

# EFEKTYWNE WYKORZYSTANIE KUSTO QUERY LANGUAGE (KQL) W ANALIZIE DANYCH

BEATA ZALEWA

ISSA POLSKA LUBLIN

22.01.2025

# O mnie



Security  
Architect



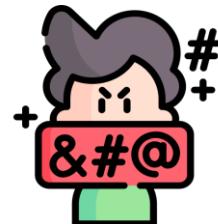
Konsultant



Microsoft Certified  
Trainer



AI & Cybersecurity  
Practitioner



Deweloper



Freelancer



Azure @ ❤️



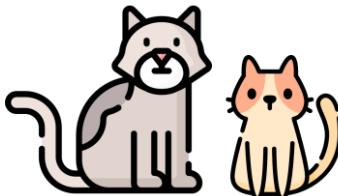
Google Cloud



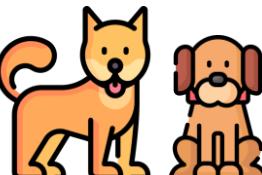
1 Mąż



1 Córka



2 Koty



2 Psy

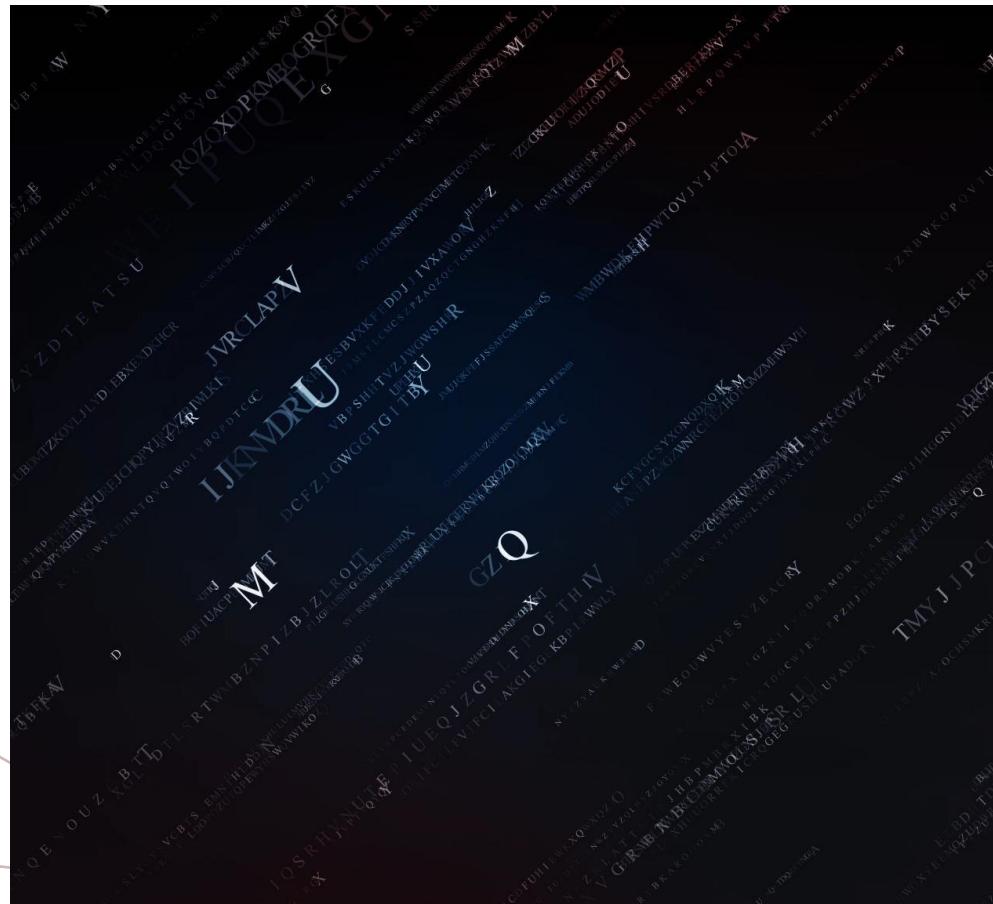


Kryminały



Fotografia

# AGENDA



- Wprowadzenie do Kusto Query Language (KQL)
- Podstawowe składniki i polecenia KQL
- Zaawansowane techniki w KQL
- Praktyczne zastosowania KQL w analizie danych
- Najlepsze praktyki i optymalizacja zapytań KQL

