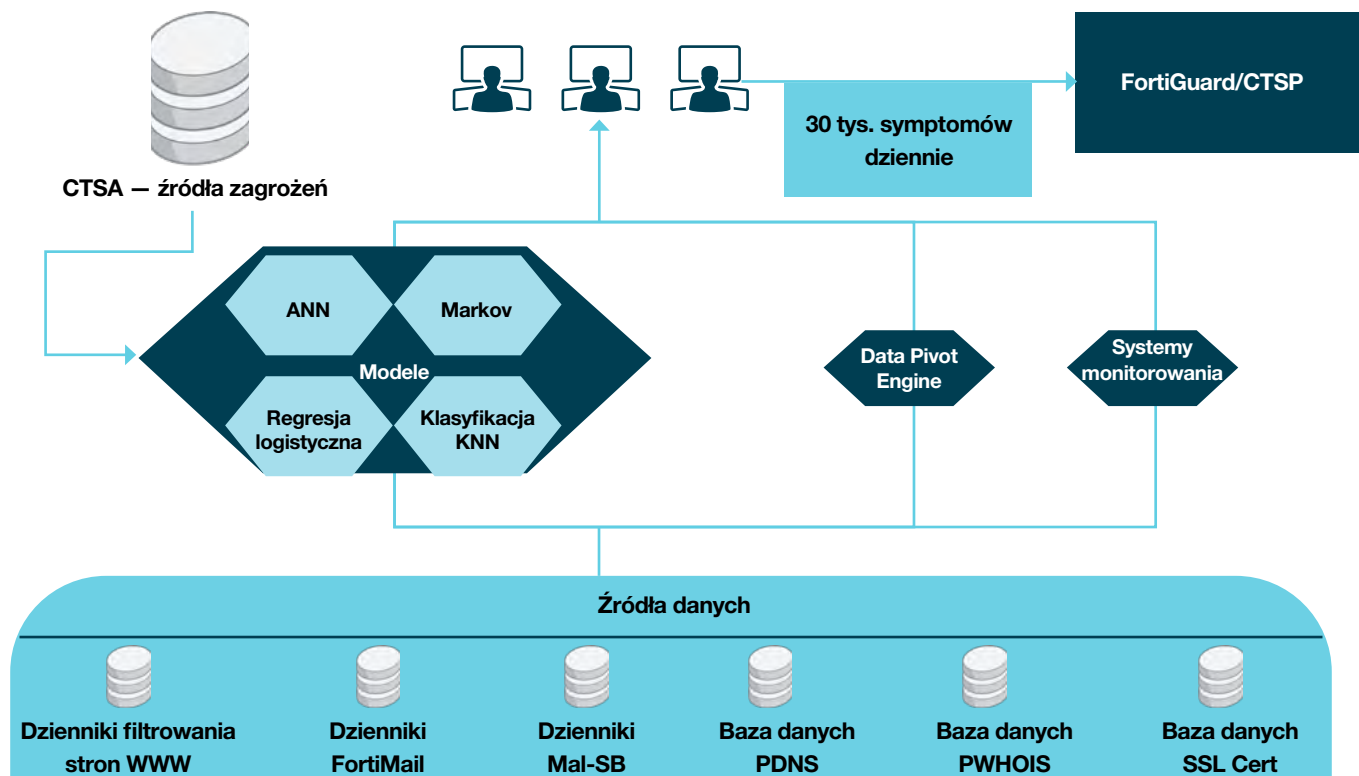
FortiGuard Labs uzyskuje informacje o zagrożeniach na podstawie opartej na mechanizmach sztucznej inteligencji analizy ponad 100 mld zdarzeń dotyczących bezpieczeństwa dziennie².

W celu skutecznego przyswajania, korelowania i analizowania dużej ilości nieprzetworzonych danych dziennych FortiGuard Labs korzysta z zaawansowanej infrastruktury i wysoce zautomatyzowanych procesów pozwalających na przekształcenie tych danych w przydatne informacje o zagrożeniach. Informacje te są następnie regularnie przesyłane do produktów Fortinet w ramach aktualizacji usług subskrypcyjnych.



