ZASTOSOWANIE SZTUCZNEJ INTELIGENCJI W CELU OCHRONY PRZED ZAAWANSOWANYMI ZAGROŻENIAMI, KTÓRYCH NIE POWSTRZYMAJĄ ZABEZPIECZENIA POPRZEDNIEJ GENERACJI

SPIS TREŚCI

STRESZCZENIE

W świecie transformacji cyfrowej (DX) działy IT mają do czynienia ze zwiększoną złożonością zagrożeń i rozszerzoną powierzchnią ataku, co naraża na szwank zarówno bezpieczeństwo, jak i wydajność sieci. Zastosowanie technologii sztucznej inteligencji (AI) jest niezbędne w obu tych obszarach, ponieważ pozwala na zautomatyzowanie i przyspieszenie procesu wykrywania zagrożeń i usuwania skutków naruszeń (które to zagrożenia również zaczynają powstawać przy zastosowaniu sztucznej inteligencji). Ponadto dzięki wdrożeniu tej technologii specjaliści ds. bezpieczeństwa mogą zostać przesunięci do realizacji bardziej strategicznych zadań.

W kontekście bezpieczeństwa sieci funkcje sztucznej inteligencji i uczenia maszynowego (ML) są stosowane w samorozwijających się systemach wykrywania zagrożeń (SEDS), które dotrzymują kroku coraz bardziej złożonemu charakterowi zagrożeń oraz są zdolne do identyfikacji ataku typu „zero-day” na podstawie jego cech. Funkcje uczenia maszynowego obejmują trzy modele uczenia: uczenie nadzorowane, uczenie nienadzorowane i uczenie ze wzmocnieniem. W efekcie zastosowania dużej ilości danych i wszystkich tych trzech modeli systemy SEDS mogą osiągnąć najwyższy stopień dokładności działania. Przy wyborze właściwego systemu SEDS należy brać pod uwagę ilość przetwarzanych danych, obecność wszystkich trzech wspomnianych modeli uczenia korzystających ze sztucznych sieci neuronowych (ANN) oraz zdolność do integracji funkcji sztucznej inteligencji w ramach kompleksowej architektury zabezpieczeń, która będzie zapewniać scentralizowaną widoczność, rzeczywistą automatyzację oraz wymianę informacji o zagrożeniach w czasie rzeczywistym.

„Jeśli zna się atakującego i ma się zdolność do szybkiej odpowiedzi, szanse na jego pokonanie są większe, gdy można zareagować w czasie rzeczywistym”.

David Strom, „Understanding the Relationship Between AI and Cybersecurity”, SecurityIntelligence, 22 marca 2018 r.