# 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.

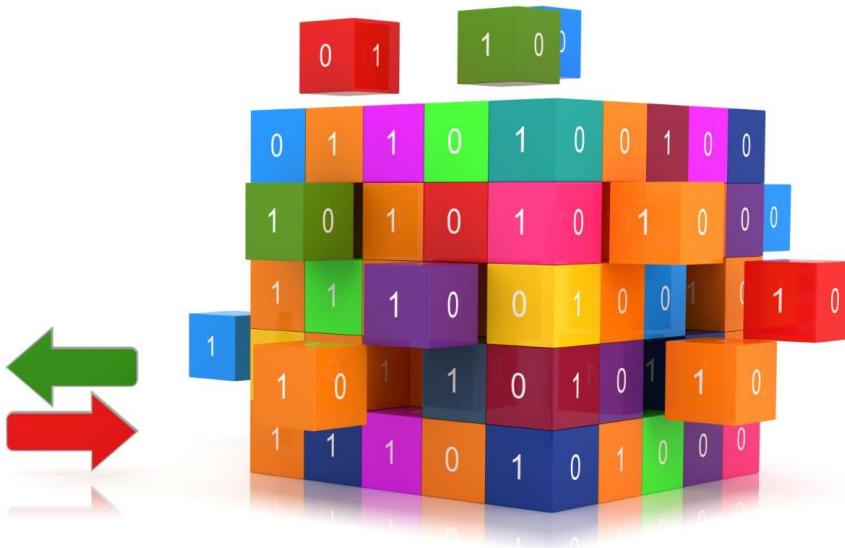
## Intuicyjne formułowanie zapytań

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

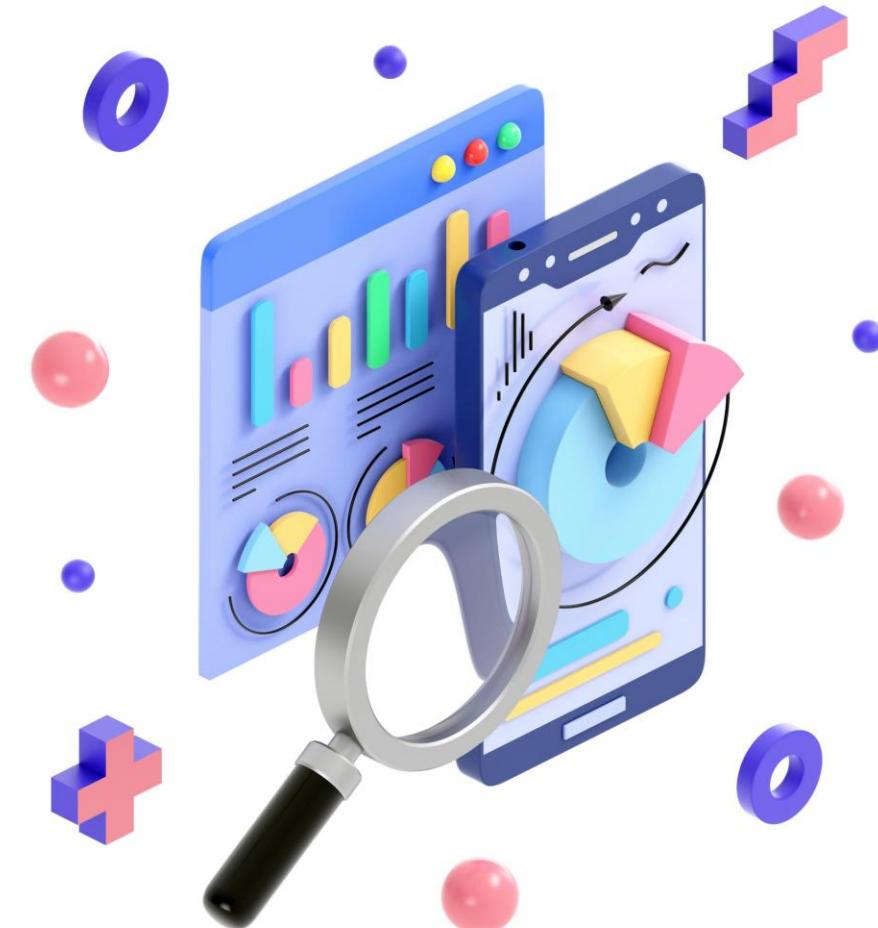
KQL jest skutecznym narzędziem do analizy logów, umożliwiając szybkie przetwarzanie i analizę dużych zbiorów danych.

## 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.



# PODSTAWOWE ZASTOSOWANIA KQL W DANYCH

## Analiza logów

KQL jest szeroko stosowane do analizy logów, co pozwala na identyfikowanie problemów i optymalizację systemów.

## Monitorowanie wydajności aplikacji

Umożliwia monitorowanie wydajności aplikacji, co pozwala na szybsze wykrywanie problemów i poprawę doświadczeń użytkowników.

## Wykrywanie anomalii

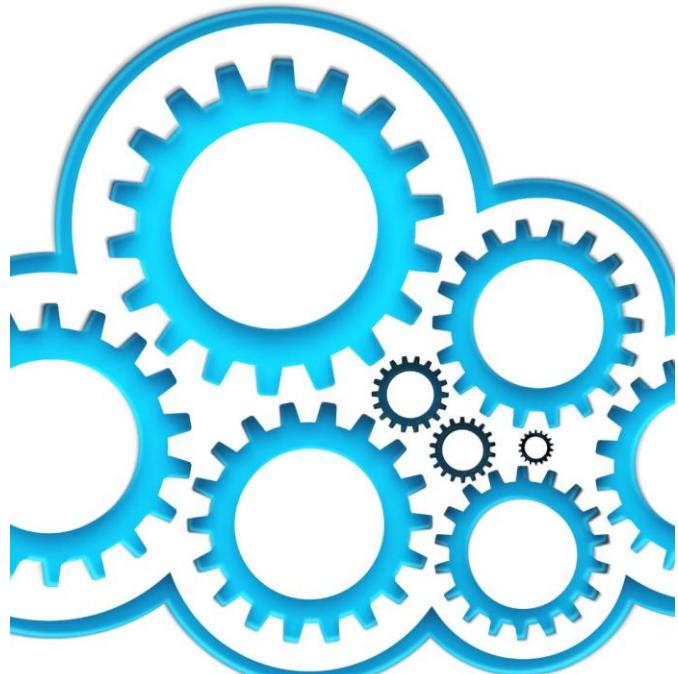
KQL pomaga w wykrywaniu anomalii w danych, co jest kluczowe dla zapewnienia bezpieczeństwa i prawidłowego działania systemów.

## Tworzenie raportów wizualnych

KQL umożliwia tworzenie wizualnych raportów, które pomagają w szybkim zrozumieniu danych i wyciąganiu wniosków.



# HISTORIA I ROZWÓJ KQL



## Tworzenie KQL

KQL został stworzony przez Microsoft dla analizy danych w czasie rzeczywistym, co zrewolucjonizowało sposób przetwarzania danych.

## Część Azure Data Explorer

KQL rozpoczął swoją historię jako część Azure Data Explorer, co umożliwiło łatwą integrację z chmurą.

## Popularność i elastyczność

KQL szybko zyskał popularność dzięki prostocie oraz elastyczności w pracy z dużymi zbiorami danych, co ułatwia użytkownikom analizę.

