secureVISIO

Cyberbezpieczeństwo wspierane przez AI

Mateusz Majewski Esecure Sp. z.o.o.

secureVISIO

O nas

- Ponad 10 lat doświadczenia w produkcji oprogramowania z zakresu cyberbezpieczeństwa
- Pomagamy klientom w skutecznym zarządzaniu cyberbezpieczeństwem
- Dostarczamy i wdrażamy platformę SecureVisio, zapewniającą ochronę w obszarze prewencji, detekcji oraz reakcji na cyberzagrożenia

PREWENCJA

- Elektroniczna dokumentacja
- Analiza ryzyka cyberzagrożeń
- Zarządzanie podatnościami

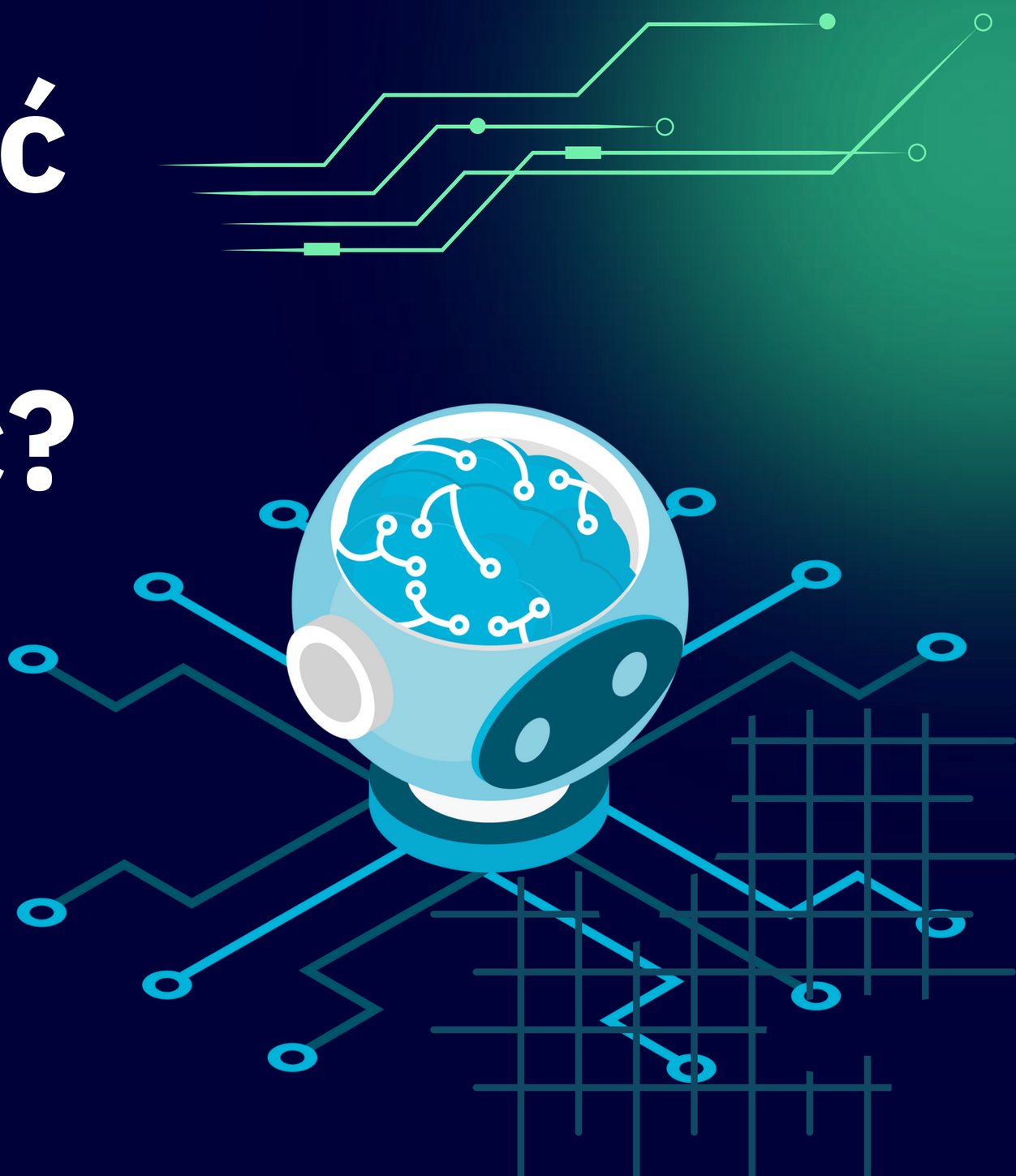
DETEKCJA

- SIEM
- Analiza behawioralna użytkownika/zasobu
- XDR

REAKCJA

- Automatyzacja obsługi incydentów

Jak wykorzystać AI w walce o cyberodporność?



