SZTUCZNA INTELIGENCJA
jako kluczowy element budowy architektury bezpieczeństwa teleinformatycznego nowej generacji

Nieustanny wzrost ilości, szybkości i stopnia zaawansowania cyberataków przytłacza zespoły bezpieczeństwa w podmiotach z każdej branży. Na szczęście, architekci bezpieczeństwa teleinformatycznego, chcący odciążyć się od swoich żmudnych codziennych obowiązków, mają do dyspozycji nowe narzędzia, bazujące na technologiach sztucznej inteligencji nowej generacji.

Rozwiązania, takie jak wirtualny analityk bezpieczeństwa, rozpoznawanie zaawansowanych zagrożeń za pomocą wyszkolonej głębokiej sieci neuronowej, czy uczenie maszynowe dla rozpoznawania określonych wzorców, pomagają stawić czoła tym wyzwaniom. Komponenty rozwiązań wykorzystujących sztuczną inteligencję ulokowane w infrastrukturze firmy, czy też serwisy dostarczane w postaci chmury obliczeniowej, pomagają analizować nadchodzące zagrożenia w czasie rzeczywistym. Dzięki temu zespoły bezpieczeństwa teleinformatycznego mają możliwość powstrzymania hakerów i złośliwego oprogramowania przed przeniknięciem do ich środowiska.

Zwiększenie liczby, szybkości i złożoności cyberataków

W 2019 r. średni cykl życia kampanii zagrożeń, od rozpoczęcia rozpowszechnienia, do pojawienia się nowego wariantu lub nowej kampanii, często wynosił jeden miesiąc i mniej. Istnieje rozwinięty ekosystem cyberprzestępczości, w którym dostępne są zestawy narzędzi wykorzystujące podatności oprogramowania, Malware-as-a-Service (MaaS), boty do wynajęcia, i inne, przez co drastycznie skrócił się czas wejścia na rynek dla cyberprzestępców.

Jednocześnie wiele zagrożeń cybernetycznych stało się bardziej wyrafinowanych i nie ograniczają się jedynie do silnie ukierunkowanych ataków na wybrane serwisy w celu ich zablokowania. Działania przestępcze w cyberprzestrzeni wykorzystują m.in. socjotechnikę i prowadzą do powstawania zagrożeń, które stają się coraz trudniej zauważalne dla użytkowników końcowych oraz trudne do wykrycia przez tradycyjne kontrole bezpieczeństwa.

Wojciech Ciesielski
Major Account Manager, Fortinet

Oczywiście, powtarzanie w kółko tego samego zachowania i oczekiwanie różnych rezultatów jest naiwnością. Aby wygrać tę wojnę, trzeba ponownie przemyśleć swoją strategię bezpieczeństwa, a zmiana paradygmatu bezpieczeństwa wymaga trzech podstawowych podejść:

1. **Zacznij od bezpieczeństwa**. Zamiast budować sieć, a następnie nakładać na nią zabezpieczenia, rozpocznij projektowanie z myślą o bezpieczeństwie. Polityki bezpieczeństwa muszą płynnie przechodzić od sieci korporacyjnej do chmury, od sieci przemysłowych do oddziałów oraz pracowników mobilnych, i konsekwentnie być egzekwowane.
2. **Wykorzystaj ekonomię cyberprzestępczości**. Cyberprzestępcy podlegają takim samym ograniczeniom finansowym jak każda organizacja. Dlatego też większość przestępców woli atakować łatwo dostępne cele przy użyciu znanych metod, ponieważ opracowywanie nowych narzędzi i ataki typu dnia zerowego są kosztowne. Można wyeliminować wiele rodzajów ryzyka, wykonując m.in. następujące działania:

- kontrolę zgodności ze standardami i politykami bezpieczeństwa,
- podnoszenie poziomu świadomości użytkowników w zakresie cyberzagrożeń,
- odkrywanie i usuwanie luk w zabezpieczeniach,

- centralizację logowania zdarzeń i kontroli,
- wprowadzenie ram bezpieczeństwa bazujących na interoperacyjności, wysokiej wydajności i głębokiej integracji,
- segmentację sieci w celu ograniczenia lub spowolnienia poziomego ruchu złośliwego oprogramowania.

