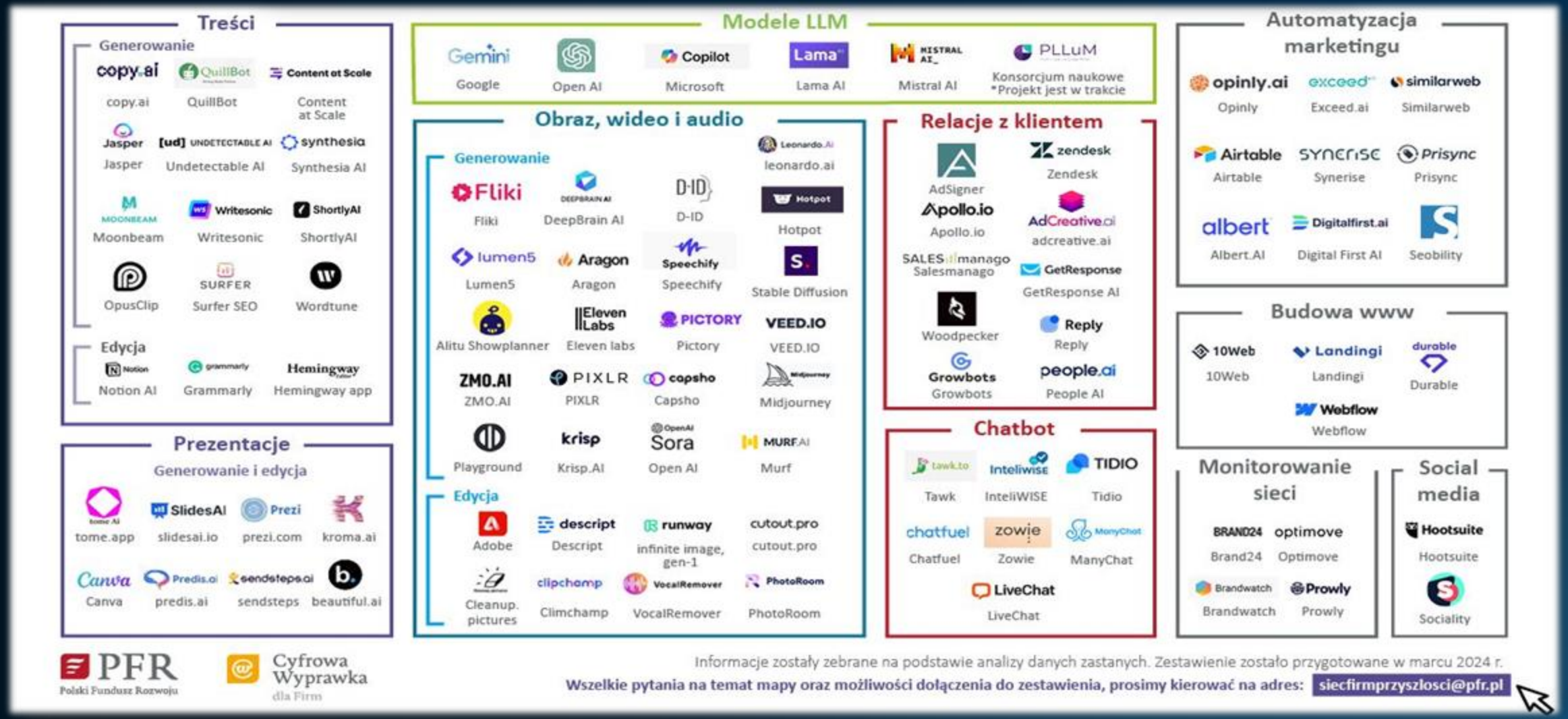
AI w rękach przestępców

Deepfake, phishing, „nowe metody” ataku z wykorzystaniem AI

Narzędzia AI



arcus KYOCERA

Cyberodporność

Cyberodporność to zdolność organizacji do:

- ✓ przygotowania się na incydenty,
- ✓ skutecznego reagowania,
- ✓ szybkiego powrotu do normalnego funkcjonowania przy minimalnych stratach i przestojach.