# **PODSTAWOWE SKŁADNIKI I POLECENIA KQL**



# PODSTAWOWE ZAPYTANIA SELECT

## Wydobywanie danych

Zapytania SELECT w KQL pozwalają na wydobywanie danych z określonych tabel, umożliwiając efektywną analizę.

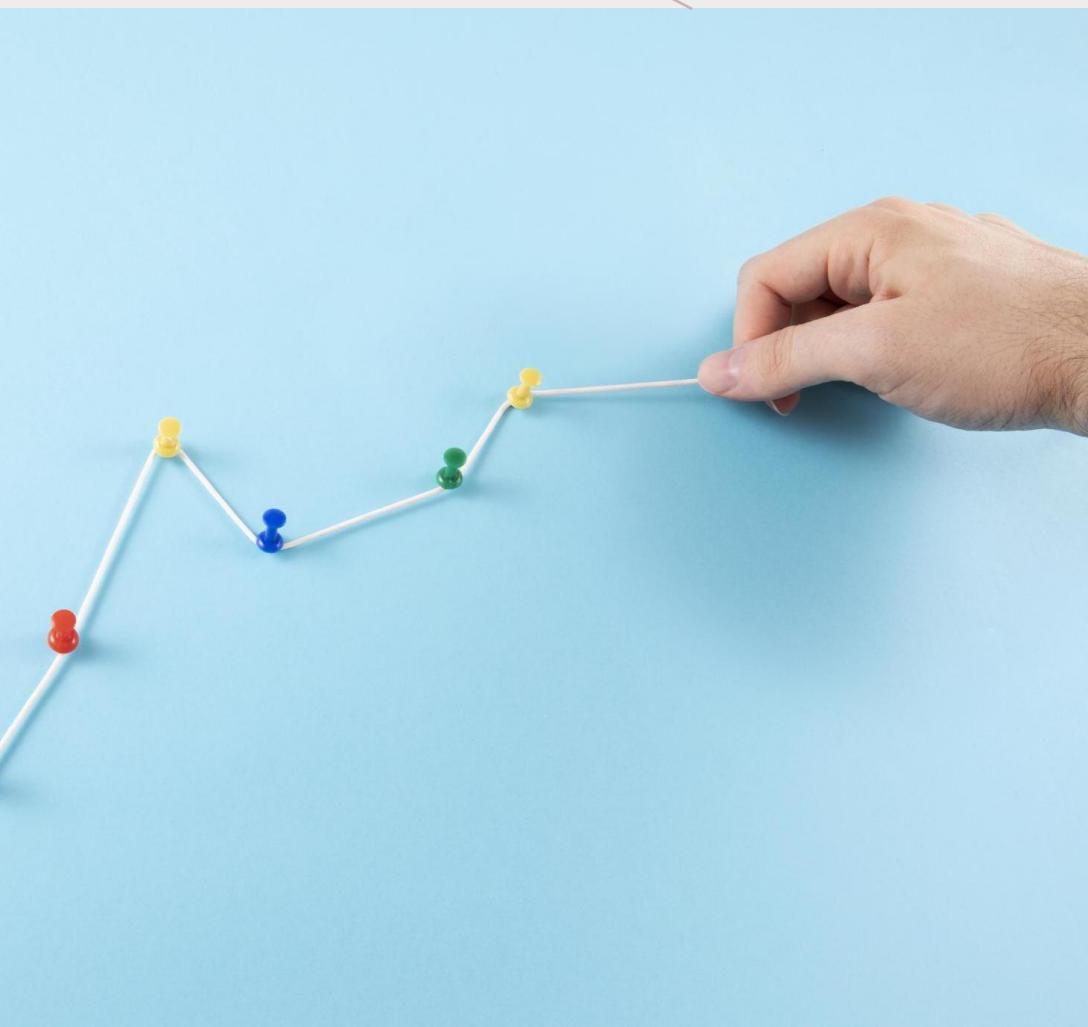
## Selekcja kolumn

Użytkownicy mogą precyzyjnie określić kolumny, które chcą wyświetlić w wynikach, co umożliwia lepszą analizę danych.

## Filtrowanie wyników

Możliwość filtrowania wyników pozwala użytkownikom na skupienie się na istotnych danych, co zwiększa efektywność analizy.

# FILTROWANIE I SORTOWANIE DANYCH



## Rekordy spełniające kryteria

Filtracja danych pozwala na wydobycie tylko tych rekordów, które spełniają zdefiniowane kryteria, co zwiększa efektywność analizy.

## Operatory porównawcze

Użytkownicy mogą używać różnych operatorów porównawczych, aby precyzyjnie określić warunki filtracji danych.

## Złożone wyniki

Korzystanie z funkcji i operatorów pozwala na uzyskanie bardziej złożonych wyników w analizie danych, co umożliwia lepsze zrozumienie danych.

