

KQL W THREAT HUNTINGU

BEATA ZALEWA

HACKUJDOBRO CZYNNIE

21.03.2025

0 mnie



Security Architect



Consultant



Microsoft Certified Trainer



AI & Cybersecurity Practitioner



Developer



Freelancer



Azure @ ❤️



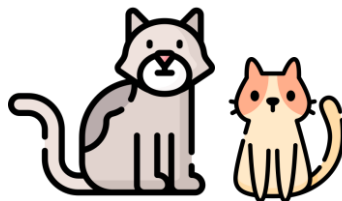
Google Cloud



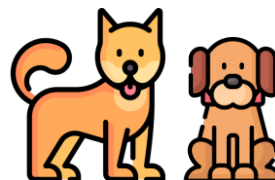
1 Mąż



1 Córka



2 Koty



2 Psy



Kryminały

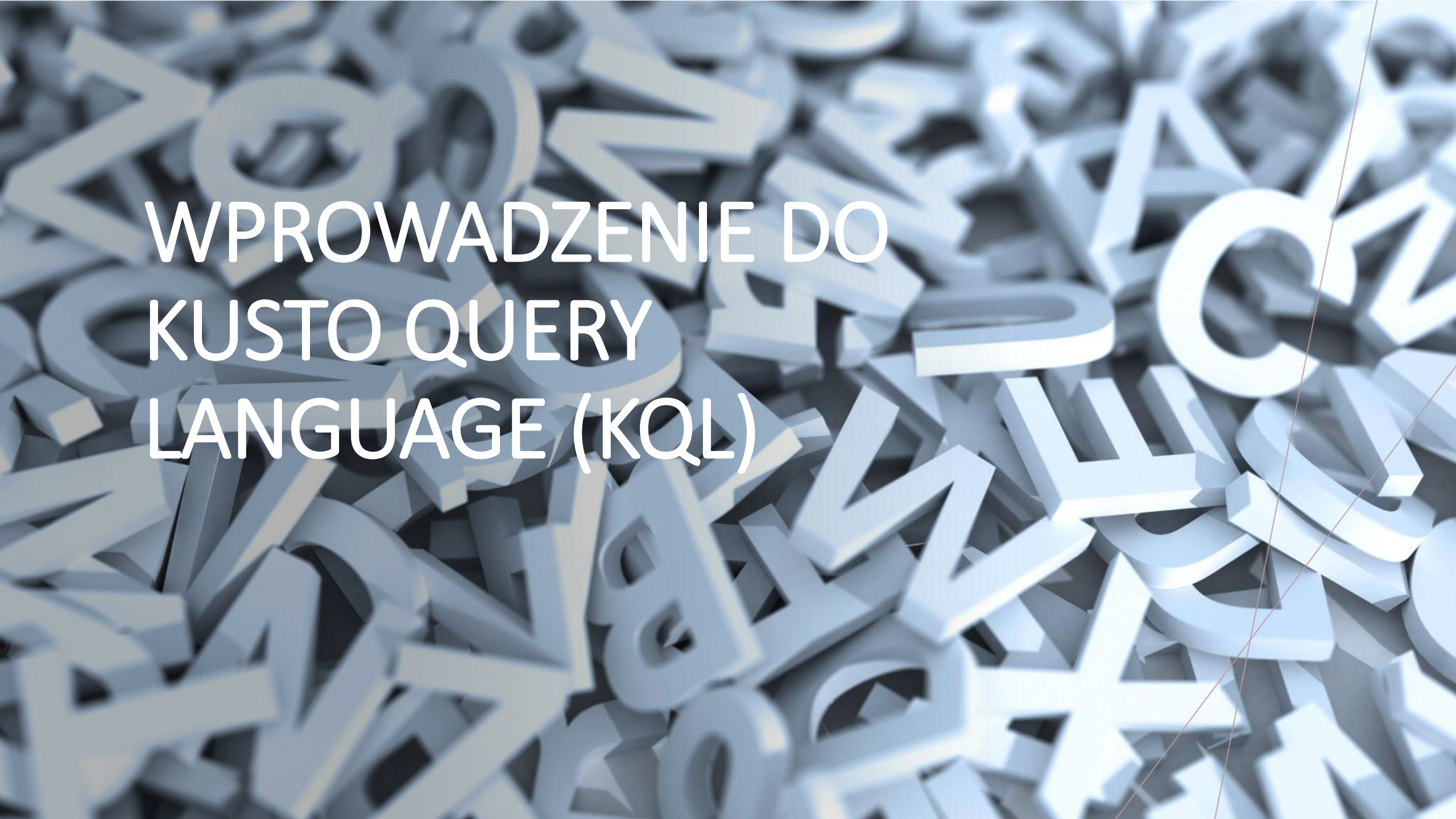


Fotografia

AGENDA



- Wprowadzenie do Kusto Query Language (KQL)
- Podstawowe składniki i polecenia KQL
- I cała reszta ...