3. **Zwalczaj ogień ogniem.** Zarówno przedsiębiorstwa, jak i cyberprzestępczość działają z prędkością cyfrową. Wiele incydentów w cyberprzestrzeni zaistniało, ponieważ szybkość ataku jest większa niż czas reakcji systemu bezpieczeństwa. Jest to szczególnie zauważalne tam, gdzie na każdym etapie procesu wymagana jest interwencja człowieka. Zamiast tego, krytyczne zdarzenia muszą wywołać natychmiastową reakcję. Oczywiście, automatyka może reagować tylko na znane zagrożenia. Dodanie maszynowego uczenia (machine learning, ML) pozwala zautomatyzowanym systemom lepiej identyfikować nietypowe zachowania i redukować liczbę fałszywych alarmów[1].

Ewolucja sztucznej inteligencji w bezpieczeństwie cybernetycznym

Firmy zajmujące się bezpieczeństwem cybernetycznym od kilku lat wykorzystują uczenie maszynowe w walce z cyberprzestępcami – przede wszystkim w dziedzinie wykrywania zagrożeń. Algorytmy szkoleniowe stosują uczenie maszynowe, aby umożliwić coraz dokładniejszą identyfikację cech złośliwych plików, a rezultatem jest wykrywanie w czasie rzeczywistym zaawansowanych zagrożeń, w tym ataków dnia zerowego.

Jednak samo lepsze wykrywanie zagrożeń nie jest wystarczające, aby zespoły odpowiedzialne za cyberbezpieczeństwo czuły się mniej obciążone. Lepsze wykrywanie oznacza jednak jeszcze większą liczbę alarmów, które muszą być obsługiwane. Potrzebna jest zatem bardziej rozwinięta automatyzacja – zwłaszcza w zakresie reagowania na zagrożenia.

Postęp zarówno w dziedzinie sztucznej inteligencji (Artificial Intelligence, AI), jak i mocy obliczeniowej pozwala nadążyć za cyberzagrożeniami. Niezależnie od tego, czy celem jest utrzymanie aktualnego stanu wiedzy o globalnych zagrożeniach w cyberprzestrzeni, identyfikowanie incydentów specyficznych dla danej organizacji, zanim staną się one naruszeniami, czy nawet wdrożenie prewencyjnych działań w czasie rzeczywistym, sztuczna inteligencja może być właściwą odpowiedzią.

W przeciwieństwie do automatyzacji i uczenia maszynowego, sztuczna inteligencja próbuje odtworzyć procesy analityczne ludzkiej inteligencji nie tylko po to, aby umożliwić podejmowanie decyzji z prędkością maszyny, ale z czasem może nawet zacząć przewidywać i zapobiegać zdarzeniom związanym z bezpieczeństwem, zanim one wystąpią.

Prawdziwy system sztucznej inteligencji wymaga sztucznej sieci neuronowej (ANN) w połączeniu z modelem głębokiego uczenia się, aby nie tylko przyspieszyć analizę danych i podejmowanie decyzji, ale także umożliwić sieci adaptację i ewolucję w przypadku napotkania nowych informacji. Ten szeroko zakrojony proces szkoleniowy obejmuje staranne dostarczanie ogromnych ilości coraz bardziej złożonych informacji, dzięki czemu sieć może nie tylko identyfikować wzorce i opracowywać strategie rozwiązywania problemów, ale także dostosowywać te algorytmy w przypadku napotkania nowego wzorca.

Sztuczna inteligencja następnej generacji: głębokie sieci neuronowe

Aby opisać potencjał sztucznej inteligencji następnej generacji dla cyberbezpieczeństwa, pomocne jest precyzyjne zdefiniowanie używanej terminologii:

- **sztuczna inteligencja** (AI) jest ogólnym terminem, który odnosi się do zdolności maszyny do naśladowania inteligentnego zachowania człowieka,
- **uczenie maszynowe** (ML) jest jednym ze składników sztucznej inteligencji, wykorzystuje dane do rozwiązywania liniowych problemów, takich jak tworzenie przewidywań lub wykonywanie zadań; sztuczne sieci neuronowe (Artificial Neural Networks, ANN) są jedną z powszechnych metod uczenia maszynowego. Używają one sprzętu i oprogramowania do budowania konfiguracji, która jest wzorowana na działaniu neuronów w ludzkim mózgu poprzez szkolenie maszyny uczącej. Modele są na bieżąco zasilane ogromną ilością informacji, a system analizuje te informacje i dostosowuje algorytmy wykorzystując nowe taktyki i możliwości stosowane przez złośliwe oprogramowanie.

