Sztuczna inteligencja w cyber bezpieczeństwie kolejna moda czy rzeczywista potrzeba?

Tomasz Matuła, Wisła, 05.11.2024

Wszechogarniająca nas „inteligencja” …

Ecovacs Deebot X1e OMNI zasilany sztuczną inteligencją

Roboty jutra już dziś

Zupełnie nowy **flagowy produkt** do odku
luksusowe i bezproblemowe sprzątanie.

Robot uczy się Twoich zwyczajów

Nie musisz pamiętać gdzie i jak cz ysyłasz robota do sprzątania. Xplorer S13 AI zr obi to za Ciebie, proponując optymalne har mon gramy pracy, na bazie Twoich zwyczajów.

Robot uczy się Twoich potrzeb

Xplorer S130 AI sam przypomni Ci o dawno nie sprzątanym pomieszczeniu i zaproponuje, że tam

Inteligentny odkurzacz !

Inteligentne urządzenie, które przewyższa zwykły odkurzacz robotyczny - Lucy łączy w jednym inteligentnym urządzeniu unkcje odkurzacza i kamery monitoringu.

Oprócz sprzątania podłóg, może używać różnych kamer do patrolowania w ciągu dnia i nocy, a także monitorować zwierzęta domowe i członków rodziny.

4. **Rozpoznawanie i unikanie przeszkód:**

Zaawansowana technologia rozpoznawania obiektów pozwala Lucy **identyfikować i omijać przeszkody**, takie jak obiekty o wysokości do 2,5 cm.

5. **Monitoring w czasie rzeczywistym:**

Posiada kamerę HD i czujnik głębokości, umożliwiające monitorowanie domu w czasie rzeczywistym zarówno w dzień, jak i w nocy.

6. **Integracja z Alexą:**

Możliwość sterowania procesem sprzątania za **pomocą Asystenta Amazon Alexa**, co zwiększa wygodę obsługi.

7. **Aplikacja Trifo Home:**

Dedykowana aplikacja umożliwiająca ustawianie programów sprzątania, mapowanie pomieszczeń oraz zarządzanie obszarami, które mają być pominięte.

Aplikacja w języku Polskim!

8. **Łatwość czyszczenia:**

Duży pojemnik na kurz (**600 ml**) oraz możliwość mycia całego pojemnika i filtra ułatwiają utrzymanie urządzenia w czystości.

9. **Samo-nauka sztucznej inteligencji:**

Lucy staje się bardziej inteligentna w miarę pracy, dostosowując się do otoczenia za pomocą zaawansowanej technologii sztucznej inteligencji.

AI

Świat oszalał na punkcie GenAI

FORBES > INNOVATION

BT PROPERTY WEEK 2024

GenAI is about to reshape the real estate world

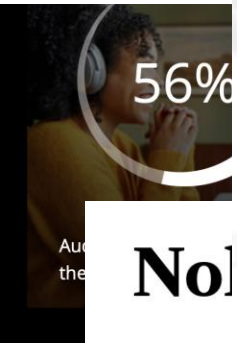
Generative
feed real es

/ Ekonomia / Praca / RYNEK PRACY

Boty AI wygryzają tych pracowników. Efekty przeszły najśmielsze oczekiwania

Skuteczność systemów sztucznej inteligencji w biznesie nie pozostawia złudzeń: zatrudnieni w niektórych działach nie mają szans w starciu z AI. Dziwi więc entuzjazm pracowników.

Aktualizacja: 04.03.2024 08:41 Publikacja: 04.03.2024 03:00



No

Wszechol
lepszego
zwiększa
Rewolucj
wielkiej zmianie, będą rozmawiać uczestnicy zbliżającego się

here – świecie, w
two

ent evaluation. It will also

lock generative AI's
tential: How to
sition your business
greater success and
oductivity

Wykorzystujemy sztuczną inteligencję od lat

Rozpoznawanie obrazów, wideo, mowy, pisma

Przemysł, predictive maintenance

Finanse i bankowość

Biometria behawioralna

Chatboty, voiceboty

Medycyna

Filtry antyspamowe

NGFW, NGAV, EDR

AI czyli właściwie co ?