secureVISIO

Wyzwania w zastosowaniu AI

Ograniczenia wydajności i efektywności

Właściwe wykorzystanie kontekstu – automatyzacja podpowiedzi (kontekstowy wybór logów do nauki – nie wszystkie logi są pod tym kątem wartościowe)

Bariera wejścia i koszty utrzymania (wysokie zużycie energii)

Problemy z niezawodnością – halucynacje (czasami nazywane bzdurami AI)

Jak to robimy?

1

Machine Learning

Służy do budowy modeli statystycznych

2

Deep Learning

Pomaga analizować korelacje medzy zdarzeniami

3

Large Language Model

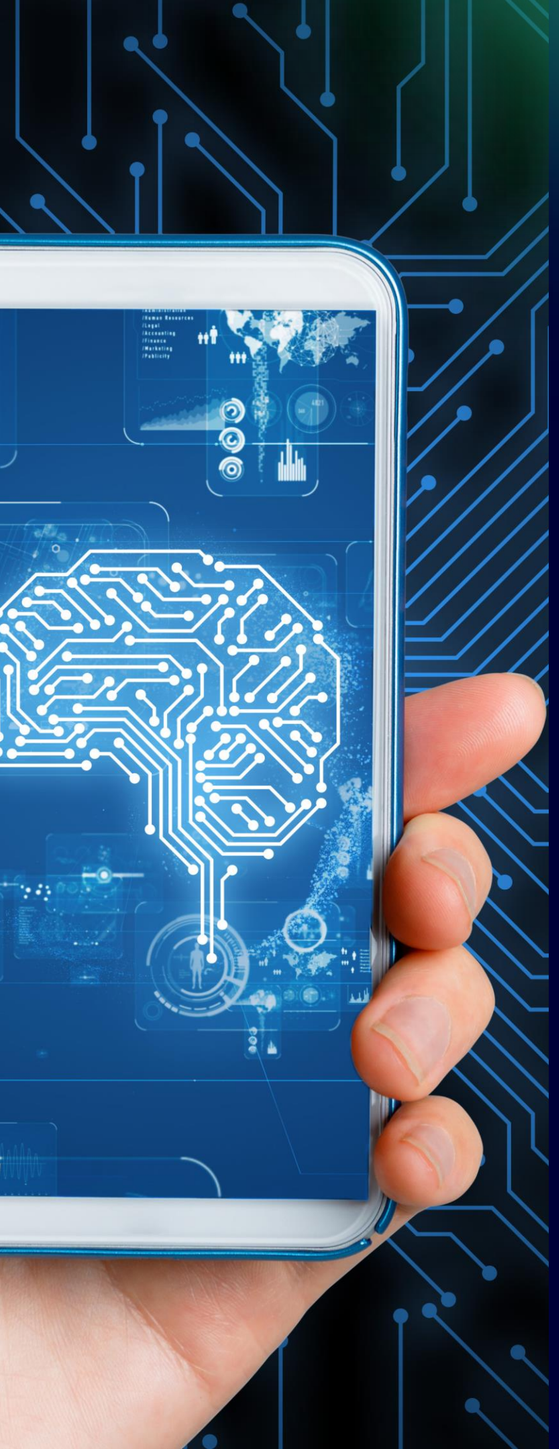
LLM to doskonałe narzędzie do prawidłowej interpretacji logów i zdarzeń związanych z bezpieczeństwem