Rysunek 3. Dzięki informacjom o zagrożeniach przekazywanym przez FortiGuard Labs produkty Fortinet mogą identyfikować najnowsze cyberzagrożenia.

Pierwszy system sztucznej inteligencji w Fortinet został opracowany w 2011 r., aby pomóc w monitorowaniu ogromnej liczby nowych witryn internetowych oraz oznaczaniu tych z nich, których wyświetlanie jest najbardziej ryzykowne i które wymagają dodatkowej analizy przez specjalistów. Obecnie codziennie rejestruje się od 130 do 150 tys. nowych witryn internetowych, co sprawia, że analiza każdej z nich przez człowieka staje się coraz mniej praktyczna. Na potrzeby automatycznej analizy tej wykładniczo rosnącej liczby witryn stosuje się zatem cztery różne systemy uczenia maszynowego (ML). Systemy te przetwarzają ogromne ilości otrzymywanych z sieci sond Fortinet danych telemetrycznych dotyczących takich witryn internetowych, aby wskazywać na potrzeby dalszej analizy witryny największego ryzyka korzystające na przykład z algorytmów generowania domen (DGA) lub serwerów Command & Control (C2).

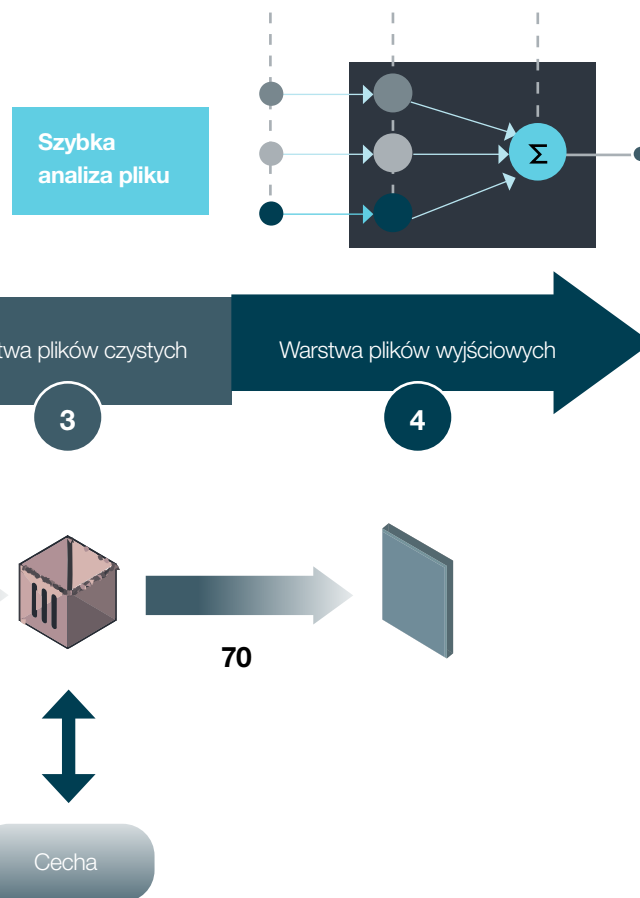


Rysunek 4. Codziennie Fortinet rejestruje ogromną liczbę witryn internetowych z różnych źródeł i stosuje cztery osobne modele uczenia maszynowego, aby wskazywać witryny na potrzeby dalszej analizy. W efekcie codziennie generowane są informacje o 30 tys. symptomach ataku (indicators of compromise, IOC).

Kolejny duży projekt, rozpoczęty w 2012 r., dotyczył rosnącej liczby próbek z plików, która na koniec 2019 r. wyniosła ponad 23 mln dziennie. Opracowany na te potrzeby system automatyzuje również proces analizy złośliwego oprogramowania, który zazwyczaj wymagał co najmniej ośmiu godzin pracy człowieka. Sztuczna sieć neuronowa (ANN) ułatwia natomiast generowanie informacji o nowych zagrożeniach, które są następnie przesyłane do klientów mniej więcej co godzinę.