AI Sztuczna Inteligencja

JAK działa:
- Ogromnie ilości danych
- Szybkie procesowanie
- Inteligentne algorytmy

Jak się uczy:
- W sposób ciągły
- Rozpoznawanie wzorców
- Znajdowanie wspólnych cech w danych

ML Uczenie maszynowe

Metody uczenia:
- nadzorowane,
- nienadzorowane
- poprzez wzmacnianie

Silna kontrola człowieka

Zdolność uczenia się bez konieczności programowania

NN Sieci neuronowe

Sieć sztucznych neuronów

Naśladuje działanie mózgu ludzkiego

Równoległe przetwarzanie

DL Uczenie głębokie

Ogromne zbiory danych

Wiele warstw sieci neuronowych

Działa na zbiorach nieustrukturyzowanych

Coraz mniej ważny człowiek

LLM, „Czarna skrzynka”

AI Analityczna

- Rozumienie i interpretacja danych
- Reaktywna – nie tworzy nowych danych

AI Generatywna (GenAI)

- Analizuje, interpretuje i (chyba☺) rozumie dane
- Kreatywna - tworzenie nowej treści

Kluczowe wyzwania organizacji w świecie Cyber

Kluczowe wyzwania organizacji w świecie Cyber

Migracja do chmury i SaaS postępuje ALE hybryda króluje

Pracować już zawsze będziemy inaczej

Supply Chain
Software Supply Chain

Ilość cyberzagrożeń i incydentów gwałtownie rośnie

”Tsunami” regulacyjne:
NIS 2, DORA, CER, AI Act

Konwergencja IT, OT i IIoT

Priorytety biznesowe stare i nowe

- TCO & Revenue Generation
- Customer journey
- Agile, mega fast development
- Modernizacja stacku technologicznego
- Totalna digitalizacja biznesu
- Innowacje, „owczy pęd” na wykorzystanie „nowinek” w tym AI
- Cyberodporność organizacji

Ewolucja cyber zagrożeń

Polska nie jest zieloną wyspą ☹

ESET (1H2025)

Polska na **1 miejscu na świecie** pod względem liczby wykrytych ataków ransomware

- Polska 6%
- USA 5,74%
- Słowacja 5,45%
- Ukraina 4,68%

Microsoft Defense Raport (styczeń 2025)

Polska **zajmuje 3. miejsce w Europie i 9. na świecie** pod względem narażenia na ataki sponsorowane przez obce państwa

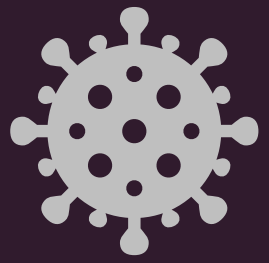
Wzrost ataków na:

- przemysł
- sektor energetyczny
- infrastruktury krytycznej
- zdrowie

Zewnętrzne

Ransomware

DDoS



Sztuczna Inteligencja

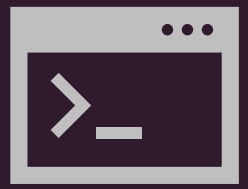
Istniejące cyber zagrożenia

Nowe cyber zagrożenia

Phishing

Wykorzystanie tożsamości

Znane podatności



Nowe podatności

Wewnętrzne

Cyber ataki na AI działające w organizacji

Ataki typu Prompt Injection

IT Dev - korzystanie z skompromitowanych modeli AI do generowania kodu

Ataki na prywatność – kradzież wrażliwych danych lub samego modelu

Ataki zatruwające w fazie szkolenia - wprowadzanie uszkodzonych danych

Wycieki wrażliwych informacji firmowych – niekontrolowane użycie publicznej GenAI