# AGREGACJE I GRUPOWANIE DANYCH

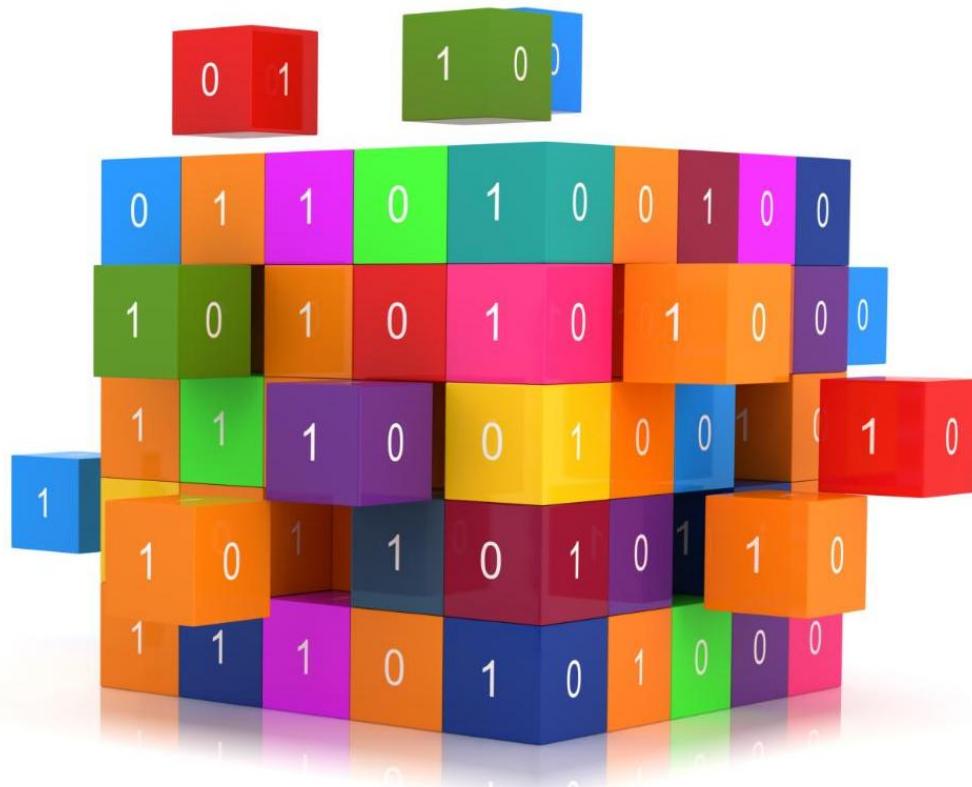
## Podsumowanie danych

Agregacje w KQL umożliwiają efektywne podsumowanie danych, takie jak liczenie, sumowanie oraz obliczanie średniej wartości.

## Analiza grup danych

Grupowanie danych pozwala na analizę zbiorów danych według określonych kategorii, co ułatwia wyciąganie wniosków.

# STRUKTURA ZAPYTAŃ W KQL



## Podstawowe polecenia KQL

Polecenia KQL definiują, jakie dane będą przetwarzane, co jest kluczowe dla efektywnego tworzenia zapytań.

## Operatory w KQL

Operatory w KQL umożliwiają manipulację danymi i ich przekształcanie, co jest niezbędne do analizy informacji.

## Funkcje KQL

Funkcje KQL pozwalają na bardziej zaawansowane przetwarzanie danych, umożliwiając osiągnięcie bardziej szczegółowych wyników.

# NAJCZĘŚCIEJ UŻYWANE OPERATORY



## Operator 'where'

Operator 'where' pozwala na filtrowanie danych według określonych kryteriów, co ułatwia analizę i selekcję interesujących informacji.

## Operator 'project'

Operator 'project' umożliwia wybieranie konkretnych kolumn danych do analizy, co pomaga w skupieniu się na istotnych informacjach.

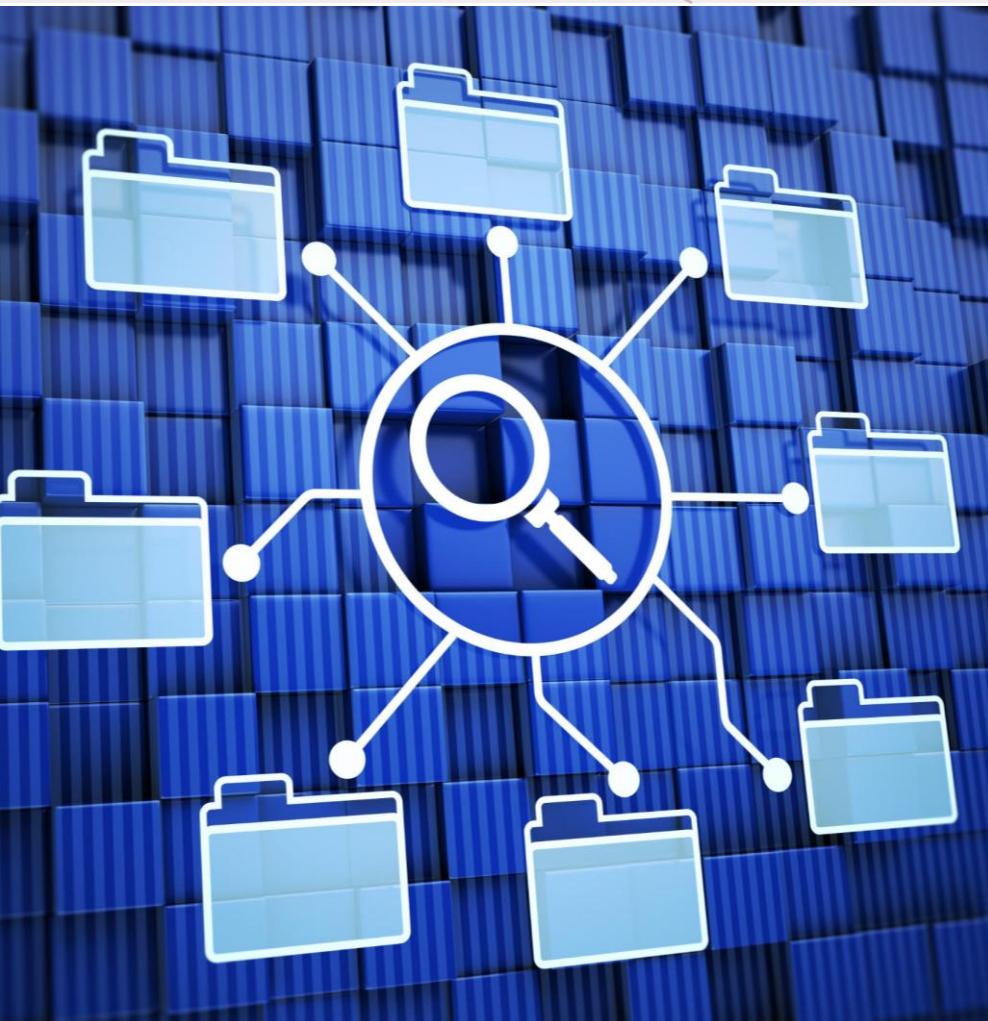
## Operator 'summarize'

Operator 'summarize' pozwala na grupowanie danych i obliczanie agregatów, takich jak suma czy średnia, co jest istotne w analizie statystycznej.