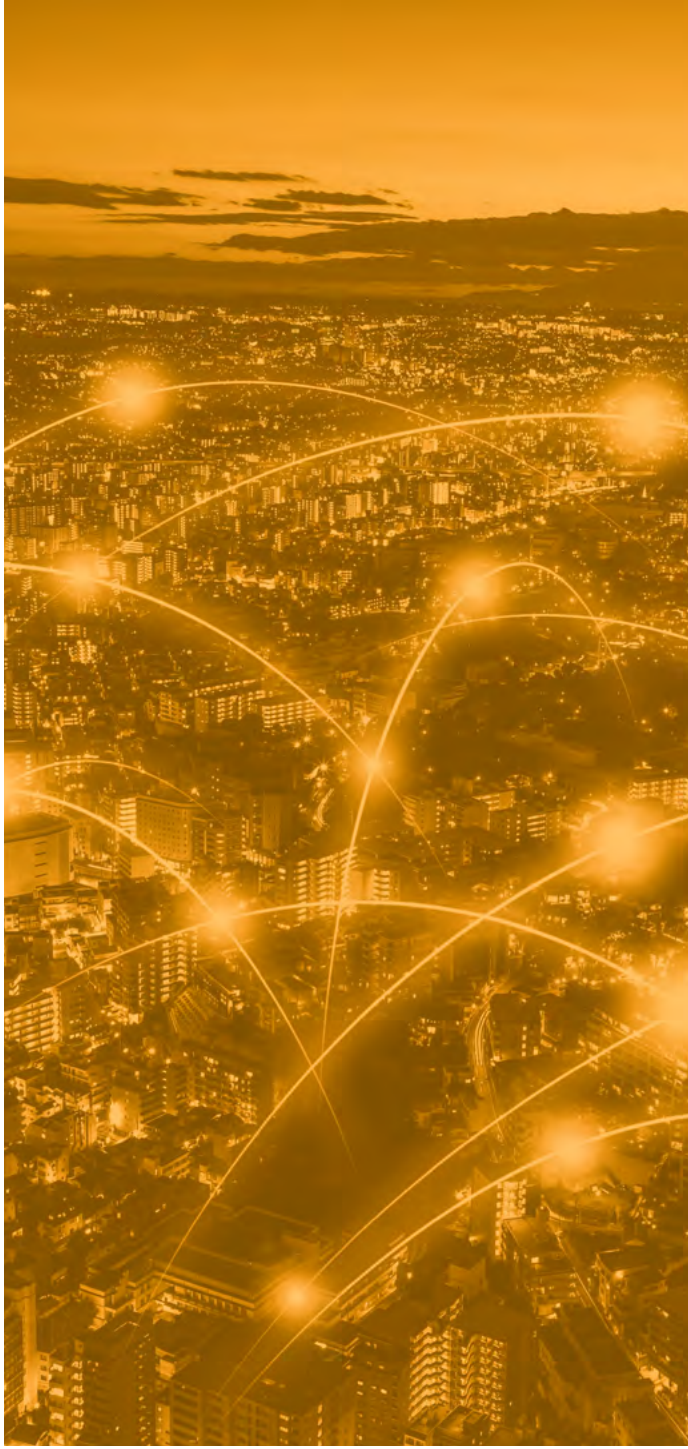
TRANSFORMACJA CYFROWA UTRUDNIA OBSŁUGĘ I ZABEZPIECZENIE SIECI

Inicjatywy dotyczące transformacji cyfrowej pomagają firmom w uzyskaniu efektywności kosztowej, wykorzystaniu nowych źródeł przychodów i wyprzedzeniu konkurencji. W efekcie architektura sieci informatycznej rozwija się w bardzo szybkim tempie, przez co dane i aplikacje o znaczeniu krytycznym dla przedsiębiorstwa znajdują się w wielu chmurach, wewnętrzny ruch sieciowy omija centrum danych za pośrednictwem sieci rozległej definiowanej programowo (SD-WAN), a urządzenia związane z Internetem rzeczy stają się obecne praktycznie w ramach każdej funkcji w przedsiębiorstwie[1].

Wspomniana złożoność dotyka również zabezpieczeń sieci. Zwiększająca się powierzchnia ataku i coraz bardziej zaawansowane zagrożenia sprawiają, że mechanizmy kontroli wbudowane w sieciach „poprzedniej generacji" nie radzą sobie z liczbą, dynamiką i zaawansowaniem cyberataków[2]. Tradycyjne oprogramowanie antywirusowe oparte na sygnaturach nie jest już zdolne do skutecznego działania, wskutek czego niezbędne jest wdrożenie mechanizmów wykrywania zagrożeń i reagowania na zagrożenia w czasie rzeczywistym.