Nowa powierzchnia ataku

Cyber ataki z wykorzystaniem AI

Większa skuteczność PHISHING

Social Engineering & DEEPFAKE

Złośliwe LLMs

Lepszy i szybszy REKONESANS potencjalnych ofiar

EKSPLOITACJA PODATNOŚCI w krótszym czasie

Obchodzenie NGAV/EDR

Ewolucja cyberataków również dzięki AI

Cyber BIZNES

WIĘKSZA

GEOPOLITYKA

SKUTECZNOŚĆ

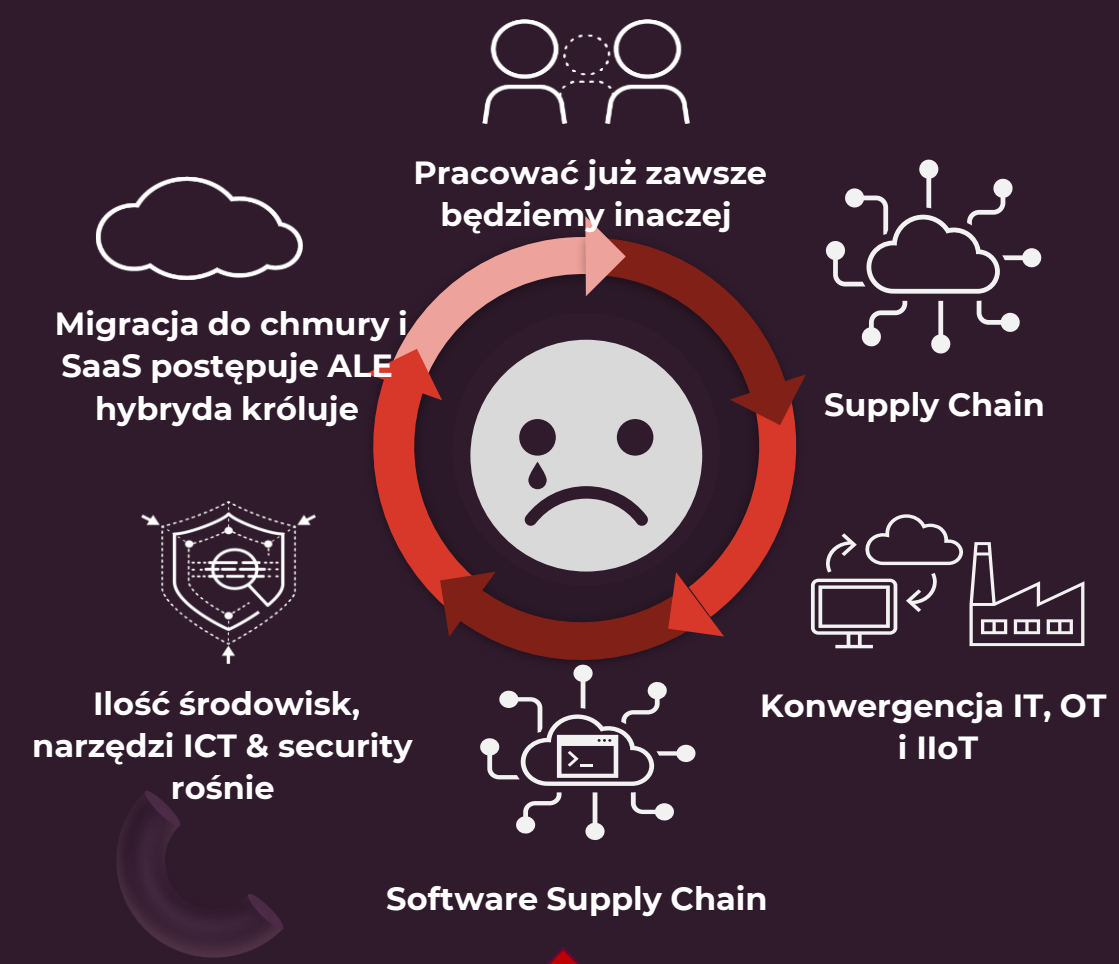
SZYBKOŚĆ

SKALA

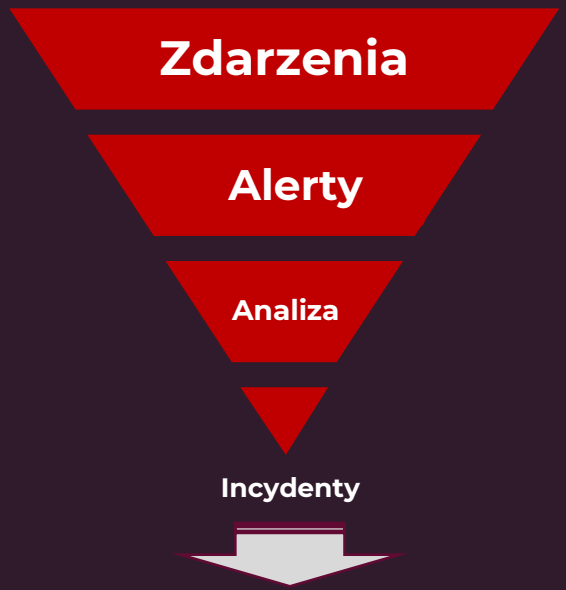
WYRAFINOWANIE

Ewolucja tego co musimy kontrolować

Za dużo third party, środowisk, zdarzeń, …



Rośnie powierzchnia ataku



Średni czas wykrycia hakerów

2022	2023	2024	2025
16 dni	10 dni	10 dni	12 dni
212 dni	207 dni	207 dni	210 dni

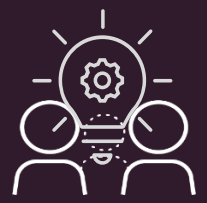
Czas potrzebny hakerom: 5-16 godzin