▪ Podejście

- **Warstwa 1** = Przetwarzanie pliku wejściowego
- **Warstwa 2** = Ponad 15 mld węzłów identyfikuje dobre i złe cechy
- **Warstwa 3** = (1 = złośliwy, 0 = czysty)



Rysunek 5. Oferowane przez Fortinet sztuczne sieci neuronowe (ANN) składają się z ponad 15 mld węzłów, które „uczą się” z jedynych w swoim rodzaju zbieranych przez wiele lat danych o zagrożeniach globalnych. Dzięki mechanizmom uczenia maszynowego stosowanym w celu „szkolenia” danego modelu, system wykrywania zagrożeń jest na bieżąco aktualizowany i coraz dokładniejszy.

Ostatnio do platformy zabezpieczającej aplikacje sieci Web **FortiWeb** włączono dwie warstwy uczenia maszynowego w celu ochrony infrastruktury sieci publicznych. Jedna warstwa buduje profile dla każdego parametru w danej aplikacji WWW oraz identyfikuje odchylenia. Druga warstwa określa (na podstawie analizy prowadzonej pod kątem ustalonych wcześniej progów dla złośliwej działalności), czy odchylenia te stanowią cyberzagrożenie, czy też są błędem ludzkim lub czymś innym. Podejście to pomaga znacznie ograniczyć konieczność ciągłego dostrajania zapory aplikacji WWW. Istnieje również wiele modeli uczenia maszynowego, które są podstawą opartych na zachowaniach funkcji antywirusowych następnej generacji oferowanych przez rozwiązanie **FortiEDR**.

Rozwiązania FortiGate, FortiMail i FortiClient są zintegrowane z produktem **FortiSandbox**, który uzupełnia tradycyjną analizę procesów w środowisku wirtualnym wykonania o dwa filtry oparte na uczeniu maszynowym. Pierwszy z tych filtrów jest używany na potrzeby statycznej analizy plików, a drugi jest stosowany do zachowań obserwowanych podczas analizy oprogramowania w bezpiecznym środowisku testowym. Dzięki tym dwóm filtrom wspomniane środowisko testowe jest często w stanie dokonać oceny zagrożenia już po 10 milisekundach analizy. W przypadku rozwiązań FortiMail i FortiClient klienci mogą poddać podejrzaną zawartość kwarantannie do czasu zakończenia analizy w bezpiecznym środowisku testowym oraz zablokować nawet wcześniej nieznane zagrożenia za pomocą opartych na mechanizmach uczenia maszynowego filtrów rozwiązania FortiSandbox.

Codziennie FortiGuard Labs przesyła klientom ponad miliard aktualizacji zabezpieczeń⁴.

Sztuczna inteligencja a wykrywanie zagrożeń właściwych dla danego przedsiębiorstwa