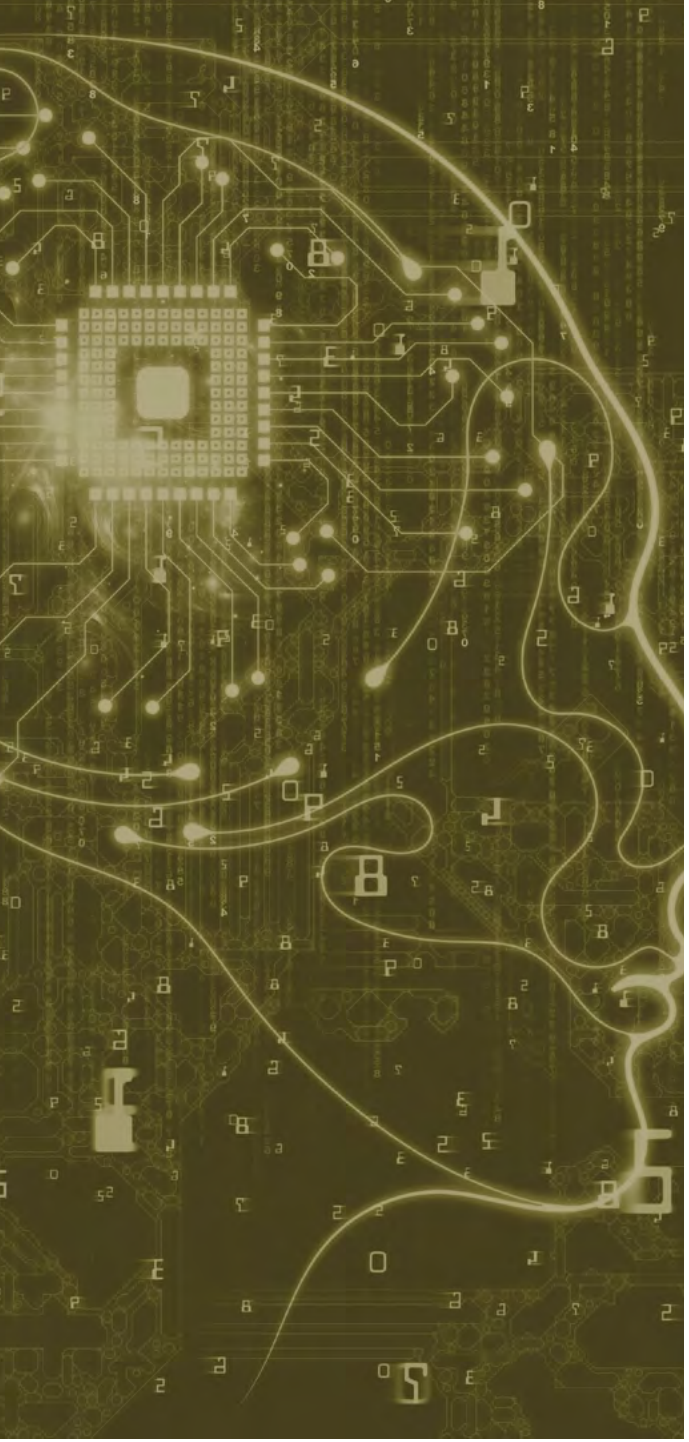
Z uwagi na te czynniki transformacja cyfrowa zbyt często wiąże się z przemęczeniem osób zajmujących się bezpieczeństwem sieci, których praca staje się coraz bardziej reaktywna niż proaktywna. Dla przedsiębiorstwa może to się zakończyć utratą danych lub przestojami spowodowanymi działaniem niewykrytych w porę zaawansowanych ataków. Tak jednak być nie musi.

[1] Benson Chan, „Digital transformation reimagines everything", Strategy of Things, 7 września 2017 r.
[2] „2018 Security Implications of Digital Transformation Report", Fortinet, 26 lipca 2018 r.



Codziennie od 28% do 40% nowych złośliwych programów śledzonych przez FortiGuard Labs służyło do przeprowadzania ataków typu „zero-day”.

FortiGuard Labs, wrzesień 2018 r.



SZTUCZNA INTELIGENCJA AUTOMATYCZNIE WYKRYWA ATAKI TYPU „ZERO-DAY”

Zastosowanie sztucznej inteligencji zaczyna mieć sens wówczas, gdy stale rosnąca moc procesorów pozwala komputerom na wykonywanie różnych rodzajów zadań szybciej i dokładniej niż ludzie. Świadczą o tym szybko rosnące inwestycje w technologie sztucznej inteligencji (według firmy IDC jest to prawie sześciokrotny wzrost w latach 2016 – 2020)[3].

W kontekście bezpieczeństwa sztuczna inteligencja jest obecnie coraz częściej stosowana do walki z cyberprzestępcami. Korzystając z mechanizmów uczenia maszynowego do analizy cech złośliwych plików, sztuczna inteligencja umożliwia najszybsze wykrywanie zaawansowanych zagrożeń, w tym coraz częściej pojawiających się ataków typu „zero-day” [4]. Oparta na informacjach przesyłanych przez funkcje sztucznej inteligencji automatyzacja zadań (takich jak tworzenie sygnatur lub obejmowanie kwarantanną i eliminowanie skutków naruszeń w czasie rzeczywistym) stanowi przyszłość systemów zabezpieczeń sieci[5].