To „jak ma żyć” CISO czy CIO?
Czy i jak „AI” może pomóc?

Nie ma skutecznego cyberbezpieczeństwa bez …

Jak najwięcej dobrej jakości danych

(Natywna) Integracja i platform approach



Skuteczne algorytmy i ekspercka wiedza

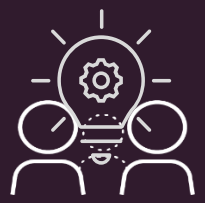
Automatyzacja

Działanie w czasie rzeczywistym

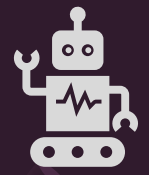
Czy i jak AI może pomóc w cybersec?

Jak najwięcej dobrej jakości danych

Integracja i platform approach

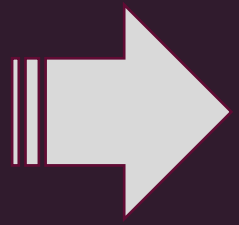


Skuteczne algorytmy i ekspercka wiedza



Automatyzacja

Real time



Analityczna AI

Machine Learning

Deep Learning

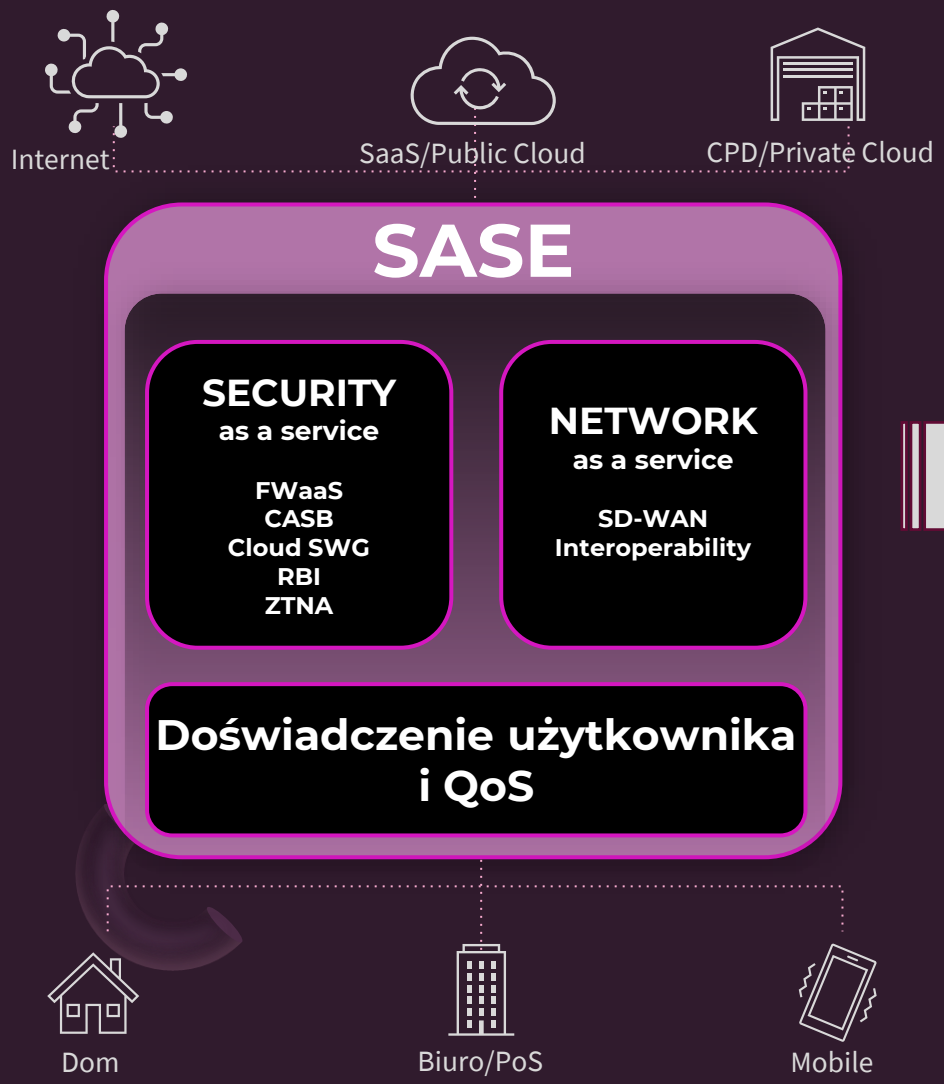
Dokładność, precyzja, działa w czasie rzeczywistym

