

# Nieważne, co myślisz o sztucznej inteligencji

nie powinieneś  
jej ignorować!

## RAPORT TOP 50 SECURITY 2018

Dział analityczny a&s International zestawiał notowane na giełdzie firmy z branży security o globalnym zasięgu i porównał ich przychody ze sprzedaży produktów zabezpieczeń technicznych w 2017 r.

## TOP 10 ŚWIATOWI PRODUCENCI SECURITY

(na podstawie przychodów ze sprzedaży w 2017 r.)

1	HIKVISION DIGITAL TECHNOLOGY	Chiny
2	DAHUA TECHNOLOGY	Chiny
3	ASSA ABLOY	Szwecja
4	BOSCH SECURITY SYSTEMS	Niemcy
5	AXIS COMMUNICATIONS	Szwecja
6	FLIR SYSTEMS	USA
7	ALLEGION	USA
8	HANWHA TECHWIN	Korea Płd.
9	TIANDY TECHNOLOGIES	Chiny
10	AVIGILON	Kanada



Tegoroczna lista a&s TOP 50 Security potwierdza, że branża światowych producentów zabezpieczeń technicznych odnotowuje stały wzrost – ubiegłoroczne przychody większości firm notowanych w zestawieniu wrosły średnio o 4,1 proc. Wśród najważniejszych kierunków rozwoju wyraźnie widocznych w ostatnich 12 miesiącach na pierwszy plan wysuwają się zaawansowane narzędzia analizy, które dają użytkownikom pełniejszy obraz sytuacji biznesowej. Wiele firm sprzedaje swoje rozwiązania pod hasłem „sztucznej inteligencji” (AI – Artificial Intelligence), choć są też dostawcy niechętnie używający tego terminu. Bez względu na to, czy rzeczywiście mamy do czynienia z AI, zaawansowane narzędzia analityczne umacniają się na rynku i w najbliższych latach będą miały duży wpływ na zapewnienie bezpieczeństwa.

Raport TOP 50 Security składa się z trzech części. Część pierwsza zawiera dyskusję na temat sztucznej inteligencji oraz prognozy na nadchodzący rok. W części drugiej zostały przytoczone opinie integratorów systemów dotyczące sektorów gospodarki o największym wzroście sprzedaży w ostatnim roku. Trzecią część stanowi podsumowanie rynku i technologii w 2018 r. przeprowadzone przez firmę Memoori, będące jednocześnie kompleksowym przeglądem branży zabezpieczeń technicznych.

#### AI: przełomowa technologia czy medialny szum?

Jeśli mielibyśmy wskazać najważniejszy trend w branży zabezpieczeń w ciągu ostatnich 12 miesięcy, to byłoby nim z pewnością wykorzystanie zaawansowanych mechanizmów analityki, które często określa się mianem sztucznej inteligencji. W jaki sposób mogą one przyczynić się do poprawy bezpieczeństwa i dlaczego niektórzy rynkowi gracze kwestionują termin „AI”?

#### Zwolennicy podkreślają zalety AI

W porównaniu do często przereklamowanej analityki obrazu (VCA) sprzed lat w zastosowaniach security, współczesne mechanizmy osiągnęły już pewien poziom dojrzałości i okazały się skuteczne

w takich zastosowaniach, jak rozpoznawanie obiektów czy inteligentne wyszukiwanie. Stało się to możliwe dzięki kilku czynnikom, takim jak większa moc obliczeniowa procesorów, bardziej zaawansowane, skuteczniejsze algorytmy, dużo większa dostępność danych, na których systemy mogą się uczyć, oraz zrozumienie potrzeb różnych branż. W efekcie powstają rozwiązania ułatwiające użytkownikom osiągnięcie większej efektywności i świadomości sytuacyjnej. Wykorzystanie technologii sztucznej inteligencji wraz z oprogramowaniem do analizy zawartości obrazu znacząco wpływa na rozwój rynku, zapowiadając jednocześnie utrzymanie tego trendu w najbliższej przyszłości. Technologia ta staje się coraz bardziej popularna, pozwalając zwiększyć ogólną efektywność podejmowania decyzji – mówi Saurabh Pradeep Sortee, analityk z Grand View Research. – Implementacja algorytmów sztucznej inteligencji w systemach security pozwala na stosowanie inteligentnych rozwiązań ochrony obwodowej, z pełną automatyzacją wykrywania intruzów i podejmowania właściwych działań.



**Kenneth Hune Petersen**  
CMO, Milestone Systems

– AI zdecydowanie zwiększa swój udział w całym rynku zabezpieczeń, ponieważ instalacje są coraz większe, zawierają większą liczbę różnych czujników i kamer. Nie jest możliwe, by człowiek był w stanie monitorować wszystkie napływające informacje – uważa Kenneth Hune Petersen, dyrektor Działu Marketingu w Milestone Systems. – Aby maksymalnie wykorzystać informacje z zainstalowanych urządzeń, należy użyć sztucznej inteligencji do właściwego interpretowania danych.