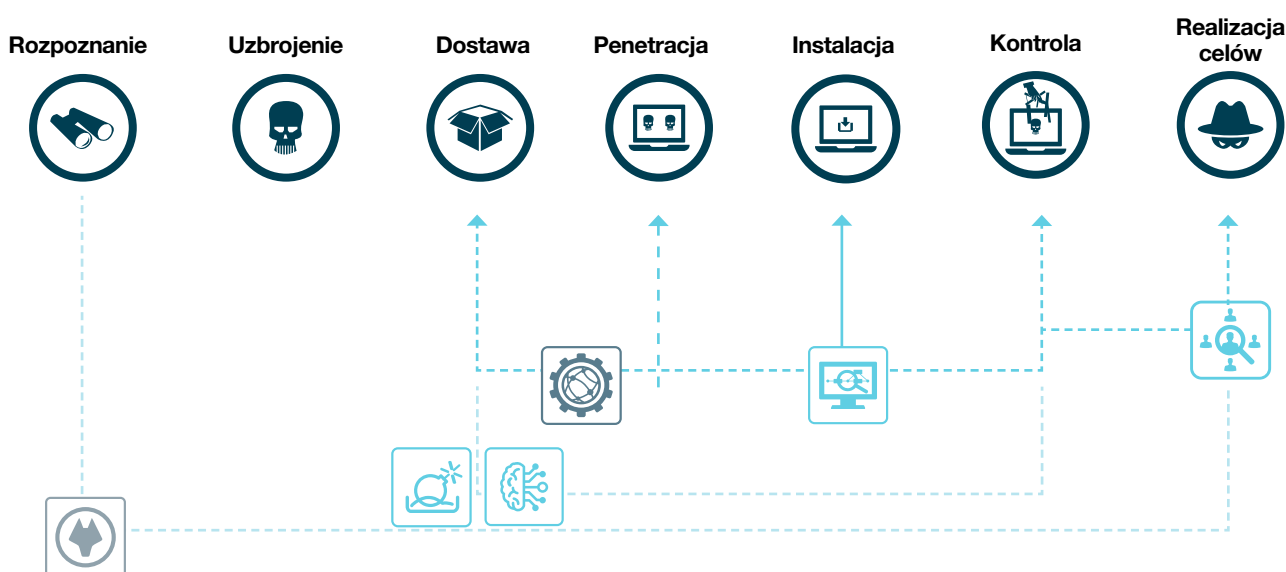
Zdeterminowany cyberprzestępca może unikać nawet najdalej idących prewencyjnych zabezpieczeń. Przedsiębiorstwa powinny zatem stosować zaawansowane metody analizy własnego ruchu i środowiska, aby identyfikować incydenty, zanim doprowadzą one do kosztownych następstw biznesowych. Fortinet oferuje szereg produktów służących do wykrywania przychodzących, zainstalowanych i aktywnych zagrożeń w całym cyklu życia cyberataku.

FortiDeceptor wdraża serię przekonujących przynęt w całym przedsiębiorstwie. Przynęty te przyciągają uwagę cyberprzestępców, zanim przystąpią oni do szerszego ataku lub podejmą próby kradzieży danych z sieci wewnętrznej.

Rozwiązanie **FortiSandbox** może być wbudowane w ścieżkę ruchu przychodzącego (jak już wspomniano) lub umieszczone w centrum zarządzania bezpieczeństwem (SOC), aby wykrywać próby przesłania złośliwych pakietów danych. Uzupełnieniem tego rozwiązania jest produkt **FortiAI**, który korzysta z określonej wersji sztucznej sieci neuronowej (ANN) opracowanej przez FortiGuard Labs na potrzeby analizy plików w środowisku przedsiębiorstwa. **FortiAI** pozwala na błyskawiczne (w czasie krótszym niż sekunda) wykrywanie nieznanego wcześniej złośliwego oprogramowania, automatyczne śledzenie symptomów występowania tego oprogramowania w przedsiębiorstwie oraz pełniejsze odwzorowanie cyklu życia zagrożenia, podobne do tego generowanego przez doświadczonego analityka bezpieczeństwa.

Jeśli przesłanie złośliwego oprogramowania zakończy się sukcesem, rozwiązanie **FortiEDR** zastosuje specjalne mechanizmy śledzenia kodu w czasie rzeczywistym (uzupełniające jego program antywirusowy następnej generacji) na potrzeby identyfikacji podejrzanych zachowań potencjalnie zainfekowanych hostów. Zachowania te mogą zostać natychmiast zneutralizowane w celu powstrzymania potencjalnego zagrożenia lub przekazane do chmury, gdzie sztuczne sieci neuronowe szybko określają, czy podejrzane zachowanie jest niezłośliwe, czy złośliwe. Dzięki temu dany host może zostać odpowiednio zbadany i naprawiony albo przywrócony do pełnej eksploatacji przy minimalnym wpływie na działalność operacyjną.

Wreszcie rozwiązanie **FortiInsight** skupia się na dostępie do danych i ich przepływie, czyli końcowym etapie ataku, i na podstawie metod bayesowskich identyfikuje nietypową aktywność w ramach podobnych grup (użytkowników lub urządzeń), która może wskazywać na wewnętrzne zagrożenie lub skutecznie zaatakowany host. Administratorzy zabezpieczeń mogą nie tylko badać anomalię, ale również przekazywać opinie na temat zasadności każdego alertu. Pomaga to w szkoleniu modelu uczenia maszynowego w celu poprawy jego skuteczności w oznaczaniu zagrożeń wewnętrznych.