## Operator 'join'

Operator 'join' łączy dane z różnych źródeł, co umożliwia tworzenie bardziej złożonych zapytań i analiz w KQL.

# FILTRACJA I SELEKCJA DANYCH



## Kluczowe operacje KQL

Filtracja i selekcja danych są fundamentalnymi operacjami w KQL, umożliwiającymi efektywne przetwarzanie danych.

## Operator 'where'

Operator 'where' pozwala na precyzyjne definiowanie warunków, co umożliwia wyodrębnienie konkretnych informacji z dużych zbiorów danych.

# ZAAWANSOWANE TECHNIKI W KQL

# TWORZENIE ZŁOŻONYCH ZAPYTAŃ



## Operatory logiczne

Operatorzy logiczni pozwalają na łączenie różnych warunków w zapytaniach, co zwiększa precyzję wyników.

## Wiele operacji i funkcji

Złożone zapytania mogą wykorzystywać wiele operacji i funkcji, co umożliwia bardziej złożoną analizę danych.

# ŁĄCZENIE TABEL I ZAPYTAŃ PODZAPYTANIA



## Łączenie tabel

Łączenie tabel w KQL pozwala na integrację danych z różnych źródeł, co umożliwia bardziej złożoną analizę.

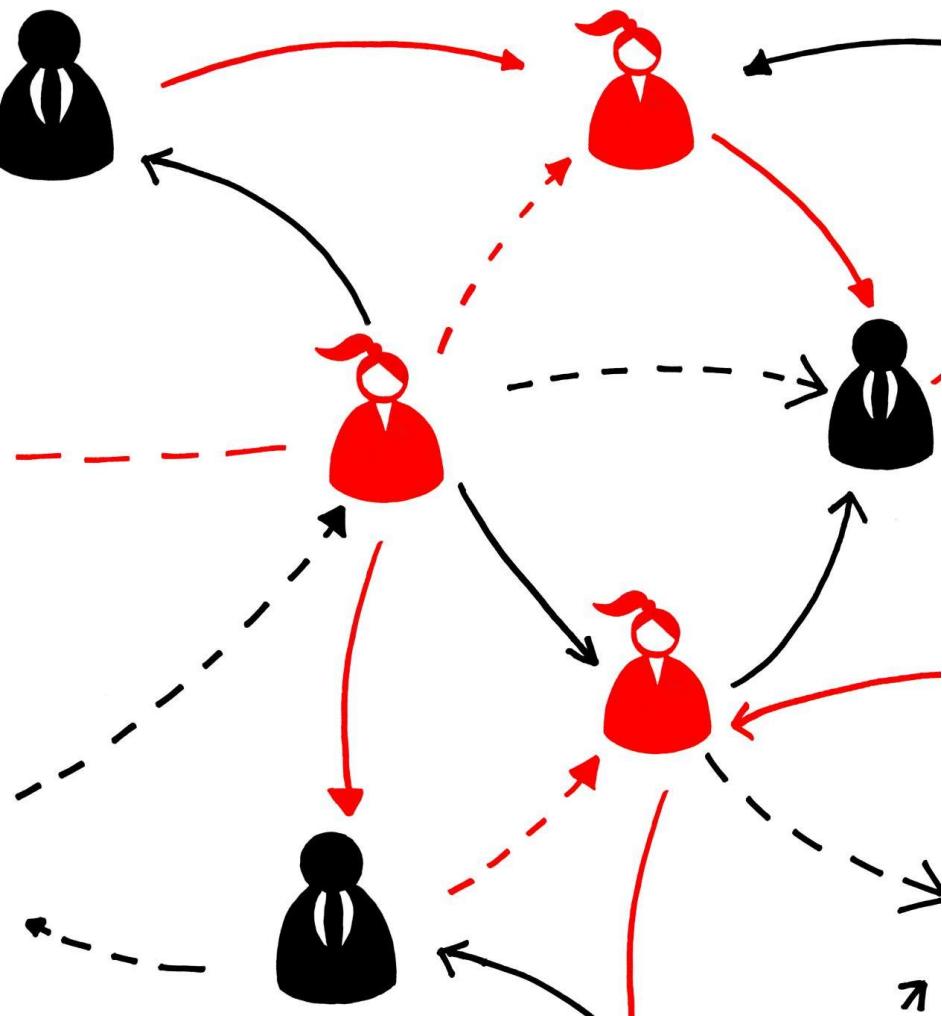
## Zapytywania podzapytania

Korzystanie z zapytań podzapytania w KQL umożliwia tworzenie bardziej zaawansowanych zapytań oraz lepszą interpretację danych.

## Analiza danych

Znajomość technik łączenia tabel oraz zapytań podzapytania pozwala na bardziej zaawansowaną analizę danych w różnych kontekstach.

# ŁĄCZENIE DANYCH Z RÓŻNYCH TABEL



## Zrozumienie operatorów join

Operatorzy join w KQL umożliwiają łączenie danych z różnych tabel, co pozwala na bardziej złożoną analizę.