4

Large Reconstruction Model

LRM jest niezbędny w analizie zdarzeń I kontroli playbooków

secureVISIO



MACHINE LEARNING

UCZENIE KONTEKSTOWE

Serwery WWW działają inaczej niż serwery lokalne lub punkty końcowe; administratorzy działają inaczej niż użytkownicy – kontekst na poziomie CMDB

UCZENIE OPARTE O METADANE

Metadane generowane podczas analizy logu są uwzględniane w procesie uczenia – kontekst na poziomie logu

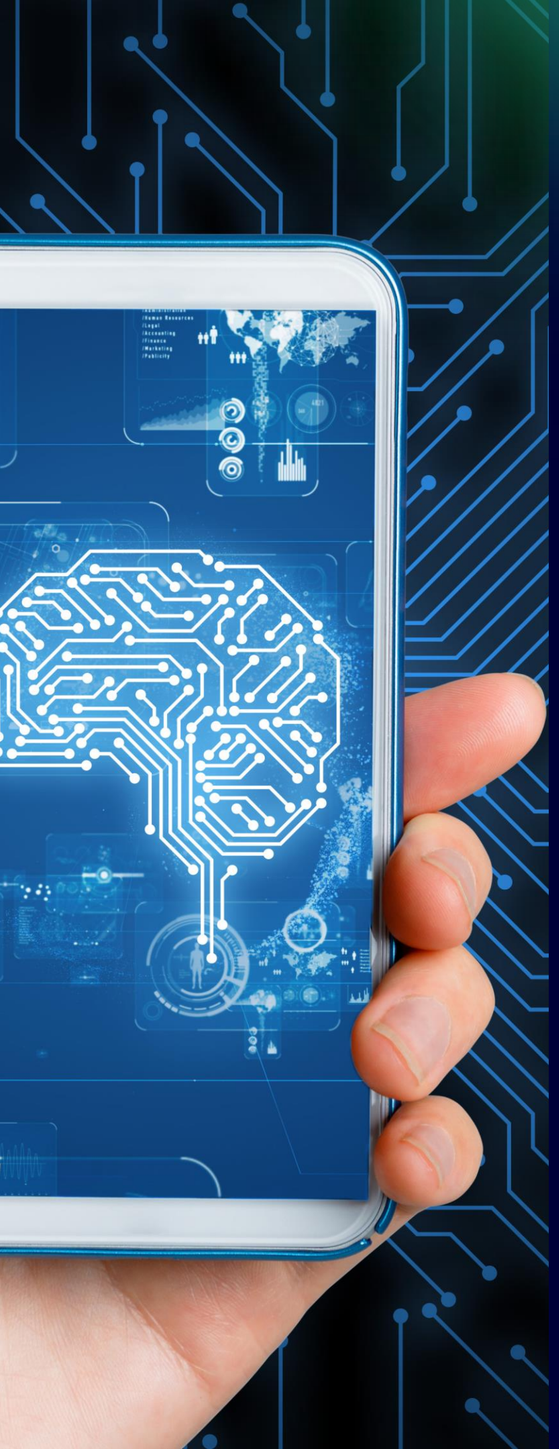
UCZENIE STATYSTYCZNE + WARTOŚCI PÓL

Uczenie statystyczne plus wartości pól – jak często zdarza się zdarzenie w kontekście tego, co się wydarzyło – znajdowanie anomalii w zdarzeniach kontra odkrywanie nowych procesów w organizacji

MĄDRZEJSZA NAUKA

Widząc i rozumiejąc więcej, możemy uczyć się szybciej, wykorzystując mniej zasobów

secureVISIO



DEEP LEARNING

UŻYTKOWNICY

Analiza zachowań użytkowników

KORELACJE

Zaawansowane mechanizmy uczenia korelują interakcje między użytkownikami i zasobami pracując na dużych zbiorach danych

ZASOBY

Analiza zachowań zasobów

WYDAJNOŚĆ

Współczynnik korelacji niemożliwy do osiągnięcia dla modeli językowych LLM

secureVISIO

MODELE JĘZYKOWE (LLM, LRM)

BAZA WIEDZY

Wykorzystanie modeli językowych (LLM) jako bazy wiedzy, np. na temat Mitre Att&ck, interpretacji logów, informacji o zagrożeniach, metod ataków i przeciwdziałań