> **Firma Fortinet dokonała przełomu w dziedzinie wykorzystania sztucznej inteligencji w obszarze cyberbezpieczeństwa, ponieważ jako pierwsza wprowadziła na rynek, dostępnego do instalacji we własnej infrastrukturze informatycznej, wirtualnego analityka bezpieczeństwa (FortiAI), bazującego na technologii głębokiej sieci neuronowej. De facto jest on drugą generację samouczącego się systemu detekcji cyberzagrożeń (Self-Envolving Detection System, SEDS) opracowanego i rozwijanego przez Fortinet FortiGuard Lab, który ustawicznie uczy się już od ponad ośmiu lat.**

- **głębokie sieci neuronowe** (Deep Neural Networks, DNN), czasami znane jako głębokie uczenie (Deep Learning, DL), są jedną z technik uczenia maszynowego, która wykorzystuje wiele sztucznych sieci neuronowych – z dwoma lub więcej warstwami pomiędzy warstwami wejściową i wyjściową – do modelowania złożonych, nieliniowych relacji.

Poziomy zrozumienia i analizy zapewniane przez głęboką sieć neuronową dają możliwość przeniesienia sztucznej inteligencji na kolejny poziom w zakresie cyberbezpieczeństwa. Kiedy sztuczna inteligencja jest używana tylko do wykrywania zagrożeń, może potencjalnie zwiększyć obciążenie zespołu bezpieczeństwa, ponieważ zwiększa ilość otrzymywanych alarmów. Podnosi to również prawdopodobieństwo, że konkretne zagrożenie nie otrzyma na czas odpowiedzi.
Z drugiej strony, jeśli sztuczna inteligencja może być wykorzystana do podejmowania decyzji dotyczących reakcji na zagrożenie, może to zacząć przynosić istotne wsparcie profesjonalistom zajmującym się cyberbezpieczeństwem. Pracownicy mogą nadal koncentrować się na strategii bezpieczeństwa, podczas gdy większość działań podejmowanych w odpowiedzi na zagrożenia jest zautomatyzowana i prowadzona w czasie rzeczywistym przez wirtualnego analityka bezpieczeństwa[2].

Szkolenie sztucznej inteligencji

Jednym z najbardziej krytycznych elementów dla jakości i skuteczności działania rozwiązania sztucznej inteligencji jest sposób prowadzenia szkolenia. Społeczność AI zaleca, aby każde rozwiązanie z zakresu sztucznej inteligencji przechodziło trzy etapy szkolenia:

1. **Nadzorowane uczenie się**. Ten początkowy model rozpoczyna się od zasilenia systemu sztucznej inteligencji ogromnym wolumenem oznaczonych danych, w których charakterystyka każdego zestawu informacji jest wyraźnie określona, a decyzje są przewidywalne. Na przykład zespół ds. rozwoju sztucznej inteligencji w Fortinet korzysta z danych opracowanych przez ponad 200 analityków z FortiGuard Lab, którzy obecnie rejestrują ponad 580 tys. godzin badania danych rocznie. Ponadto wykorzystuje on dane zbierane w czasie rzeczywistym z urządzeń i czujników działających na całym świecie oraz dane pochodzące z wielu źródeł wiedzy o zagrożeniach. Ostatecznie to właśnie ten poziom i ilość danych wejściowych pozwalają systemom sztucznej inteligencji na ciągłe doskonalenie poprzez rozszerzanie zestawu oznaczonych wzorców i reakcji.

2. **Nauka bez nadzoru**. W tej kolejnej fazie dane nieoznaczone są wprowadzane powoli, co zmusza system do samodzielnego uczenia się, gdy zaczyna dostrzegać i rozpoznawać nowe wzorce.