Niestety cyberprzestępcy już teraz korzystają ze sztucznej inteligencji do tworzenia polimorficznego złośliwego oprogramowania nowej generacji, które samorzutnie tworzy całkowicie nowe, odpowiednio dostosowane do potrzeb hakerów zagrożenia[6]. W tym kontekście zastosowanie sztucznej inteligencji do obrony przed takimi zagrożeniami staje się podwójnie ważne.

[3] Margaret de Silva, „2017 was just the tipping point for AI”, Vision Critical, dostęp z dnia 20 sierpnia 2018 r.
[4] Rick M. Robinson, „Zero-Day Malware Poses a Growing Threat”, SecurityIntelligence, 1 maja 2017 r.
[5] Zeljka Zorz, „AI is key to speeding up threat detection and response”, Help Net Security, 14 sierpnia 2017 r.
[6] Derek Manky, „Fortinet FortiGuard Labs 2018 Threat Landscape Predictions”, Fortinet, 14 listopada 2017 r.; Kevin Townsend, „The Malicious Use of Artificial Intelligence in Cybersecurity”, SecurityWeek, 28 marca 2018 r.

Według firmy Constellation Research sztuczna inteligencja stanie się w 2018 r. głównym obszarem eksperymentów technicznych.

Courtney Sato, „AI and Internet of Things will drive digital transformation through 2020", ZDNet, 25 października 2017 r.

SZTUCZNA INTELIGENCJA OPTYMALIZUJE PRACĘ SPECJALISTÓW DS. BEZPIECZEŃSTWA SIECI

W przypadku działów zajmujących się zarządzaniem siecią i inżynierią sieci zastosowanie sztucznej inteligencji może pomóc w optymalizacji pracy zatrudnionego tam personelu przy jednoczesnym spełnieniu lub przekroczeniu ustalonych poziomów wydajności i bezpieczeństwa sieci. Ograniczone budżety, sprzeczne priorytety i istniejące niedobory specjalistów ds. cyberbezpieczeństwa (do 2021 r. brakować ma 3,5 mln takich specjalistów) oznaczają, że zwiększenie zatrudnienia w tych działach może okazać się niemożliwe, nawet jeśli byłyby na ten cel przeznaczone odpowiednie środki[7].

Nawet jednak nieograniczona liczba wspomnianych specjalistów nie rozwiązałaby problemu, ponieważ wywołane atakami szkody powstają szybciej niż może im zapobiec działanie nawet armii informatyków[8]. Według danych FortiGuard Labs od 28% do 40% nowych złośliwych programów służyło do przeprowadzania ataków typu „zero-day”[9].

Korzystanie ze sztucznej inteligencji w celu automatyzacji procesów wykrywania zagrożeń pozwala przedsiębiorstwu na przesunięcie najlepszych specjalistów ds. cyberbezpieczeństwa do realizacji bardziej strategicznych zadań. Jeśli przedsiębiorstwo ma ponadto zintegrowaną architekturę zabezpieczeń, która zapewnia scentralizowaną widoczność i automatyzację innych procesów bezpieczeństwa, przyjmuje wówczas postawę proaktywną, umożliwiając wspomnianym specjalistom planowanie działań przeciwdziałających przyszłym zagrożeniom, a nie zwykłe reagowanie na zagrożenia z przeszłości.

[7] Ryan Kh, „How AI is the Future of Cybersecurity”, Infosecurity, 1 grudnia 2017 r.
[8] Laurent Gil, „The Debate is Over: Artificial Intelligence is the Future for Cybersecurity”, SC Media, 22 marca 2018 r.
[9] FortiGuard Labs, wrzesień 2018 r.

„Twierdzenie, że ogromne problemy z bezpieczeństwem, z którymi obecnie borykają się przedsiębiorstwa, można rozwiązać przez zwiększenie liczby pracowników działu IT, jest naiwne”.

Laurent Gil, „The Debate is Over: Artificial Intelligence is the Future for Cybersecurity”, SC Media, 22 marca 2018 r.