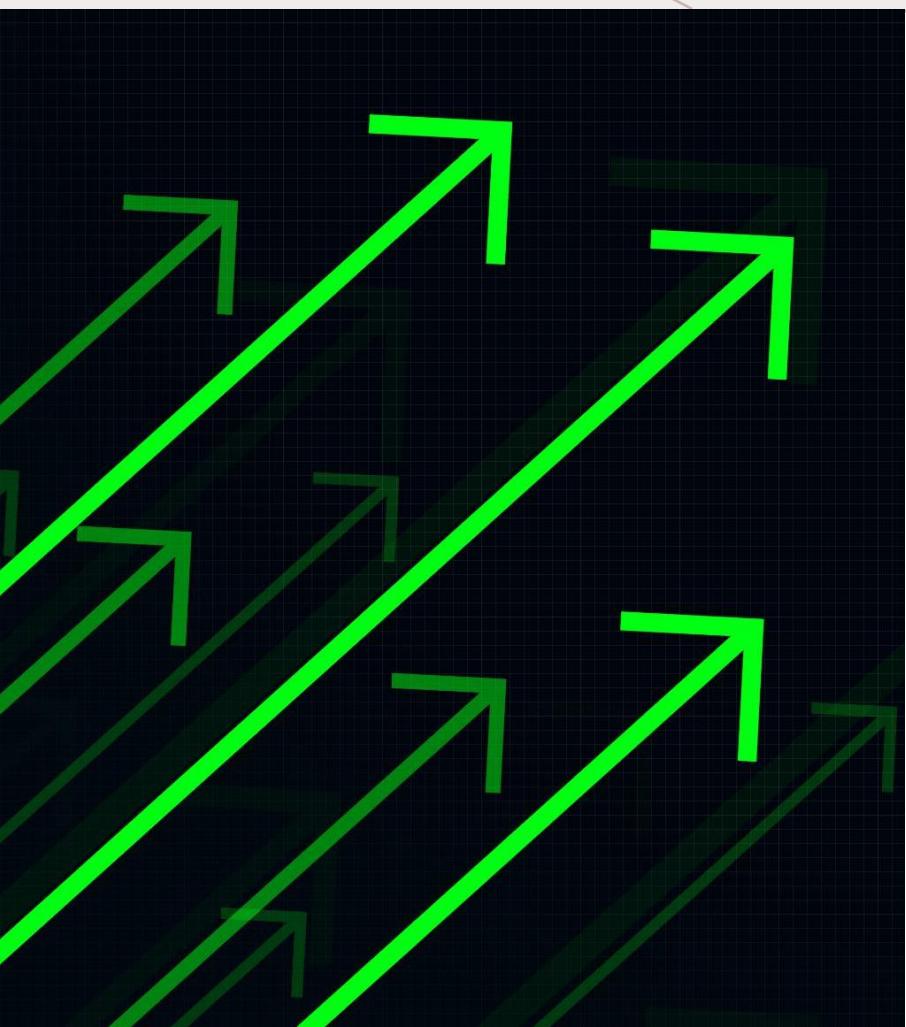
## Tworzenie złożonych analiz

Użytkownicy mogą tworzyć złożone analizy, łącząc różnorodne źródła danych, co zwiększa wartość informacyjną analiz.

## Szeroki kontekst danych

Łączenie danych z różnych tabel pozwala na uzyskanie szerszego kontekstu, co prowadzi do lepszych wniosków.

# AGREGACJA DANYCH I FUNKCJE AGREGUJĄCE



## Zbiorcze przetwarzanie danych

Agregacja danych w KQL umożliwia efektywne zbiorcze przetwarzanie dużych zbiorów danych, co przyspiesza analizę.

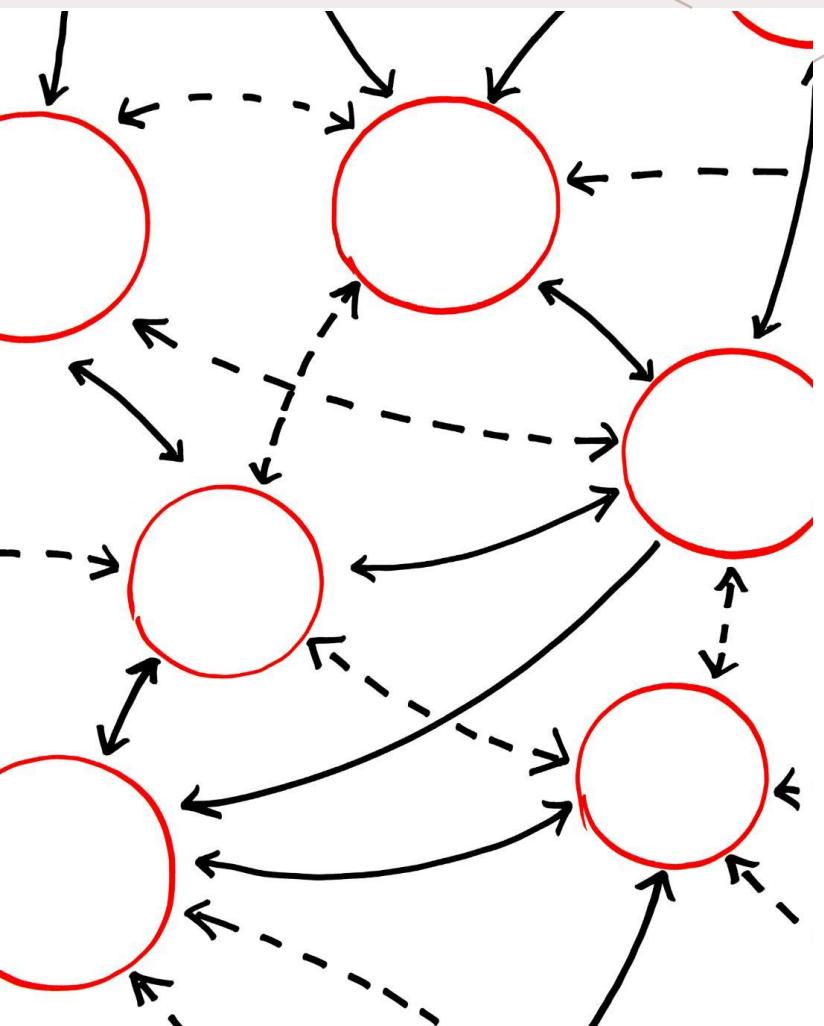
## Funkcje agregujące

Funkcje takie jak 'count', 'sum' i 'avg' są kluczowe w analizie danych, umożliwiając uzyskiwanie użytecznych podsumowań.