3. **Wzmocnienie**. Oba te procesy monitorują działanie systemu za pomocą znanych i nieznanych plików i „nagradzają" system za dobre wyniki. Cykle szkoleniowe pomiędzy tymi trzema strategiami uczenia się odbywają się na bieżąco przez miesiące, a czasami lata, w zależności od złożoności problemów, które system musi zidentyfikować i rozwiązać.

Ze względu na powtarzające się wymogi procesu uczenia się, każdy system sztucznej inteligencji, który nie wykorzystuje wszystkich trzech z powyższych modeli uczenia się jest niepełny. Każdy model uczenia się pomaga udoskonalić wyniki i poprawić dokładność.

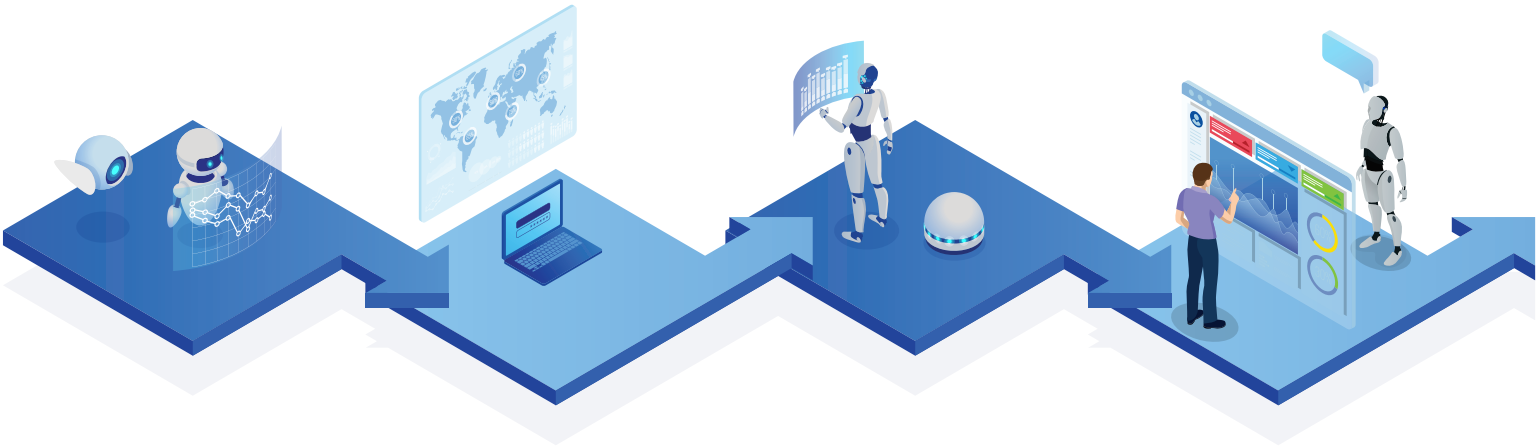
Ponieważ środowisko zagrożeń wciąż się zmienia, modele szkolenia w zakresie sztucznej inteligencji nie mogą pozostawać statyczne. System musi być stale wzbogacany o nowe modele, które bazują na nowych zagrożeniach i technikach ataku, a także o nowe strategie identyfikacji i wykrywania. Należy również stosować stały monitoring jakości rozpoznawania wzorców. Sztuczna inteligencja może zostać niezamierzenie zatruta złymi danymi, tworząc tendencję, która wpływa na jej zdolność do podejmowania dobrych decyzji, lub zostać celowo zatruta w celu ominięcia pewnych rodzajów zagrożeń[3].

Wykorzystanie AI do poznania konkretnych organizacji

Aby bardzo przyspieszyć wykrywanie wzrastającej liczby zaawansowanych zagrożeń, wirtualny analityk bezpieczeństwa FortiAI uczy się i dostosowuje do nowych ataków na konkretną organizację, stale ulepszając i optymalizując metody ochrony przed zagrożeniami. W rezultacie wirtualny analityk bezpieczeństwa wspiera personel zespołu bezpieczeństwa poprzez identyfikację i analizę złośliwego oprogramowania niebazującego na plikach, jak i opartego na plikach, oraz identyfikuje zagrożone systemy w całej organizacji ze stuprocentową pewnością

w czasie poniżej jednej sekundy. W tym celu FortiAI wykorzystuje technologię głębokiej sieci neuronowej do podejmowania decyzji, które podejmowałby analityk bezpieczeństwa podczas ręcznego badania ataków, m.in:

- klasyfikacja ataku na konfigurowalne kategorie, takie jak: wymuszenie okupu (ransomware), złośliwe wydobywanie kryptowalut (cryptojacking), robaki (worms), ataki back-door, wycieki danych (data leaks), botnety i przejmowanie kontroli nad urządzeniami (rootkit),



- dochodzenie do źródła ataku poprzez identyfikowanie pierwotnego miejsca zakażenia i zapewnienie pełnej widoczności rozprzestrzenienia się infekcji od pacjenta zerowego do wszystkich kolejnych narażonych systemów,

- analiza złośliwego oprogramowania pod kątem jego cech i osi czasu incydentu. Przypomina to miniaturowy model łańcucha ataku (kill-chain), który opisuje w sposób naukowy, co zagrożenie próbowało zrobić krok po kroku, w tym zastosowaną technikę – przykładowo: w „chwili zerowej" nastąpiło pobranie pliku HTML; w „chwili pierwszej" w przeglądarce doszło do złośliwego wykorzystania kodu; w „chwili drugiej" do pobrania trojana do katalogu użytkownika lub katalogu tymczasowego.

Dane opracowane przez wirtualnego analityka bezpieczeństwa FortiAI mogą zostać automatycznie wykorzystane przez inne elementy architektury bezpieczeństwa w organizacji, takie jak zapory sieciowe nowej generacji (NGFW), umożliwiając zablokowanie zidentyfikowanych przez niego zagrożeń. Pracownicy działu bezpieczeństwa teleinformatycznego mogą następnie wykorzystać tę wiedzę do kontroli bezpieczeństwa w całej sieci.

Wirtualny analityk bezpieczeństwa

Firma Fortinet dokonała przełomu w dziedzinie wykorzystania sztucznej inteligencji w obszarze cyberbezpieczeństwa, ponieważ jako pierwsza wprowadziła na rynek, dostępnego do instalacji we własnej infrastrukturze informatycznej, wirtualnego analityka bezpieczeństwa, o nazwie FortiAI, bazującego na technologii głębokiej sieci neuronowej. Wirtualnego analityka bezpieczeństwa FortiAI można de facto określić jako „SEDS 2.0", drugą generację samouczącego się systemu detekcji cyberzagrożeń (Self-Envolving Detection System, SEDS) opracowanego i rozwijanego przez Fortinet FortiGuard Lab, który ustawicznie uczy się już od ponad ośmiu lat. FortiAI zawiera niezależną, samowystarczalną sztuczną inteligencję, która naśladuje funkcję analityka bezpieczeństwa informacji i, podobnie do człowieka, dostosowuje się do nowych ataków i zdobywa doświadczenie w miarę upływu czasu. Jednak w przeciwieństwie do analityków zajmujących się bezpieczeństwem, robi to z prędkością maszyny. Wirtualny analityk bezpieczeństwa z bardzo wysoką wydajnością wykorzystuje głęboką sieć neuronową do automatyzacji badania incydentów bezpieczeństwa i budowania wiedzy o zagrożeniach w celu przerywania ukierunkowanych ataków.

Model uczenia się bez nadzoru głębokiej sieci neuronowej wykorzystywany w wirtualnym analityku bezpieczeństwa FortiAI, może być tak naprawdę nazwany „przyjazną sztuczną inteligencją" (Friendly Artificial Intelligence, FAI), terminem, który do tej pory był w dużej mierze aspiracyjny. Ze względu na swoje możliwości związane z wykorzystaniem techno-

FORTINET®

SKALA ZAGROŻEŃ JEST WIĘKSZA NIŻ KIEDYKOLWIEK

Reakcja musi być szybka, jak nigdy dotąd

www.fortinet.com

logii uczenia maszynowego, wirtualny analityk bezpieczeństwa identyfikuje i analizuje zagrożenia z coraz większą prędkością i dokładnością, zwiększając tym samym wydajność pracy całego zespołu odpowiedzialnego za bezpieczeństwo cybernetyczne.