W dobie sztucznej inteligencji, zagrożenia:

- ✓ Są bardziej zaawansowane
- ✓ Są trudniejsze do wykrycia
- ✓ Proces odbudowy po ataku staje się bardziej złożony i kosztowny

Nowoczesna cyberodporność opiera się na AI – wykorzystując ją do predykcji zagrożeń, automatyzacji reakcji i przywracania ciągłości działania.

arcus KYOCERA

1

AI zagrożeniem dla cyberodporności?

arcus KYOCERA

Cyberzagrożenia

- ✓ **Sztuczna inteligencja** jest coraz częściej wykorzystywana przez grupy przestępcze do tworzenia szkodliwego oprogramowania (malware) i automatyzacji ataków.
- ✓ Modele generatywne, takie jak **ChatGPT**, mogą służyć do **tworzenia fragmentów szkodliwego kodu**, który następnie bywa dostosowywany do konkretnych celów (w tym ataków na wybrane organizacje).
- ✓ AI wspiera także **łamanie haseł metodą brute-force** – znacznie szybciej testuje miliony kombinacji, skracając czas potrzebny do przejęcia dostępu.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS > Learn how we made this table at hivesystems.io/password

AI w socjotechnice

Ataki, które obchodzą technologię – i uderzają w ludzi

- Socjotechnika to nie phishing sprzed dekady. To psychologia w służbie cyberprzestępczości, która dziś korzysta ze wsparcia sztucznej inteligencji.

AI

AI-powered phishing – atak nowej generacji
Wiadomości generowane przez AI są niemal nie do odróżnienia od prawdziwych: Styl pisma, logo, sygnatura, format – wszystko się zgadza.

- Pracownik dostaje e-mail od „dyrektora finansowego” lub „dostawcy” – i klika. Zdarza się to nawet w firmach z najlepszymi systemami bezpieczeństwa.

arcus KYOCERA

AI w socjotechnice – „phishing”

From: Kundenservice DHL Logistik [mailto:stegnitz@silometal.sk]
Sent: Wednesday, May 20, 2015 9:56 AM
To:
Subject: Obecny stan przesylki DHL

Sledzenie trasy przesylki DHL

DHL Sendungsverfolgung

Numer przesylki	49177414936436
Produkt / serwis	DHL RETOURE
Status od środa, 20.05.2015 07:55:19	Przesylka jest przygotowywana w poczatkowym centrum pakowania.
Doreczono do	Przesylka zwrotna do nadawcy

http://www.cetil.com.uy/4if30oexj8y
Kliknij, aby śledzić łącze

Sprawdź informacje od odbiorcy
(ZIP Format)

AI - „Deepfake” & „Cheapfake”

Deepfake – AI, która tworzy „kłamstwa” w jakości 4K

- ✓ Wideo z prezesem, który „mówi” coś, czego nigdy nie powiedział.
- ✓ Fałszywe nagranie rozmowy telefonicznej z Twoim CFO.
- ✓ Sztuczna inteligencja potrafi dziś stworzyć **realistyczny obraz, głos lub film**, który przekona każdego – również media.

Cheapfake – prosto i skutecznie

- ✓ To nie AI, a **proste triki montażowe**: przycięcie wypowiedzi, zmiana tonu, wyrwanie z kontekstu.
- ✓ Tanio, szybko i z dużym zasięgiem w mediach społecznościowych.

arcus KYOCERA

AI - „Deepfake” & „Cheapfake”