WPROWADZENIE DO KUSTO QUERY LANGUAGE (KQL)



CZYM JEST KQL?

Język zapytań KQL

Kusto Query Language (KQL) został stworzony przez Microsoft i służy do analizy danych na platformach takich jak Azure Data Explorer.

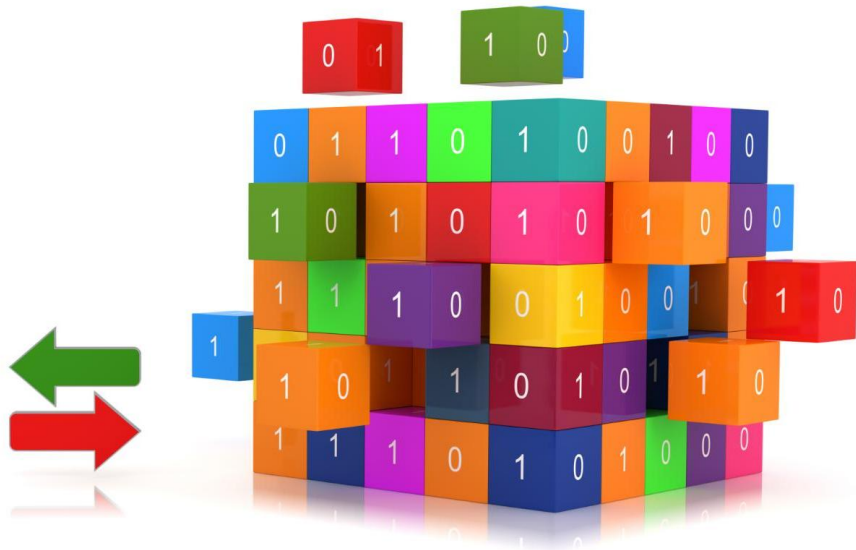
Intuicyjne formułowanie zapytań

KQL pozwala użytkownikom formułować zapytania w sposób zrozumiały i intuicyjny, co ułatwia analizę danych.

Analiza dużych zbiorów danych

KQL jest idealny do wydobywania informacji z dużych zbiorów danych, co czyni go potężnym narzędziem dla analityków.

PODSTAWOWE SKŁADNIKI JĘZYKA



Zapytania KQL

Zapytania KQL są podstawowym elementem umożliwiającym interakcję z danymi i ich analizę. Umożliwiają one precyzyjne określenie danych, które chcemy uzyskać.

Operatory KQL

Operatory KQL są używane do wykonywania różnych operacji na danych, takich jak filtrowanie, sortowanie i porównywanie wartości. Kluczowe dla efektywnej analizy danych.

Funkcje KQL

Funkcje KQL pozwalają na przetwarzanie i manipulację danymi w bardziej złożony sposób. Umożliwiają użytkownikom wykonywanie zaawansowanych obliczeń.

Składnia KQL

Składnia KQL definiuje sposób, w jaki zapytania są pisane i interpretowane. Zrozumienie składni jest kluczowe dla tworzenia poprawnych zapytań.