W JAKI SPOSÓB SZTUCZNA INTELIGENCJA POMAGA POPRAWIĆ BEZPIECZEŃSTWO SIECI

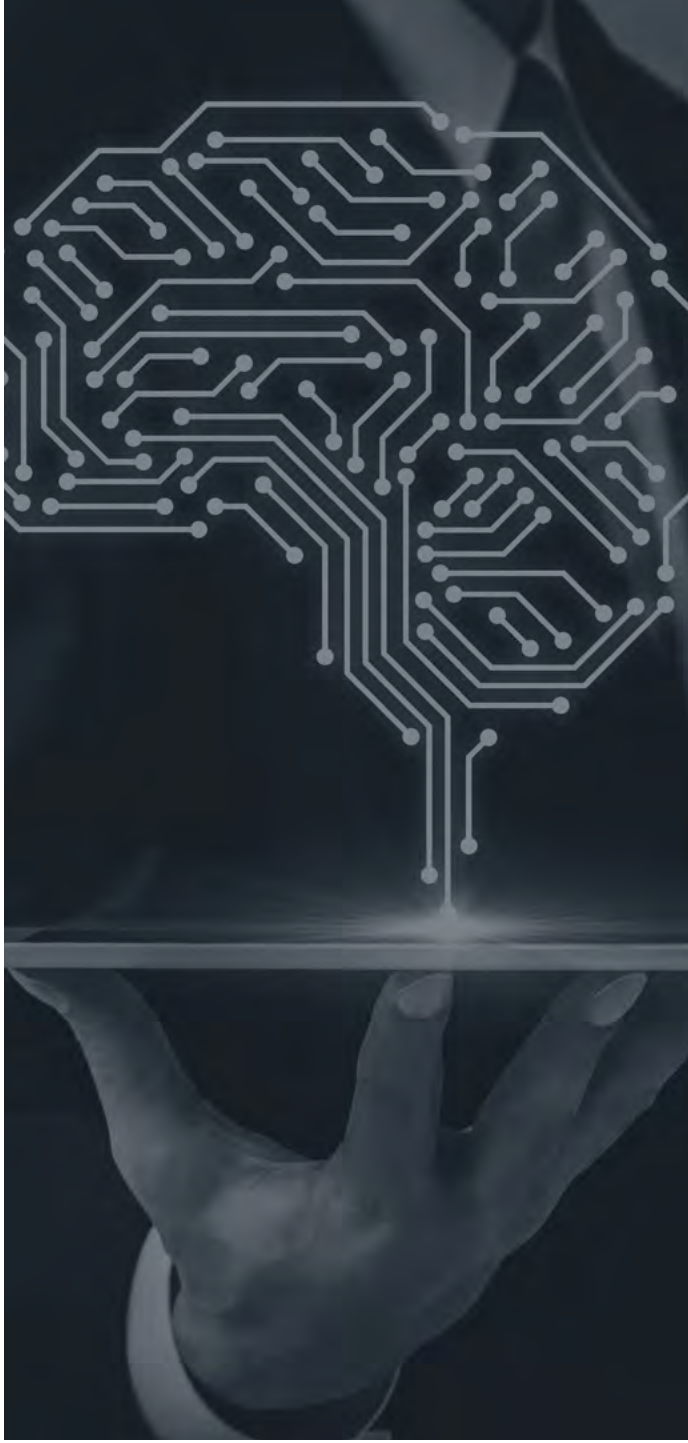
Wdrożenie sztucznej inteligencji to ostatni etap na drodze do uzyskania zdolności do wykrywania w czasie rzeczywistym znanych i nieznanych zagrożeń. Wykracza to poza zwykłe funkcje tworzenia sygnatur wirusów i rozpoznawania wzorców zachowań oraz oznacza wdrożenie samorozwijających się systemów wykrywania zagrożeń (SEDS). Zapewnienie takim systemom przydatnych informacji o zagrożeniach wymaga trzech następujących elementów:

- **Sztuczna inteligencja**. Zdolność komputera do imitowania procesów myślowych ludzi.
- **Uczenie maszynowe**. Korzystanie z danych w celu doskonalenia sposobu, w jaki komputery dokonują przewidywań lub wykonują zadania, ucząc się podejmowania decyzji we własnym zakresie i reagowania na nowe sytuacje.
- **Uczenie głębokie**. Technika uczenia maszynowego, w której dane są filtrowane przez samoregulujące się sieci luźno przypominające neurony w mózgu człowieka.