Architektura bezpieczeństwa cyfrowego wsparta sztuczną inteligencją

Firma Fortinet od dawna inwestuje w rozwiązania sztucznej inteligencji (AI), aby sprostać rosnącym wyzwaniom w zakresie bezpieczeństwa cybernetycznego. Modele maszyn uczących się i bardziej zaawansowane sztuczne sieci neuronowe (ANN), szkolone przez analityków zagrożeń w laboratoriach FortiGuard Labs, przetwarzają ogromne ilości danych, pomagając aktualizować wiedzę na temat globalnych cyberzagrożeń. Są one uzupełniane przez podobne systemy sztucznej inteligencji, które mogą być wdrażane w infrastrukturze danej organizacji w celu zapobiegania atakom, wykrywania ich i reagowania na nie. Rozwiązania te obejmują urządzenia końcowe, pocztę elektroniczną, systemy oraz aplikacje, niezależnie od tego, czy znajdują się one w sieci wewnętrznej firmy, chmurze publicznej, czy działają przez internet.

Dzięki temu możliwe jest zbudowanie solidnej architektury cyberbezpieczeństwa sterowanej przez sztuczną inteligencję, która wykorzystuje zalety globalnego scentralizowanego oraz lokalnego rozproszonego uczenia maszynowego. Z zastosowaniem technik sztucznej inteligencji przeszkolonych i zastosowanych na każdym etapie łańcucha ataku, począwszy od prowadzonego rozpoznania, a skończywszy na realizacji celów, rozwiązania Fortinet są w stanie zarządzać ryzykiem cybernetycznym zarówno zewnętrznym, jak i wewnętrznym, dzięki zaawansowanym funkcjom zapobiegania, wykrywania i reagowania na zagrożenia.

Zasoby, uczenie i integracja wyznacznikiem skuteczności AI

Wiele firm zajmujących się bezpieczeństwem cybernetycznym twierdzi, że wprowadziły do swoich rozwiązań mechanizmy ochrony z wykorzystaniem sztucznej inteligencji. W rzeczywistości jednak większość z nich nie posiada prawdziwej sztucznej inteligencji, ponieważ ich infrastruktura jest zbyt mała lub ich modele uczenia się są niekompletne. Inne odmawiają ujawnienia stosowanych przez nie metod, co budzi obawy co do wiarygodności ich rozwiązań sztucznej inteligencji. Powinny to być czerwone flagi dla każdej organizacji chcącej przyjąć system bazujący na sztucznej inteligencji.

Równie ważne jest, aby nawet jeśli system sztucznej inteligencji spełnia podstawowe wymogi szkoleniowe i infrastrukturalne, nadal musiał współdziałać w ramach istniejącego środowiska bezpieczeństwa. Inteligencja w izolacji jest bezużyteczna. Im więcej informacji o zagrożeniach jest współdzielonych – czy to z zewnętrznego źródła informacji, czy też ze zintegrowanych systemów bezpieczeństwa rozmieszczonych w sieci rozproszonej – tym skuteczniejsze staną się systemy obronne bazujące na sztucznej inteligencji.

Systemy wyposażone w rozwiązania sztucznej inteligencji zapewniają firmom i organizacjom przewagę nad cyberprzestępcami. Wplatają one zabezpieczenia w infrastrukturę, identyfikują i reagują na najbardziej zaawansowane zagrożenia. Mają działanie odstraszające i zniechęcające cyberprzestępców do podejmowania prób ataków, ponieważ wiązałoby się to z koniecznością opracowania nowych narzędzi i technik, co przekłada się na wysokie po ich stronie koszty[4].

> **Sztuczna inteligencja w izolacji jest bezużyteczna. Im więcej informacji o zagrożeniach jest współdzielonych – czy to z zewnętrznego źródła informacji, czy też ze zintegrowanych systemów bezpieczeństwa rozmieszczonych w sieci rozproszonej – tym skuteczniejsze staną się systemy obronne bazujące na sztucznej inteligencji.**

1 Disrupting Cybercriminal Strategy With AI and Automation, Security Week, August 2019

2 Using AI to Address Advanced Threats That Last-Generation Network Security Cannot, 2019 Fortinet.

3 Disrupting Cybercriminal Strategy With AI and Automation, Security Week, August 2019

4 Disrupting Cybercriminal Strategy With AI and Automation, Security Week, August 2019