Forbes

PREMIUM

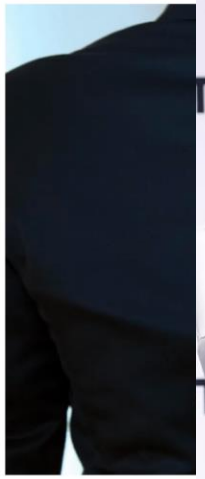
EDITORS' PICK

Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find

By Thomas Brewster , Forbes

Published Oct 14, 2021, 07:01am ED

Save Article



Cybercriminals cloned the voice of
heist. GETTY

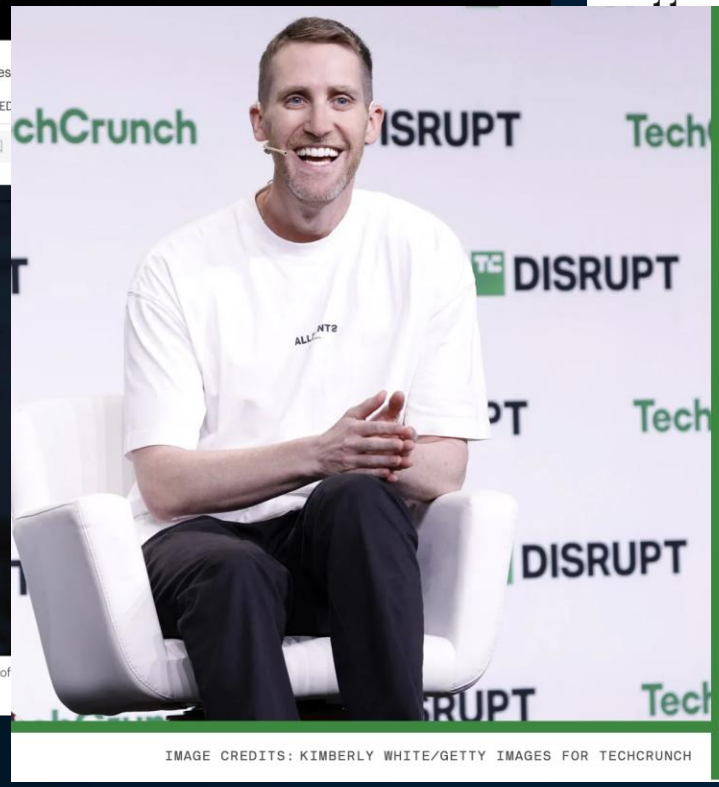


IMAGE CREDITS: KIMBERLY WHITE/GETTY IMAGES FOR TECHCRUNCH

SEARCH FORTUNE SIGN IN Subscribe Now

Home News Tech Finance Leadership Well Education Fortune 500

LEADERSHIP · CYBERSECURITY

Ferrari exec foils deepfake

SECURITY

Wiz CEO says co
targeted with de
that used his voi

Sarah Perez 11:10 AM PDT · October 28

CNN Business Markets Tech Media Calculators Videos Watch

Business / Tech

British engineering giant Arup revealed as $25 million deepfake scam victim

By Kathleen Magramo, CNN

3 minute read · Updated 4:53 AM EDT, Fri May 17, 2024

Zrzut ekranu

Dezinformacja: ciche zagrożenie dla Twojej organizacji

1. Wpływa na decyzje biznesowe – fałszywe dane mogą prowadzić do błędnych inwestycji i działań operacyjnych.

2. Podważa zaufanie – zarówno wewnętrzne (pracownicy), jak i zewnętrzne (klienci, partnerzy).

3. Wzmacnia skutki cyberataków – np. kampanie phishingowe oparte na zmanipulowanych informacjach.

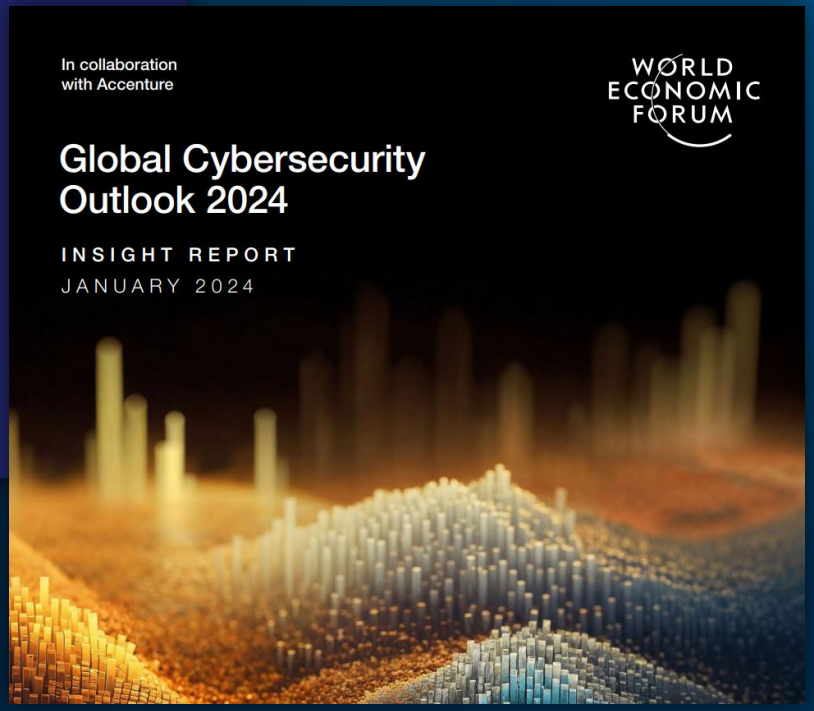
4. Trudna do wykrycia i neutralizacji – szczególnie w erze AI i deepfake'ów.