## Szybka analiza

Agregacja pozwala na szybkie uzyskiwanie analiz i podsumowań, co jest nieocenione w procesie podejmowania decyzji.

# GRUPOWANIE I SORTOWANIE DANYCH



## Technika grupowania danych

Grupowanie danych za pomocą operatora 'summarize' umożliwia organizację danych w logiczne zbiory, co ułatwia ich analizę.

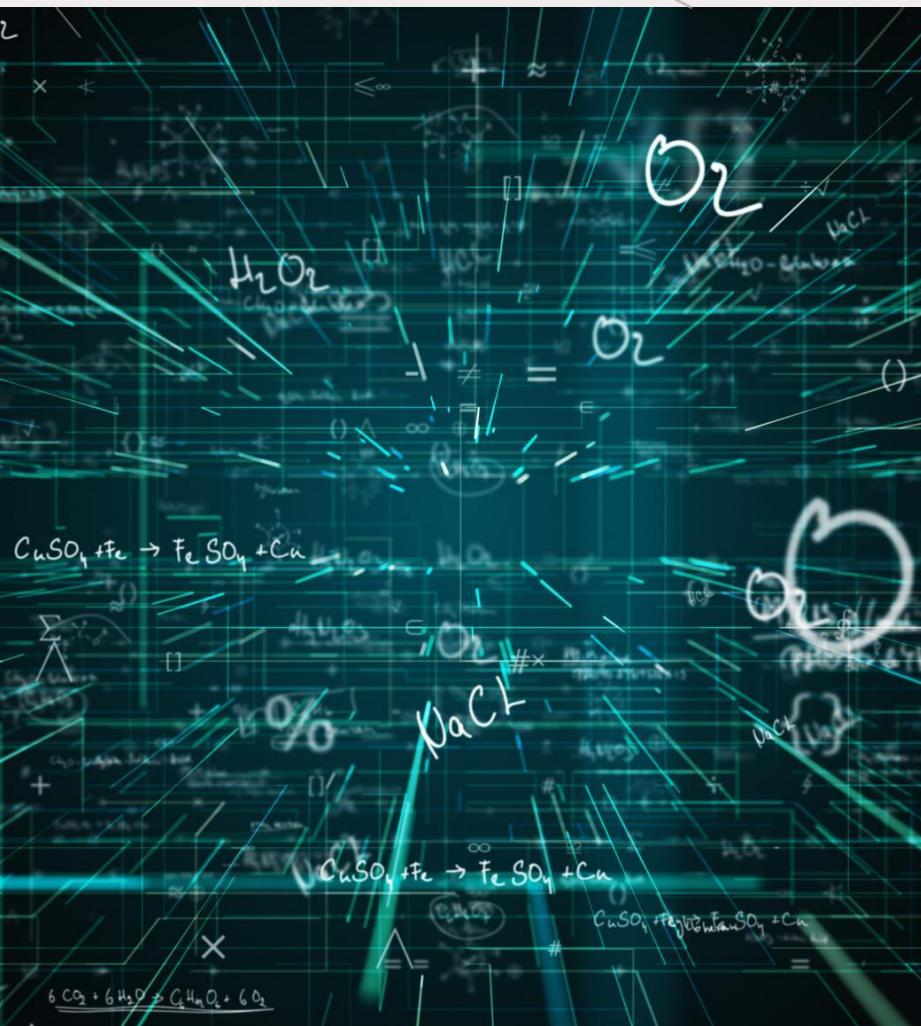
## Sortowanie danych

Sortowanie danych za pomocą 'order by' pozwala uporządkować dane według określonych kryteriów, co ułatwia ich interpretację.

## Zrozumienie wzorców

Grupowanie i sortowanie pomagają w identyfikacji wzorców i relacji w danych, co jest kluczowe dla ich analizy.

# UŻYWANIE FUNKCJI I OPERATORÓW



## Manipulacja tekstem

KQL umożliwia manipulację tekstem poprzez różne funkcje, co pozwala na łatwe przetwarzanie danych tekstowych.

## Operacje matematyczne

Dzięki wbudowanym funkcjom matematycznym użytkownicy mogą wykonywać różne obliczenia i analizy numeryczne na danych.

## Funkcje agregujące

Funkcje agregujące w KQL pozwalają na zbieranie i analizowanie danych, co zwiększa ich użyteczność w analizach.

# PRAKTYCZNE ZASTOSOWANIA KQL W ANALIZIE DANYCH

# MONITOROWANIE WYDAJNOŚCI SYSTEMÓW

## Zastosowanie KQL

KQL jest kluczowym narzędziem w monitorowaniu wydajności systemów, umożliwiającym analizę danych w czasie rzeczywistym.

## Analiza logów

Analiza logów pozwala na szybkie wykrywanie awarii oraz oceny wydajności systemów, co wspiera szybsze podejmowanie decyzji.

## Optymalizacja działania

Identyfikacja problemów poprzez analizę metryk prowadzi do optymalizacji wydajności systemów informatycznych.





# ANALIZA LOGÓW I ZDARZEŃ

## Kluczowe zastosowanie KQL

Analiza logów i zdarzeń jest fundamentalnym zastosowaniem KQL, które wspiera działania związane z bezpieczeństwem informatycznym.

## Wydobywanie istotnych informacji

Umożliwia wydobycie istotnych informacji z logów systemowych, co jest kluczowe dla wykrywania anomalii.

## Wykrywanie anomalii

Analiza zdarzeń pozwala na efektywne wykrywanie anomalii, co zwiększa bezpieczeństwo systemów informatycznych.

# PRZEWIDYWANIE TRENDÓW I ZACHOWAŃ

## Analiza danych

KQL umożliwia analizę danych w celu przewidywania trendów, co usprawnia proces podejmowania decyzji.

## Identyfikacja wzorców

Użytkownicy mogą identyfikować wzorce w danych, co pozwala na lepsze prognozowanie przyszłych zachowań.

## Prognozowanie przyszłych zdarzeń

Dzięki funkcjom analitycznym KQL, użytkownicy mogą prognozować przyszłe zdarzenia na podstawie dostępnych danych.