**Willem Ryan**  
wiceprezes, Avigilon

– Liczba kamer i nagrań wideo jest obecnie tak duża, że operatorzy muszą znaleźć sposób, by sobie z nimi radzić. Co więcej, potrafią skupić uwagę na krótko. W rozwiązaniu tego problemu może pomóc sztuczna inteligencja, która przeanalizuje o wiele więcej danych wizyjnych, niż mógłby to zrobić człowiek – twierdzi Willem Ryan, wiceprezes ds. marketingu i komunikacji w Avigilon. – Wspomagane sztuczną inteligencją oprogramowanie do zarządzania wideo pozwala operatorom zwiększyć wydajność i skuteczność pracy bez potrzeby ciągłego obserwowania obrazów na monitorach. Dzięki automatyzacji wykrywania mogą teraz szybko weryfikować krytyczne zdarzenia i reagować na nie. A to nie tylko przyspiesza działania dochodzeniowo-śledcze, ale także umożliwia reakcję na zdarzenia w czasie rzeczywistym.



**Dror Sharon**  
prezes Magal Security Systems

Jednym z przykładów zastosowań jest automatyczne wyszukiwanie obiektu. W tym przypadku użytkownik nie musi już spędzać wielu godzin na żmudnym przeglądaniu zarejestrowanego materiału. Wystarczy wprowadzić pytanie, by szybko otrzymać odpowiedni fragment archiwalnego nagrania. – Dahua jest liderem branży w zakresie korzystania z technologii AI, zwłaszcza stosowania analizy kognitywnej w wymagających rozwiązaniach security. Przy tysiącach kanałów trudno wyszukiwać i przesyłać strumieniowo dane wideo. Technologia Dahua strukturyzuje te dane na podstawie cech charakterystycznych ludzi lub pojazdów, zapewniając funkcje wyszukiwania i analizę dwustopniową – podkreśla Gao Jiaqi, Overseas Marketing Director w Dahua Technology. Taką analizę daleko wykracza poza automatyczne wyszukiwanie. Przykładowo, oparte na AI rozpoznawanie twarzy może być bardzo skuteczne i dokładne w dopasowaniu osoby widocznej na ekranie do zdefiniowanej w bazie danych, nawet jeśli ta osoba ma częściowo zakrytą twarz.

– Sztuczna inteligencja i uczenie maszynowe zapowiadają znaczną poprawę wydajności istniejących aplikacji oraz wprowadzenie nowych, zaawansowanych funkcji, które wcześniej były niedostępne – mówi Dror Sharon, dyrektor generalny firmy Magal Security Systems. – Niezależnie od tego, czy wyzwaniem jest wizyjna detekcja zamaskowanej twarzy ukrytej w tłumie, czy też wyizolowanie charakterystycznej sygnatury naruszenia bezpieczeństwa z tła o wysokim szumie otoczenia, AI ma potencjał zwiększania wydajności w przyszłości.

#### AI ułatwia analizę biznesową w różnych branżach

– Oferując analizę kognitywną, Dahua powiększa zakres aplikacji o smart retail, in-



teligentne zarządzanie ruchem czy smart parking. Stosujące je organizacje mogą pracować dużo wydajniej, a to przekłada się na większe zyski – mówi Gao Jiaqi. Opracowując nowe strategie mające na celu poprawę wyników finansowych, mogą korzystać z bezcennych informacji uzyskanych z analizy biznesowej. Przykładowo, w centrach handlowych technologia analizy kognitywnej Dahua może posłużyć do identyfikowania ruchu klientów i określania wysokości czynszu pobieranego od sprzedawców za wynajem.

### Kontrowersje wokół AI

Niektórzy dostawcy i konsultanci, z którymi były prowadzone rozmowy, mieli problem z samym pojęciem „sztuczna inteligencja”. Według nich stosowane obecnie technologie to w najlepszym przypadku zaawansowana analityka, do sztucznej inteligencji wciąż im daleko.



**Pierre Racz**  
prezes i dyrektor generalny firmy Genetec

– Należy być ostrożnym z określaniem różnych rozwiązań inteligentnymi – ostrzega Pierre Racz z firmy Genetec. – Obecnie bardzo dużo mówi się o AI, które ma zapewniać ogromne zaawansowanie technologiczne. Prawda jest taka, że ta marketingowa „sztuczna inteligencja” w rzeczywistości nie jest jeszcze w stanie zapewnić nam obiecanych latających pojazdów czy w pełni inteligentnych autonomicznych samochodów. To nie jest jedyny krytyczny głos w dyskusji o sztucznej inteligencji...



**Anna Sliwon**  
Research Analyst, IHS Markit

– AI z impetem wkracza do branży security, ale stosowane na tym rynku rozwiązania są jeszcze ograniczone. Przed nami nadal długa droga do osiągnięcia prawdziwie inteligentnych rozwiązań security, które – bazując na inteligentnych systemach – potrafiłyby podjąć niezbędne decyzje dotyczące wymaganych akcji w określonych przypadkach. Nie chodzi jednak o działanie na bazie wcześniej napisanych algorytmów – tłumaczy Anna Sliwon, Research Analyst w IHS Markit.