2

Konsekwencje cyberataków

arcus KYOCERA

Konsekwencje cyberataków



arcus

Konsekwencje cyberataków

Utrata informacji i danych

Przechwycenie wrażliwych i poufnych danych

Straty finansowe

Utrata zaufania klientów

arcus KYOCERA

Konsekwencje cyberataków

W 2024 roku liczba cyberataków na polskie firmy i organizacje osiągnęła rekordowy poziom, przekraczając 110 tysięcy ataków. Najbardziej zagrożone sektory to użyteczność publiczna oraz wojsko-rządowy, które były atakowane średnio ponad 2150 razy tygodniowo.

Wzrost liczby incydentów obsłużonych przez CSIRT NASK. W 2021 r. było to blisko 30 tys. incydentów, w kolejnym roku już prawie 40 tys. (wzrost o ok. 25% r/r), a w 2023 r. już ponad 80 tys. (wzrost o ponad 100% r/r).

Jednym z najistotniejszych zagrożeń dla bezpieczeństwa kraju stały się ataki APT (ang. Advanced Persistent Threat) sponsorowane przez wrogie państwa.

Wzrosła liczba ataków napędzanych przez sztuczną inteligencję - AI, Ransomware jako usługa (**RaaS**) oraz podatności typu „Zero-day” w przeglądarkach internetowych.

Szczególnie dotkliwe były ataki Ransomware, które dotknęły sektor opieki zdrowotnej i administracji rządowej, stanowiąc 67% wszystkich takich ataków, a średnia żądana kwota okupu w pierwszej połowie 2024 roku wynosiła ponad 5,2 miliona dolarów.

arcus KYOCERA

Agent AI

arcus KYOCERA

Agent AI

AI

Agent AI - to zaawansowany system oprogramowania, który wykorzystuje „sztuczną inteligencję” do realizacji zadań i osiągania celów „w imieniu” użytkowników.

Agenci AI „działają samodzielnie”, podejmując decyzje i wykonując zadania bez ciągłej „interwencji” człowieka.

Agenci AI mogą się uczyć na podstawie doświadczeń i danych, co pozwala im na ciągłe doskonalenie swoich umiejętności i adaptację do nowych sytuacji.

arcus KYOCERA

Agent AI – rozwój w kolejnych 24 miesiącach

Poziom 0

Teraźniejszość

„Naśladowanie” działań człowieka, automatyczne powtarzanie zadań.

Poziom 1

Od 3 do 6 miesięcy

Agent AI z elementami „rozumowania”, wykorzystujący narzędzia do osiągniecia celu.

Poziom 2

12 do 18 miesięcy

Samo-modyfikacja Agenta AI lub ulepszanie w celu osiągania założonych celów i zadań.

Poziom 3

18 do 24 miesięcy

Agent AI zdolny do bieżącego dostosowywania do zmieniających się warunków, oceniający pośrednie cele, zmierzając do wykonania zadania.

arcus KYOCERA

Agent AI – zagrożenia 2025 +

- ✓ Autonomiczne cyberataki
- ✓ Zatruwanie modeli AI, co prowadzi do błędnych decyzji i niewłaściwego działania systemów zabezpieczeń.
- ✓ Agenci AI mogą automatyzować procesy ataków
- ✓ Agenci mogą być używani do monitorowania, analizowania podatności i generowania oprogramowania szkodliwego.
- ✓ Sterowanie i zarządzanie infrastrukturą do generowania „Deepfake”, kampaniami informacyjnymi, generowaniem informacji głosowych.

arcus KYOCERA

„Shadow AI” – zagrożenia 2025 +

- **„Shadow AI”** odnosi się do nieautoryzowanego użycia narzędzi lub aplikacji sztucznej inteligencji przez pracowników lub użytkowników końcowych bez formalnej zgody lub nadzoru działu IT.
- Pracownicy często sięgają po te narzędzia, aby zwiększyć produktywność i przyspieszyć procesy, zwłaszcza gdy uważają, że zatwierdzone rozwiązania są niewystarczające lub zbyt wolne.