Generative AI

GenAI

Wsparcie

Next Gen bezpieczny dostęp & SASE



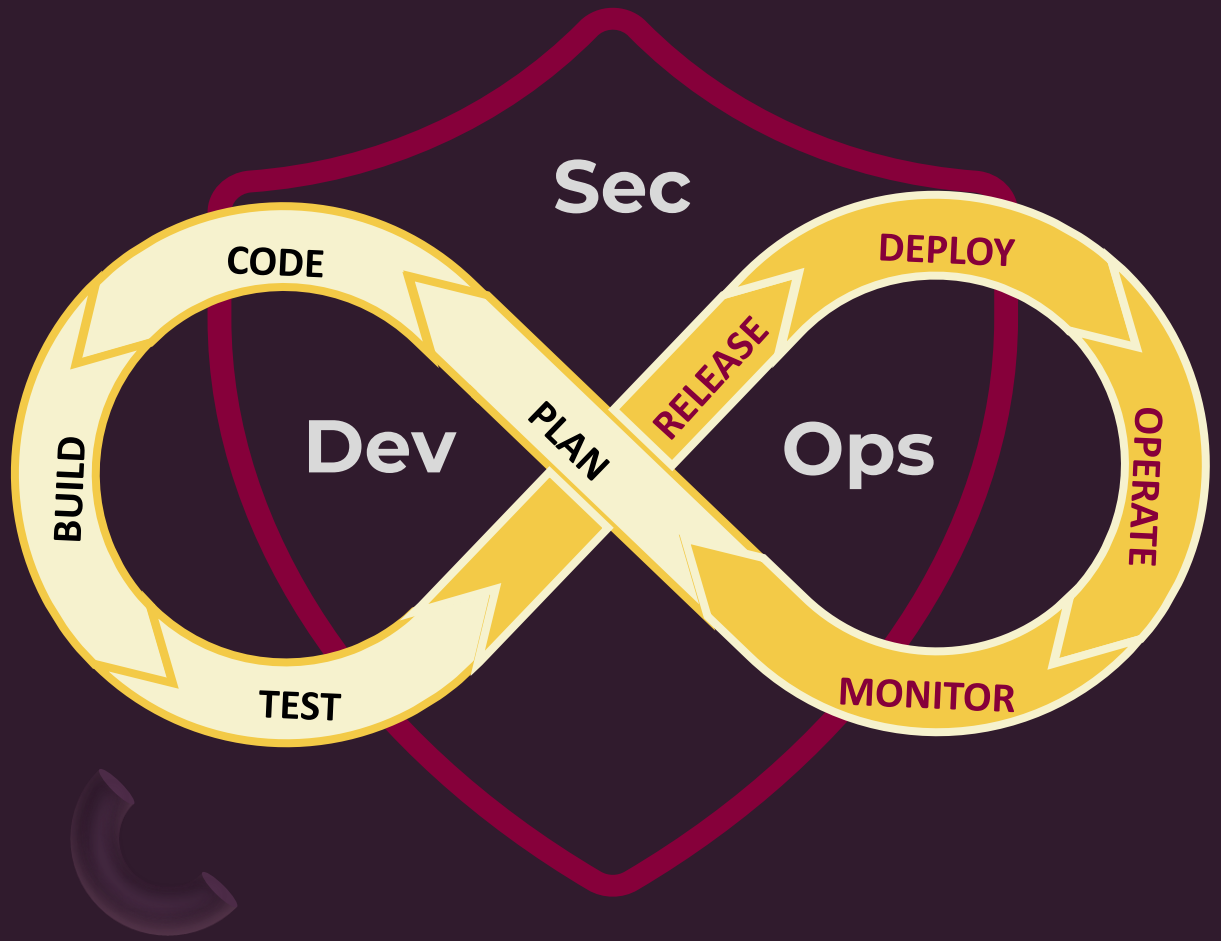
Korzyści

- Prawdziwe ZTNA
- Least-Privilege Access
- Ciągła weryfikcja kontekstu i zaufania
- Ciągła inspekcja security
- Ochrona wszystkich danych i wszystkich aplikacji

Zapracowane, proaktywne AI ;-)

- SandBox chmurowy na sterydach
- Inline DL real time zatrzymywania ataków typu Zero Day
- Wykrywanie podejrzanych logowań i aktywności użytkowników
- Zapobieganie real time nieznanym atakom C2
- Zapobieganie złośliwej zawartości w plikach inline
- Eliminowanie niebezpiecznych błędnych konfiguracji
- Proaktywne naprawianie problemów z QoS