Rysunek 6. Rozwiązania Fortinet na poszczególnych etapach cyberataku

Sztuczna inteligencja a szybka reakcja na incydenty

Wykrycie wymaga reakcji, Fortinet oferuje zatem szereg rozwiązań pomagających przedsiębiorstwom na wszystkich poziomach zabezpieczeń w orkiestracji i automatyzacji reakcji na wykryte zagrożenia. Rozwiązanie **FortiAnalyzer** udostępnia zarówno standardowe funkcje analizy, jak również bardzo przydatne funkcje automatyzacji w ramach całej architektury Fortinet Security Fabric i jest odpowiednie nawet dla najmniejszych lub mało doświadczonych zespołów zajmujących się bezpieczeństwem.

W miarę jak przedsiębiorstwa rozwijają posiadane funkcje bezpieczeństwa i poszukują narzędzi zapewniających widoczność i możliwości reakcji obejmujące rozwiązania różnych producentów rozwiązanie **FortiSIEM** może zostać zintegrowane z szeroką gamą zabezpieczeń i produktów IT, aby pobierać, korelować i wykorzystywać zaawansowane dane analityczne na potrzeby inicjowania zautomatyzowanych działań naprawczych w ramach całych niejednorodnych środowisk.

W przypadku zaawansowanego centrum zarządzania bezpieczeństwem z dobrze zdefiniowanymi procesami operacyjnymi rozwiązanie **FortiSOAR** może uzupełniać działanie dowolnego narzędzia do zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM) w celu tworzenia procedur orkiestracji i automatyzacji tych procesów. Uwaga: sztuczna inteligencja jest stosowana do określania priorytetów nowych alertów oraz do przypisywania do nich właścicieli. W rezultacie procesy reakcji stają się ukierunkowane i efektywniejsze, a w wielu przypadkach istnieje możliwość zautomatyzowania najważniejszych działań.

Rozwiązania Fortinet umożliwiają przedsiębiorstwom zastosowanie mechanizmów sztucznej inteligencji na wszystkich etapach cyklu życia cyberataku, aby przyspieszyć procesy wykrywania zagrożeń i reagowania na zagrożenia⁵.