Ryzyka, zagrożenia dla organizacji:

- Bezpieczeństwo danych
- Zgodność z przepisami

(od 02.02.2025 r. obowiązuje rozporządzenie UE „AI Act”
- **Akt o Sztucznej Inteligencji**)*

- Utrata reputacji

arcus KYOCERA

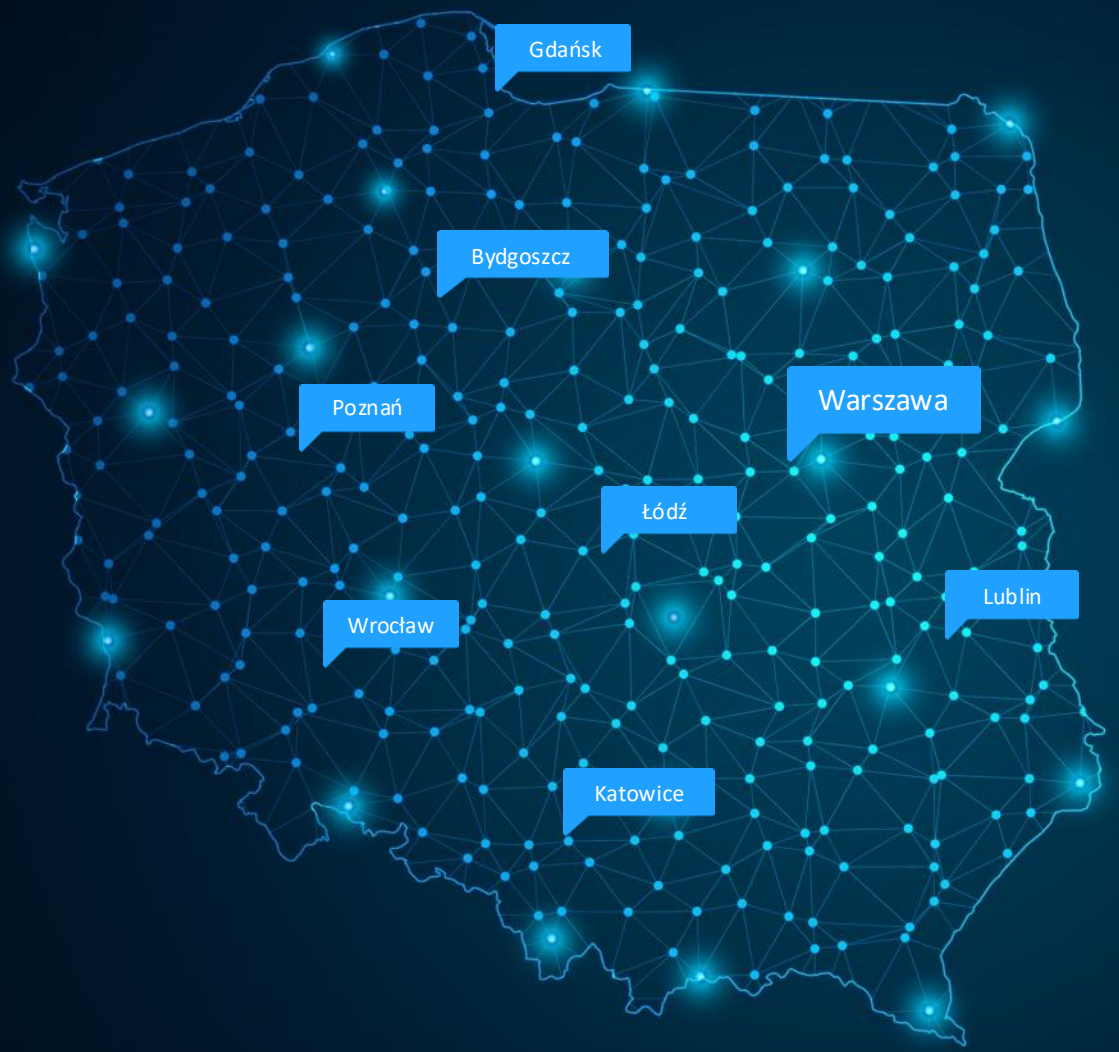
AI – cyberodporność - lista „To-Do”

Twoje działania na „dziś”?

- ✓ Rozpoznaj „swoje” ryzyka związane z użyciem modeli AI.
- ✓ Korzystaj z rozwiązań GenAI z rozwagą.
- ✓ Bądź ostrożny, zwłaszcza w sytuacjach „pod presją czasu” - sprawdzaj, weryfikuj i potwierdzaj podejmowane działania.
- ✓ W sytuacja krytycznych, wystąpienia incydentu, informuj innych, korzystaj z dostępnych kanałów i źródeł pomocy.
- ✓ Definiuj, kieruj, wskazuj oraz zarządzaj pracą realizowaną przez Agentów AI.

arcus KYOCERA

arcus docusoft arcus si geotik



Skontaktuj się z nami!

ARCUS S.A.
Kolejowa 5/7
01-217 Warszawa

handlowy@arcus.pl

(22) 536 08 00

www.arcus.pl

arcus docusoft arcus si geotik