**Pomysł: Wykrywanie oszustw w transakcjach bankowych**

**Plan:**

1.Zbieranie i integracja danych:

* Azure Event Hub – przyjmuje dane z aplikacji bankowych. To narzędzie pozwala na wygodną analizę w czasie rzeczywistym
* Azure Data Factory – budowa pipelinów ETL dla danych historycznych i intergacja danych i przygotowanie do dalszej analizy.

2. Przetwarzanie i przygotowanie danych:

* Azure Databricks - agregacja, czyszczenie, eksploracja i analiza danych, podział danych na sety treningowe i testowe. To narzędzie pozwala też użyć feature engineeringu i budowy modelu ML.

3.Modelowanie i AI:

* Azure Machine Learning – trening i rejestracja modeli ML do wykrywania anomalii i oszustw
* ML Ops z Azure DevOps – zarządzanie cyklem życia modelu: versioning, pipeline’y, testowanie i deployment modelu.

4. Detekcja i reakcja w czasie rzeczywistym:

* Azure Functions – implementacja automatycznych reakcji np. zablokowania transakcji lub wysłanie jakiegoś alertu do użytkownika lub do zespołu bezpieczeństwa banku

5. Monitoring i wizualizacja:

* Azure Monitor – pomaga w śledzeniu działania modelu, czasu odpowiedzi API i logów systemu wykrywania oszustw bankowych

6. Zarządzanie, bezpieczeństwo i compliance:

* Azure Key Vault – przechowywanie kluczy API
* Azure DevOps – kod analityczby, modele ML, infrastruktura jako kod