WYSZUKIWANIE

Wykorzystanie modeli językowych LRM do przeszukiwania Internetu pod kątem konkretnego zagrożenia, interpretacja zagrożeń na podstawie danych historycznych

ZARZĄDZANIE INCYDENTEM

Możliwość kontrolowania procesu obsługi incydentów – pomoc w określeniu dalszych kroków na podstawie zebranych informacji

KONTEKST

Efektywne zasilanie modelu językowego kontekstem – interfejs podpowiedzi w pełni zintegrowany z systemem

secureVISIO

AUTOMATYZACJA

REGUŁY I PARSERY

Parsery, reguły – wszystko czego potrzebujesz to przekierowanie logów, system automatycznie zastosuje niezbędne parsery i reguły bezpieczeństwa

MODYFIKACJA REGUŁ

Scalanie, wykluczenia – automatyczne dostrajanie reguł w oparciu o uczenie maszynowe

SECOPS

System jest w stanie automatycznie klasyfikować zdarzenia jako fałszywie pozytywne lub incydenty, a następnie blokować uruchamianie złośliwego oprogramowania lub izolować hosta

secureVISIO

AUTOMATYZACJA

PRZESZUKIWANIE LOGÓW

Automatyzacja przeszukiwania logów (przeszukiwanie logów oparte na sztucznej inteligencji i kontekście), tj. przeszukiwanie logów wtedy, gdy ma to sens, na podstawie informacji uzyskanych automatycznie przez playbook

KONTROLA

Automatyzacja w pełni kontrolowana przez sztuczną inteligencję – możesz zapytać sztuczną inteligencję, na co zwrócić uwagę.

KONTEKST

Automatyzacja zarządzania kontekstem (reguły, które uczą się o organizacji samodzielnie (autodiscovery) i playbookii, które zmieniają wyniki uczenia się na podstawie kontekstu)

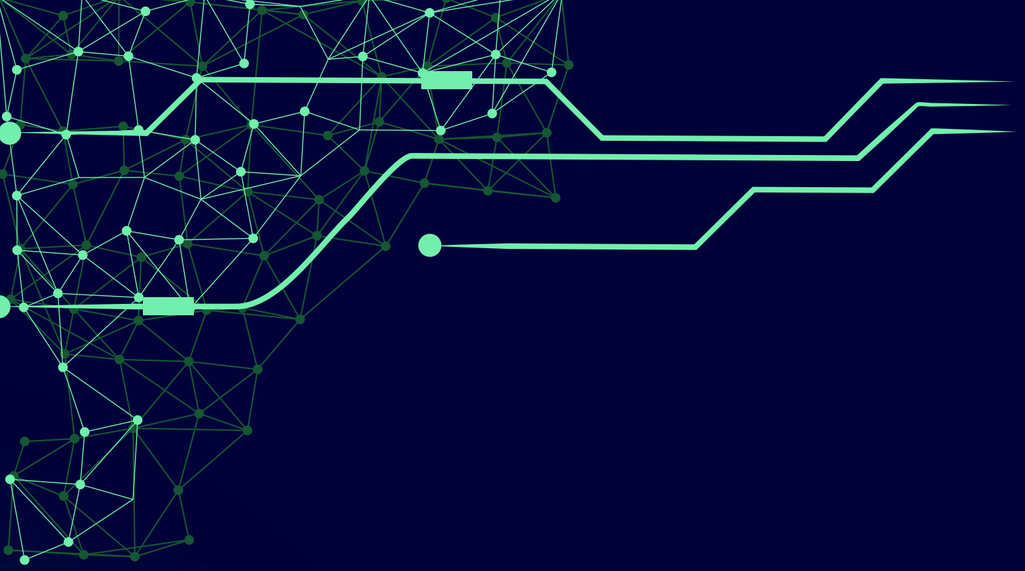
WNIOSKI

Prezentowanie podsumowań z wykorzystaniem kontekstu i sztucznej inteligencji, podsumowanie wszystkich zebranych informacji z właściwą interpretacją, poszukiwanie analogii w różnych zdarzeniach, korelacja

secureVISIO

Dziękuję za uwagę!

secureVISIO



secureVISIO