Systemy SEDS nieustannie korzystają z technologii uczenia maszynowego, w tym czasami z technologii uczenia głębokiego, w miarę upływu czasu są zatem zdolne do coraz dokładniejszego wykrywania zagrożeń. W procesie uczenia waga każdej cechy zagrożeń może być korygowana w miarę ich rozwoju, a jednocześnie mogą być rejestrowane nowe cechy w miarę ich wykrywania[10]. Im więcej danych zasili taki system, tym dokładniejsze będą wyniki jego działania.

„Specjaliści ds. zabezpieczeń korzystający z funkcji sztucznej inteligencji... są bardziej efektywni od swoich odpowiedników lub wręcz całych centrów zarządzania bezpieczeństwem, które nie korzystają z takich funkcji”.

Zeljka Zorz, „AI is key to speeding up threat detection and response”, Help Net Security, 14 sierpnia 2017 r.



[10] Nick Ismail, „How artificial intelligence can stop the malware threats of the future”, Information Age, 14 listopada 2017 r.

W JAKI SPOSÓB ZABEZPIECZENIA UCZĄ SIĘ WYKRYWAĆ ZŁOŚLIWE OPROGRAMOWANIE

Do właściwego działania systemy SEDS wymagają dużej ilości danych i odpowiednich zasobów. Zadaniem dużych sztucznych sieci neuronowych (ANN), czyli systemów sprzętu i oprogramowania połączonych w sieć na wzór neuronów połączonych w mózgu człowieka, jest codzienne rejestrowanie, analizowanie i klasyfikowanie milionów zagrożeń. Następujące potem „uczenie" algorytmów sztucznej inteligencji obejmuje trzy różne rodzaje tego uczenia[11]:

1. **Uczenie nadzorowane.** Zasilanie systemu prawidłowo oznaczonymi danymi, które system ten następnie analizuje, a wyniki tej analizy stosuje do danych nieoznaczonych.
2. **Uczenie nienadzorowane.** Zasilanie systemu nieoznaczonymi danymi, które system ten analizuje pod kątem ewentualnych wzorców, a wyniki tej analizy stosuje w celu odpowiedniego oznaczenia tych danych.
3. **Uczenie ze wzmocnieniem.** Optymalizacja działania systemu w drodze zasilania go nieoznaczonymi danymi i „dawania mu nagród" za dobre wyniki.

Taki kompleksowy, realizowany w dłuższym czasie proces uczenia skutkuje rejestracją miliardów próbek, które są poddawane szczegółowej analizie pod kątem cech i zachowań sugerujących, czy dany plik jest złośliwy, czy niezłośliwy (czysty). Wynikiem takiej analizy jest natychmiastowa decyzja o wysokim stopniu dokładności, która ewentualnie pozwala na podjęcie działań naprawczych w czasie rzeczywistym.

„Próba [ręcznego] oznaczania danych byłaby bardzo czasochłonna... często o wiele łatwiej jest po prostu pozwolić komputerowi na wyręczenie nas w odpowiednim pogrupowaniu takich danych".

Eliezer Kanal, „Machine Learning in Cybersecurity", SEI Blog, Carnegie Mellon University, 5 czerwca 2017 r.

[11] „Machine Learning 101: Supervised, Unsupervised, Reinforcement & Beyond", Towards Data Science, 28 sierpnia 2017 r.

JAK WYBRAĆ WŁAŚCIWE ZABEZPIECZENIA SIECI OPARTE NA SZTUCZNEJ INTELIGENCJI

Wielu dostawców zabezpieczeń korzysta już w oferowanych rozwiązaniach z różnych funkcji sztucznej inteligencji, duża część tych dostawców bardzo mgliście przedstawia jednak efekty działania tych funkcji. Poniżej przedstawiono kilka zagadnień, na które należy zwrócić uwagę przy wyborze właściwego rozwiązania:

1. **Rzeczywisty system SEDS.** Czy dostawca stosuje rzeczywisty system SEDS, który dostosowuje swoje analizy do zachodzących w czasie rzeczywistym zmian w charakterystyce zagrożeń?

