

**AI-lytics**

—

# **portal do analizy danych oparty o GenAI**

Mikołaj Gałkowski

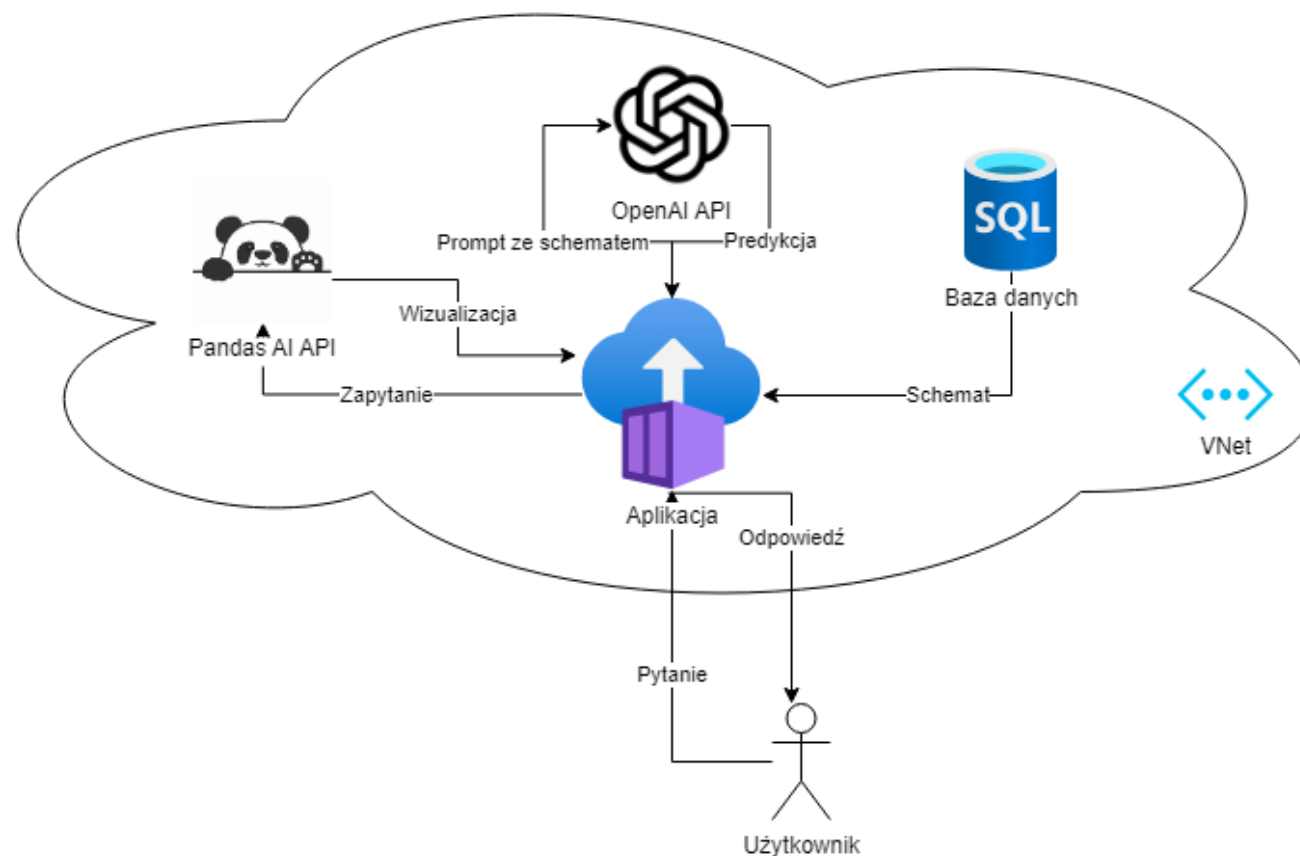
Wiktor Jakubowski

Łukasz Tomaszewski

# Opis projektu

- Projekt obejmuje rozwiązanie napisane w języku Python, oparte o Generatywną Sztuczną Inteligencję, która automatyzuje proces ekspolaracji i analizy danych.
- Narzędzie udostępnia aplikację webową, która pozwala na interakcję z ChatBot'em, który odpowiada na zapytania użytkownika w oparciu o wiedzę pozyskiwaną z bazy danych SQL.