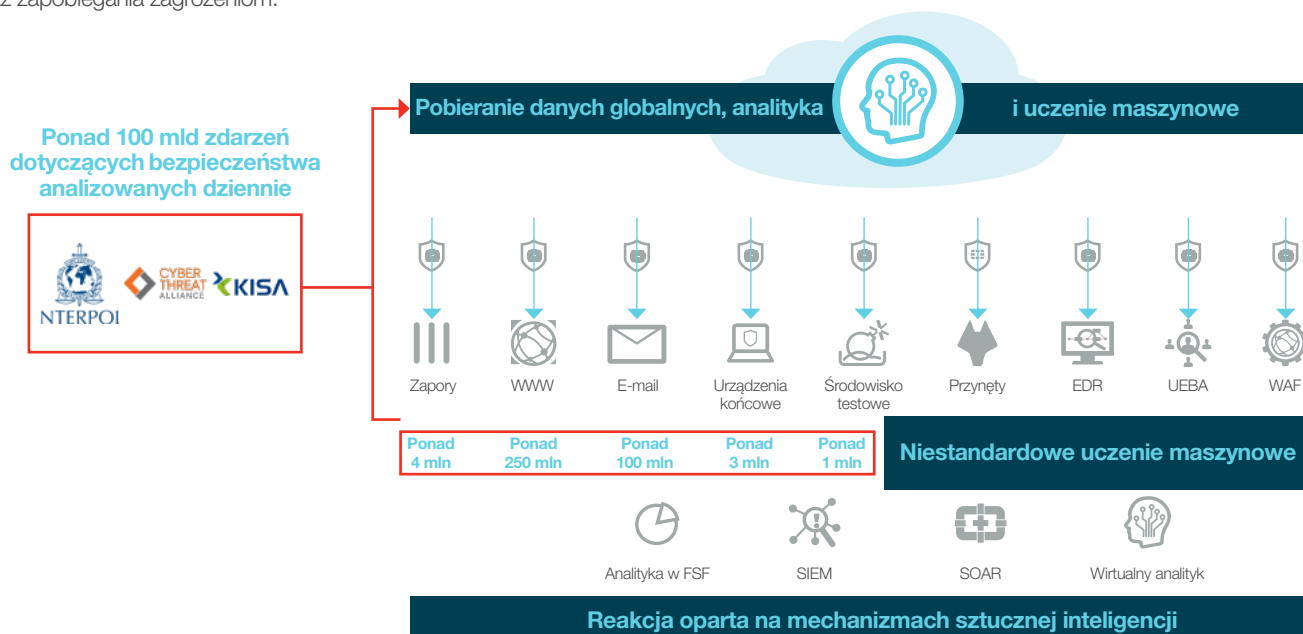


Rysunek 7. Rozwiązania Fortinet eliminują luki w zabezpieczeniach oraz skracają czas działań naprawczych w wyniku automatyzacji procesów wykrywania zagrożeń i reagowania na zagrożenia.

Sztuczna inteligencja a ścieżki cyberataku, cykl życia cyberataku i kontekst globalny

Fortinet od dawna inwestuje w mechanizmy sztucznej inteligencji, aby sprostać rosnącym wyzwaniom w zakresie cyberbezpieczeństwa. Szkolone przez specjalistów ds. zagrożeń z FortiGuard Labs modele uczenia maszynowego i bardziej zaawansowane sztuczne sieci neuronowe analizują ogromne ilości nieprzetworzonych danych telemetrycznych i pomagają generować aktualizacje dotyczące globalnych zagrożeń. Są one uzupełniane przez podobne systemy sztucznej inteligencji, które mogą być wdrażane na całej linii obrony przedsiębiorstwa przed zagrożeniami obejmującej punkty końcowe, pocztę elektroniczną, sieć i chmurę na potrzeby bieżącego wykrywania zagrożeń, a nawet reagowania na te zagrożenia.

Dzięki temu rozwiązania Fortinet mogą zaoferować zaawansowaną cyberobronę wspomaganą przez mechanizmy sztucznej inteligencji korzystające z zalet uczenia maszynowego w modelu globalnym, scentralizowanym i rozproszonym. Dzięki modelom sztucznej inteligencji szkolonym i stosowanym w kontekście każdego etapu cyklu życia cyberataku, od rozpoznania po realizację celów, rozwiązania Fortinet pozwalają zarządzać zarówno ryzykiem wewnętrznym, jak i zewnętrznym, a także zapewniają zaawansowane funkcje wykrywania i eliminowania zagrożeń oraz zapobiegania zagrożeniom.



Rysunek 8. Codziennie mechanizmy sztucznej inteligencji FortiGuard Labs przetwarzają dane dotyczące 100 mld zdarzeń związanych z bezpieczeństwem, aby przesyłać do produktów Fortinet aktualizacje informacji o zagrożeniach.

¹ „Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security”, Capgemini, dostęp z dnia 23 marca 2020 r.

² „FortiGuard Security Services”, Fortinet, październik 2019 r.

³ „Fortinet Security Fabric Enables Digital Innovation: Broad, Integrated, and Automated”, Fortinet, 13 luty 2020 r.

⁴ „FortiGuard Security Services”, Fortinet, październik 2019 r.

⁵ „Fortinet Introduces Self-Learning Artificial Intelligence Appliance for Sub-Second Threat Detection”, Fortinet, 24 luty 2020 r.

FORTINET

www.fortinet.com

Copyright © 2020 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyrażne lub dorozumiane gwarancje i rękojnie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisananej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działał zgodnie z wyrażnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyrażne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).

sierpnia31,202012:41PM