2. **Rozmiar bazy danych o zagrożeniach.** Jak duża jest posiadana przez dostawcę baza danych o zagrożeniach oraz jak długo na jej podstawie dany model się uczy? Im większa baza danych i im dłuższy okres uczenia się, tym skuteczniejsze rezultaty można będzie odnotować.

3. **Korzystanie ze wszystkich trzech modeli uczenia maszynowego.** Czy dostawca uczy algorytmy sztucznej inteligencji za pomocą wszystkich tych trzech modeli (uczenie nadzorowane, uczenie nienadzorowane i uczenie ze wzmocnieniem)?

4. **Funkcje sztucznej sieci neuronowej.** Czy dostawca korzysta ze sztucznej sieci neuronowej do analizowania przychodzących plików? Ile aktywnych węzłów i czujników bezpieczeństwa ma oferowana przez dostawcę sztuczna sieć neuronowa? Wspomniane funkcje będą mieć kluczowe znaczenie w kontekście rosnącej liczby zagrożeń.

5. **Funkcje wykrywania elementów służących do szyfrowania złośliwego kodu.** Czy rozwiązanie dostawcy przeprowadza głęboką inspekcję elementów służących do szyfrowania złośliwego kodu i przesyła wyniki tej inspekcji do wszystkich zabezpieczeń sieci przedsiębiorstwa?

6. **Integracja architektury.** Czy rozwiązanie dostawcy wchodzi w skład zintegrowanej architektury zabezpieczeń, która zapewnia dobrą widoczność i scentralizowane mechanizmy kontroli dostępu w ramach całej sieci przedsiębiorstwa, oraz jest zdolne do przesyłania w czasie rzeczywistym informacji o zagrożeniach do wszystkich elementów systemu zabezpieczeń przedsiębiorstwa? Dodawanie kolejnego odrębnego „silosu” do posiadanej architektury zabezpieczeń nie jest produktywne.