SDLC & DevSecOps



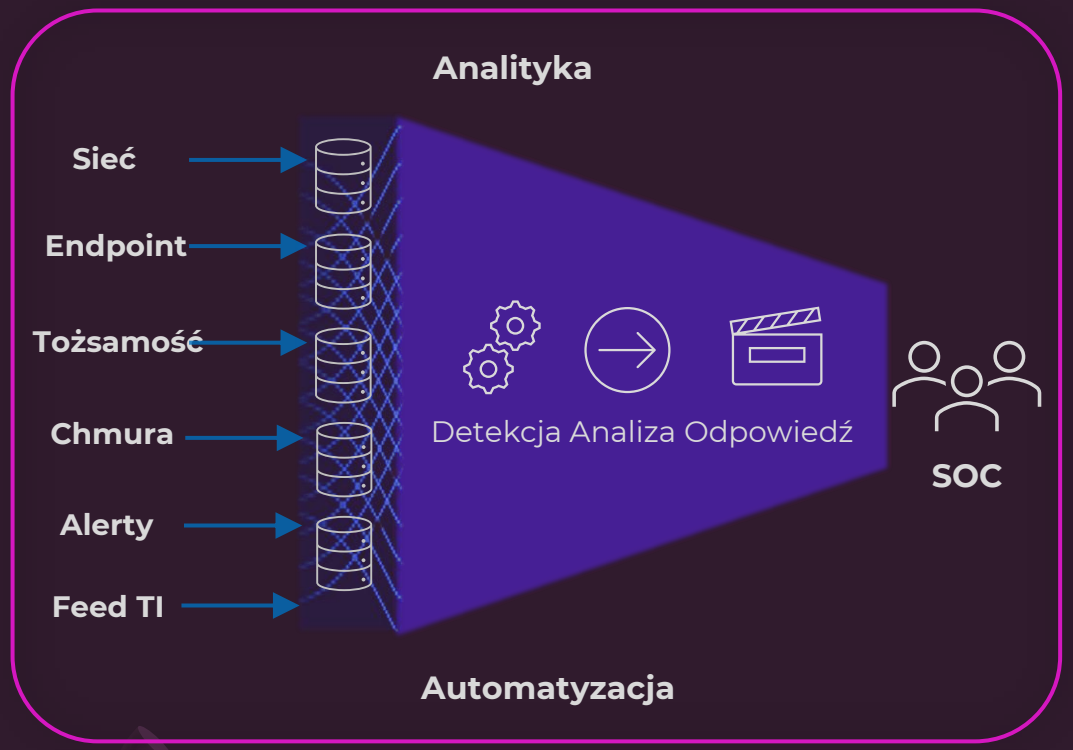
Wyzwania

- Multicloud + hybryda + software supply chain
- ”Szorstka przyjaźń” IT Dev, IT Ops i Security
- Agile, mega fast development
- Open Source Vulnerabilities
- Ochrona środowisk, danych i aplikacji
- **„Złe” modele AI do generowania kodu:**
  - Luki i tylne furtki
  - Prywatność i etyka
  - Jakość i legalność kodu

SecApps w całym cyklu życia

- Pełna widzialność Software Supply Chain
- Wykrywanie niebezpiecznych błędnych konfiguracji
- Wczesne wykrywanie podatności
- Właściwy dostęp do danych i kodu
- Runtime & workload protection
- Bezpieczeństwo API
- Malware scanning

SecOps & Next Generation SOC



NDR, EDR, XDR, SIEM, SOAR, UEBA, CDR, TI, ASM, ...

CEL: ~~obsługa~~ incydentów → zarządzanie

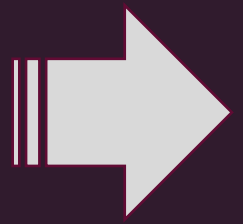
- Zbyt wiele informacji
- Zbyt wiele silosów danych
- Wiele narzędzi, duplikacja pracy
- Niewystarczający wgląd

Zapracowane, proaktywne AI ;-)

- Grupowanie alertów i ocena incydentów
- SOAR [2] - automatyzacja detekcji, analizy i odpowiedzi
- XDR na sterydach - wykrywanie i blokowanie:
  - Malware, C2,
  - Lateral movement, exfiltration
- Raportowanie
- Semi-autonomiczny, real-time SOC
- MTTD & MTTR – z dni do godzin i minut

Gen AI w cybersec – hit czy kit?

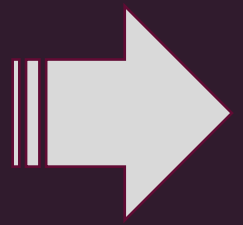