ZASTOSOWANIA KQL W ANALIZIE DANYCH

Analiza logów

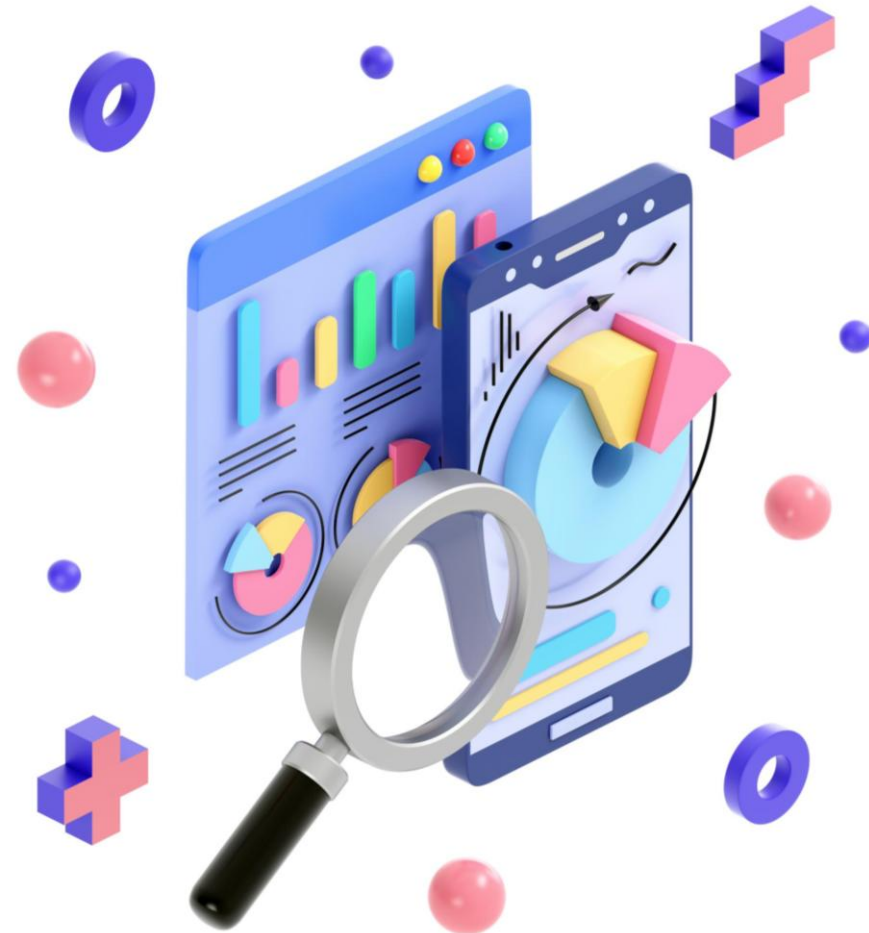
KQL jest skutecznym narzędziem do analizy logów, umożliwiając szybkie przetwarzanie i analizę dużych zbiorów danych.

Monitorowanie wydajności systemów

KQL wspomaga monitorowanie wydajności systemów, pozwalając na bieżące śledzenie i analizowanie kluczowych wskaźników wydajności.

Eksploracja danych

Dzięki elastyczności KQL, użytkownicy mogą skutecznie eksplorować dane, odkrywając ukryte wzorce i informacje w czasie rzeczywistym.



PRZYKŁAD 1: ANALIZA LOGÓW SERWERA



Analiza logów serwera

Zastosujemy KQL do analizy logów serwera, aby zidentyfikować istotne błędy oraz trendy w ruchu.

Identyfikacja błędów

Używając KQL, zidentyfikujemy błędy w logach serwera, co pozwoli na szybsze ich rozwiązywanie.

Trendy w ruchu

Analizując logi, zidentyfikujemy trendy w ruchu, co pomoże w optymalizacji wydajności serwera.

PRZYKŁAD 2: MONITOROWANIE WYDAJNOŚCI APLIKACJI



Monitorowanie wydajności aplikacji

Monitorowanie wydajności aplikacji jest kluczowe dla zapewnienia ich optymalnego działania i minimalizowania problemów.

Analiza danych o wydajności

Analizowanie danych o wydajności pozwala na identyfikację słabych punktów oraz potencjalnych obszarów do optymalizacji.

Identyfikacja problemów

Identyfikacja problemów wydajnościowych jest niezbędna do zapewnienia stabilności i efektywności aplikacji.

PRZYKŁAD 3: WYSZUKIWANIE ANOMALII W DANYCH



Wykrywanie anomalii

Techniki wykrywania anomalii pomagają identyfikować nieprawidłowości w danych, co może prowadzić do szybkiej reakcji na problemy.

Techniki KQL

KQL oferuje różnorodne techniki do analizy danych i wykrywania anomalii, co jest niezbędne w analizie danych.

Reakcja na nieprawidłowości

Identyfikacja anomalii w danych pozwala na szybszą reakcję i rozwiązywanie problemów, co poprawia jakość analizy danych.

WNIOSKI

Potęga KQL

KQL to bardzo potężne narzędzie do analizy danych, które umożliwia użytkownikom wydobywanie cennych informacji z dużych zbiorów danych.

Wsparcie dla decyzji

Rozumienie składni KQL jest kluczowe dla efektywnego wykorzystywania jego możliwości analitycznych w praktyce.

Najlepsze praktyki

Zastosowanie najlepszych praktyk w KQL zwiększa efektywność analiz danych, pozwalając na szybsze i dokładniejsze wyniki.

Stale poszukuję nowych możliwości i ekscytujących wyzwań. Jeśli chcesz się ze mną skontaktować, proszę, skorzystaj z poniższych kanałów:



Email: beata@zalnet.pl

LinkedIn: <https://www.linkedin.com/in/beatazalewa/>

Blog: <https://zalnet.pl/blog/>

X: <https://x.com/beatazalewa>

GitHub: <https://github.com/beatazalewa/Conferences/>