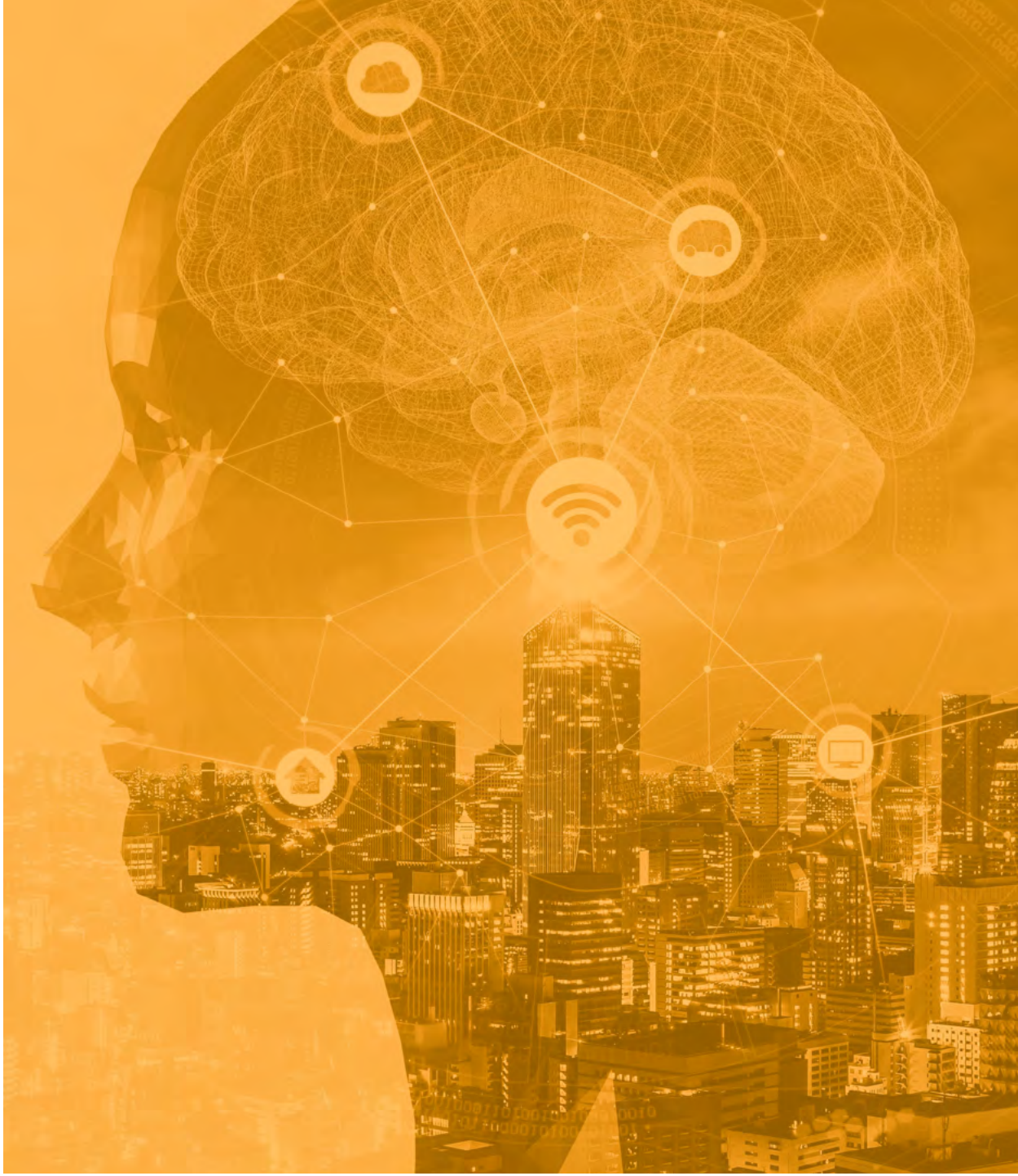
„Nie ma się co oszukiwać. Przyszłością cyberbezpieczeństwa jest akceptacja i rozwój partnerstwa człowieka z komputerem, w ramach którego będzie można skutecznie walczyć z hakerami”.

Laurent Gil, „The Debate is Over: Artificial Intelligence is the Future for Cybersecurity”, SC Magazine, 22 marca 2018 r.

PODSUMOWANIE

Bez wątpienia funkcje sztucznej inteligencji muszą być obecnie elementem każdej strategii zabezpieczenia sieci przedsiębiorstwa. Cyberprzestępcy już z tych funkcji korzystają, aby uczynić w ten sposób swoje złośliwe oprogramowanie trudniejszym do wykrycia oraz szybszym i bardziej destrukcyjnym w działaniu. Jedynie sztuczna inteligencja jest dziś zdolna do wykrycia ataków typu „zero-day" na podstawie zachowania i innych cech takich ataków. Powiązana ze sztuczną inteligencją automatyzacja poprawia również efektywność działu ds. bezpieczeństwa, pozwalając mu skupiać się raczej na proaktywnym zapobieganiu atakom niż reaktywnym usuwaniu ich skutków.

Podobnie jak w przypadku wszystkich aspektów zarządzania sieci, przy projektowaniu każdego rozwiązania najlepsze jest podejście strategiczne. Rozwiązanie kompleksowe i zintegrowane, które będzie utrzymywać dział ds. bezpieczeństwa w trybie proaktywnym, jest bowiem zdecydowanie lepsze od dodania do architektury bezpieczeństwa sieci kolejnego silosu, który będzie utrzymywać dział ds. bezpieczeństwa w trybie reaktywnym.



SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1.408.235 7700
www.fortinet.com/sales

BIURO SPRZEDAŻY — REGION EMEA
905 rue Albert Einstein
06560 Valbonne
Francja
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY — REGION APAC
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapur 038988
Tel: +65-6395-7899
Faks: +65-6295-0015

CENTRALA — AMERYKA ŁACIŃSKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel.: +1 954 368 9990

POLSKA
ul. Złota 59
Budynek Lumen II (6 piętro)
00-120 Warszawa
Polska

246201-0-A-PL 13 lutego, 2019 3:02 PM

ebook-using-ai-to-address