# Diagram rozwiązania



# Infrastruktura

- Azure Container Instances wykorzystane do wdrożenia aplikacji dla użytkowników z możliwością konwersacji (użyty Streamlit)
- Azure OpenAI do połączenia się za pomocą API Key do usług GPT-3.5
- Baza danych SQL zawierająca dane
- Skonfigurowane Network Security Groups i podsieci VNet do komunikacji pomiędzy kontenerem aplikacji oraz bazą danych oraz filtracji ruchu (blokowania zapytań do API modeli i bazy danych z innych adresów IP niż aplikacji)

# Instrukcja obsługi

Cały proces jest krótki i opisano go w README w repozytorium\*:

1. Uzupełnij dane w plikach .yml o repozytorium kontenerów, regionie, a także zmienne środowiskowe
2. Wykonaj polecenia związane z budowaniem i wypchnięciem obrazu Docker do repozytorium kontenera, a potem zbudowaniem Azure Container Instances na podstawie tego kontenera
3. Aplikacja po chwili będzie widoczna pod domeną (u nas: <http://ailytics.francecentral.azurecontainer.io>)

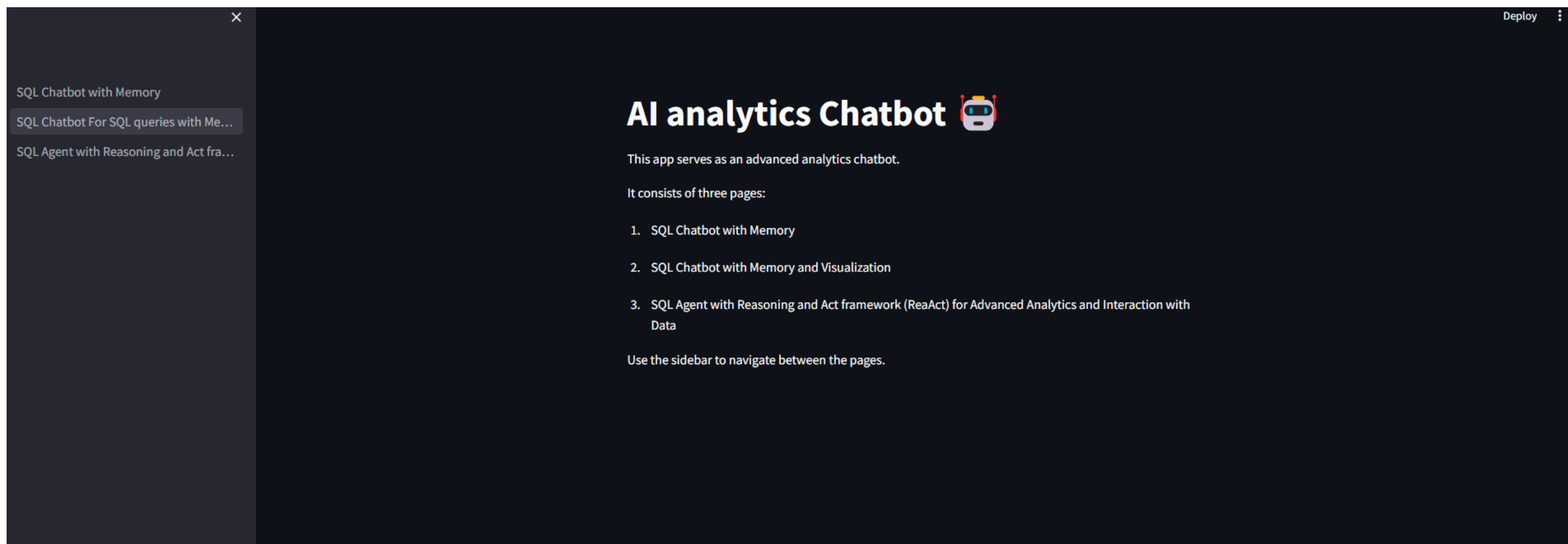
\*[https://github.com/WJakubowski/gen\\_ai\\_hackaton](https://github.com/WJakubowski/gen_ai_hackaton)

# **Wdrożone elementy**

# Funkcjonalności

- ✓ Narzędzie oparte o GenAI, odpowiadające na pytania dotyczące zawartości bazy danych za pośrednictwem przyjemnego interfejsu sieciowego
- ✓ Czat umożliwiający uzyskiwanie informacji w sposób konwersacyjny z zachowaniem poprzednich wiadomości (pamięć)
- ✓ Możliwość generowania zapytania SQL na zadane pytanie w języku naturalnym
- ✓ Wizualizacja zapytań użytkownika w formie przystępnych wykresów
- ✓ Wyświetlanie kosztu zapytania wykonanego przez użytkownika
- ✓ Rozwiązanie w pełni wdrożone na platformę Microsoft Azure
- ✓ Zidentyfikowane ryzyka w procesie analiz i mitygacja znacznej większości z nich (SQL-injection, dostęp do API z zewnątrz itp.) przy użyciu narzędzi GitGuardian oraz Microsoft Defender for Cloud

# Podgląd





# Potencjalne ulepszenia

# Miejsce na poprawę

- Zabezpieczenie strony poprzez certyfikat SSL (komponenty są na repozytorium, z braku czasu nie zostały postawione i przetestowane)
- Wprowadzenie indywidualnych kont wraz z logowaniem w aplikacji
- Zwiększenie weryfikacji poprawności zwracanych rozwiązań

**Dziękujemy za uwagę!**