„Security coopilots” to game changer ?



NIE

Większa efektywność

- **Przejęcie czasochłonnych zadań**
- **Szybsza reakcja i automatyzacja odpowiedzi na ataki**
- **Szybszy wgląd i analizy**
- **Przygotowanie raportów**
- **„Nauczyciel” dla juniorów**



TAK

„Nie wszystko złoto co się świeci”

„Nie wszystko złoto co się świeci”

Woda smakowa truskawkowa

„Krystaliczna, górska woda źródlana z sokiem owocowym i naturalnym aromatem”

ALE

- 0.1% soku truskawkowego
- 1.5 l zawiera 60 g cukru = 12 łyżeczek cukru

Mintaj a’la łosoś

„Wędzone filety z mintaja w oleju roślinnym zachwycają swym wspaniałym smakiem”

ALE

- Solony, barwiony filet z mintaja, sól, ocet, barwniki (*żółcień pomarańczowa i czerwień koszenilowa), aromat dymu wędzarniczego, substancja konserwująca
- * mogą mieć szkodliwy wpływ na aktywność i skupienie uwagi dzieci

Ewolucja cyberataków również dzięki AI

Cyber BIZNES

WIĘKSZA

GEOPOLITYKA

- **SKUTECZNOŚĆ**
- **SZYBKOŚĆ**
- **SKALA**
- **WYRAFINOWANIE**
- **NOWE ZAGROŻENIA**

Nie ma skutecznego cyberbezpieczeństwa bez …

Jak najwięcej dobrej jakości danych

Automatyzacja

(Natywna) Integracja i platform approach

Działanie w czasie rzeczywistym

Skuteczne algorytmy

Ekspercka wiedza

„Nie wszystko AI (złoto) co się świeci”

Zapraszam do kontaktu

tomasz.matula@ictmasters.com