– Mamy do czynienia z „zaawansowaną analityką”, a nie ze „sztuczną inteligencją”. AI jest znacznie szerszym pojęciem i obejmuje możliwości daleko wykraczające poza rozpoznawanie obiektów i ich klasyfikowanie – uważa Alex Ganin, Project Manager w BitRefine Group. – AI oznacza, że komputer dosłownie „myśli”. Aby spowodować to myślenie, należy połączyć wiele złożonych technologii.

Technologiom brakuje obecnie elementu predykcyjnego, np. zdolności przewidywania, że ktoś ma zamiar zrobić coś złego, ponieważ wykazuje zachowanie nietypowe dla jego profilu.

– Istnieje mnóstwo samouczących się algorytmów. Powstały one jeszcze długo przed obecnymi, bardzo obiecującymi algorytmami opartymi na sieciach neuronowych. Te samouczące się mechanizmy, które są w stanie przechwytać obiekty i porównać ich prędkość ze średnią prędkością obiektów w ich otoczeniu, są w gruncie rzeczy prymitywne. Trudno oczekiwać od nich, że automatycznie rozpoznają podejrzane zachowania danej osoby – twierdzi Alex Ganin. – Sieci neuronowe potrafią wyjątkowo dobrze rozpoznać wszelkie obiekty statyczne, począwszy od twarzy, skończywszy na obiektach w skanerze rentgenowskim. W ostatnim czasie

pojawiły się również konwolucyjne sieci neuronowe 3D. Algorytmy te umożliwiają ocenę złożonego wzorca ruchu w celu klasyfikacji zachowania obiektów. Wciąż jednak pozostaje wiele problemów do rozwiązania, zanim ta technologia będzie mogła zostać w pełni wykorzystana w dostępnych na rynku systemach zabezpieczeń. Gdy tylko to się stanie, będziemy mogli rozpocząć tworzenie prewencyjnych systemów CCTV.



**John Distelzweig**  
dyrektor generalny i wiceprezes ds. security w firmie FLIR Systems

– Na razie nie zaprezentowano publicznie, że produkty oparte na sztucznej inteligencji są w stanie dokonywać bardziej złożonych rozstrzygnięć, np. czy dana osoba działa w podejrzany sposób lub czy dane działanie jest typowe dla określonej osoby, sceny, środowiska – podkreśla John Distelzweig, dyrektor generalny i wiceprezes ds. bezpieczeństwa w firmie FLIR Systems.

Nie oznacza to jednak, że zaawansowana analityka – bez względu na to, jak się ją nazywa – jest faktycznie pozbawiona wartości. To bardzo złożona i potężna technologia, która otwiera ogromne perspektywy w niemal każdym aspekcie życia. Security jest tylko niewielką częścią możliwych zastosowań.

– Uczenie maszynowe i wnioskowanie statystyczne w programach, które dają iluzję inteligencji, zapewniają naszym użytkownikom końcowym większą użyteczność i funkcjonalność rozwiązań. Z ostatnich osiągnięć w zakresie technologii uczenia maszynowego, w szczególności w głębszych sieciach neuronowych, mogą obecnie korzystać wszyscy. Zastosowaliśmy te techniki do poprawy wydajności niektórych naszych kluczowych rozwiązań, m.in. w automatycznym odczycie tablic rejestracyjnych (ALPR) Genetec AutoVu – podsumowuje Pierre Racz. ■

## WARUNKI UDZIAŁU W RANKINGU TOP50

### W rankingu mogą uczestniczyć:

- dostawcy urządzeń i systemów z branży security, w tym produktów telewizji dozorowej, kontroli dostępu, sygnalizacji włamania i napadu oraz produktów z więcej niż jednego z tych segmentów, produkujący pod własną marką lub na zlecenie innych firm;
- firmy notowane na giełdzie (Uwaga: co roku a&s International uwzględnia również niewielką liczbę międzynarodowych firm nienotowanych na giełdzie, które udostępniają swoje poświadczane sprawozdania roczne. Ich udział w rankingu jest dokładnie analizowany pod kątem rozpoznawalności marki oraz udziału firmy w rynku międzynarodowym);
- firmy, które dostarczają sprawozdania finansowe za pełny 2016 r., pełny 2017 r. oraz za pierwszą połowę 2018 r. Sprawozdania muszą być sprawdzone lub zatwierdzone przez biegłego rewidenta.

W rankingu nie są uwzględniani: dystrybutorzy, integratorzy systemów, resellerzy, dealerzy, instalatorzy, agencje ochrony osób i mienia, firmy z branży ochrony informacji i bezpieczeństwa pożarowego. Nie są też uwzględniane przychody powiązane z działalnością w tych obszarach.

a&s nie ponosi odpowiedzialności za dane finansowe udostępnione przez firmy. Dla celów porównawczych kwoty podane w innych walutach niż USD zostały przeliczone na USD wg średniego kursu wymiany z dn. 11.07.2017 r. (notowania XE.com). Udział w rankingu i przekazanie wyników finansowych są bezpłatne i dobrowolne.