# TWORZENIE WIZUALIZACJI DANYCH

## Łatwe tworzenie wizualizacji

KQL umożliwia użytkownikom szybkie i proste generowanie wizualizacji danych, co ułatwia analizę wyników.

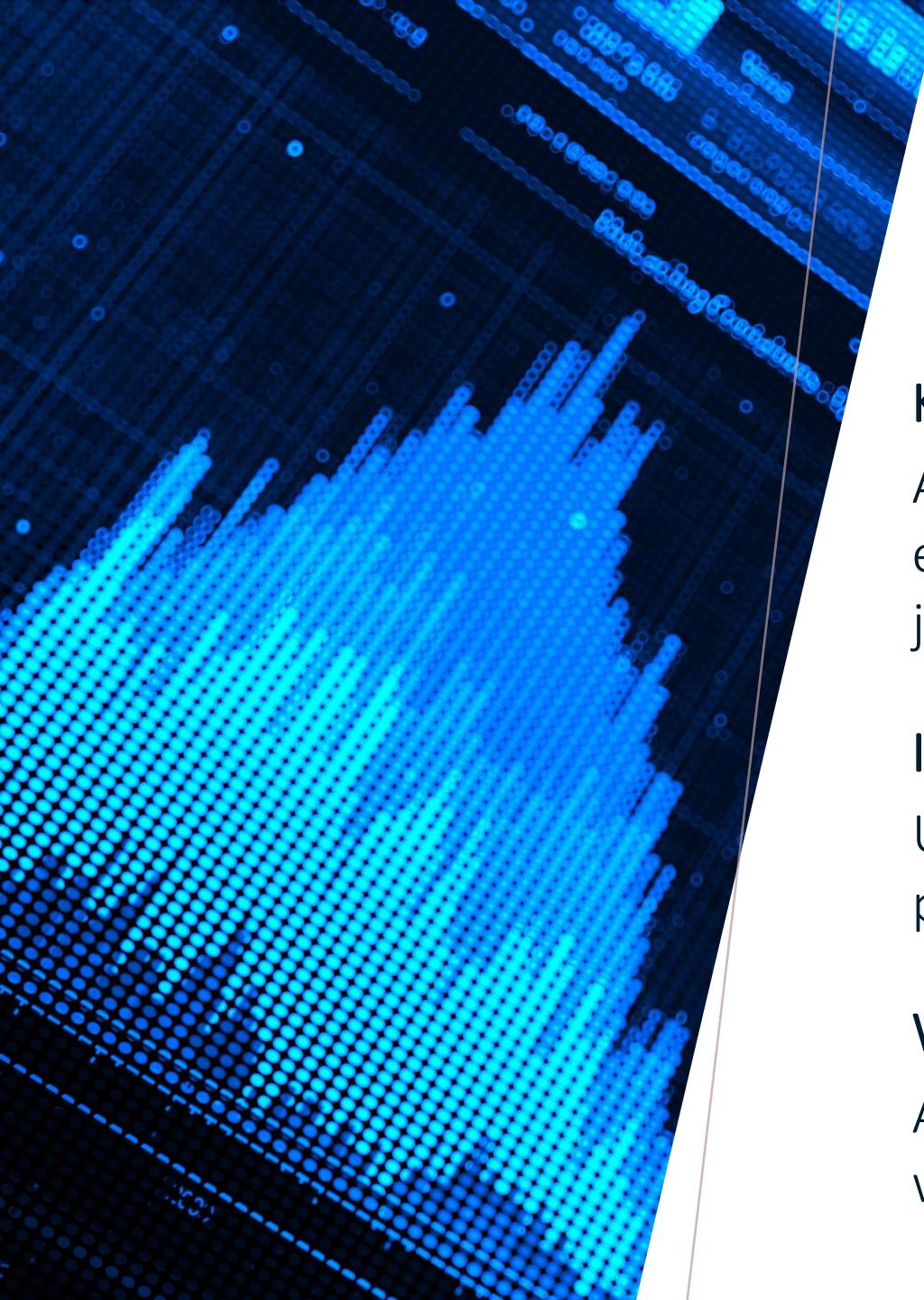
## Rodzaje wizualizacji

Użytkownicy mogą wybierać spośród różnych typów wizualizacji, takich jak wykresy liniowe, słupkowe i mapy, dostosowując je do swoich potrzeb.

## Interpretacja wyników

Wizualizacje pomagają w lepszej interpretacji danych oraz w zrozumieniu wyników zapytań i analiz.





# ANALIZA TRENDÓW I WZORCÓW

## Kluczowy aspekt analizy danych

Analiza trendów i wzorców jest niezbędna do efektywnego przetwarzania danych w systemach takich jak KQL.

## Identyfikacja zmian w danych

Użytkownicy mogą zidentyfikować zmiany w danych na przestrzeni czasu, co jest kluczowe dla efektywnej analizy.

## Wykrywanie ukrytych wzorców

Analiza trendów pozwala użytkownikom wykrywać ukryte wzorce, co może wspierać lepsze podejmowanie decyzji.

# MONITOROWANIE I ALERTOWANIE

## Monitorowanie danych

KQL pozwala na skuteczne monitorowanie danych, umożliwiając użytkownikom szybkie identyfikowanie istotnych zmian.

## Ustawianie alertów

Użytkownicy mogą ustawiać alerty na podstawie określonych kryteriów, co zwiększa efektywność zarządzania danymi i bezpieczeństwem.

## Reagowanie na zmiany

Dzięki KQL użytkownicy mogą reagować na zmiany w danych w odpowiednim czasie, co pozwala na szybsze podejmowanie decyzji.



# **NAJLEPSZE PRAKTYKI I OPTYMALIZACJA ZAPYTAŃ KQL**

# OPTYMALIZACJA WYDAJNOŚCI ZAPYTAŃ

## Kluczowe praktyki optymalizacji

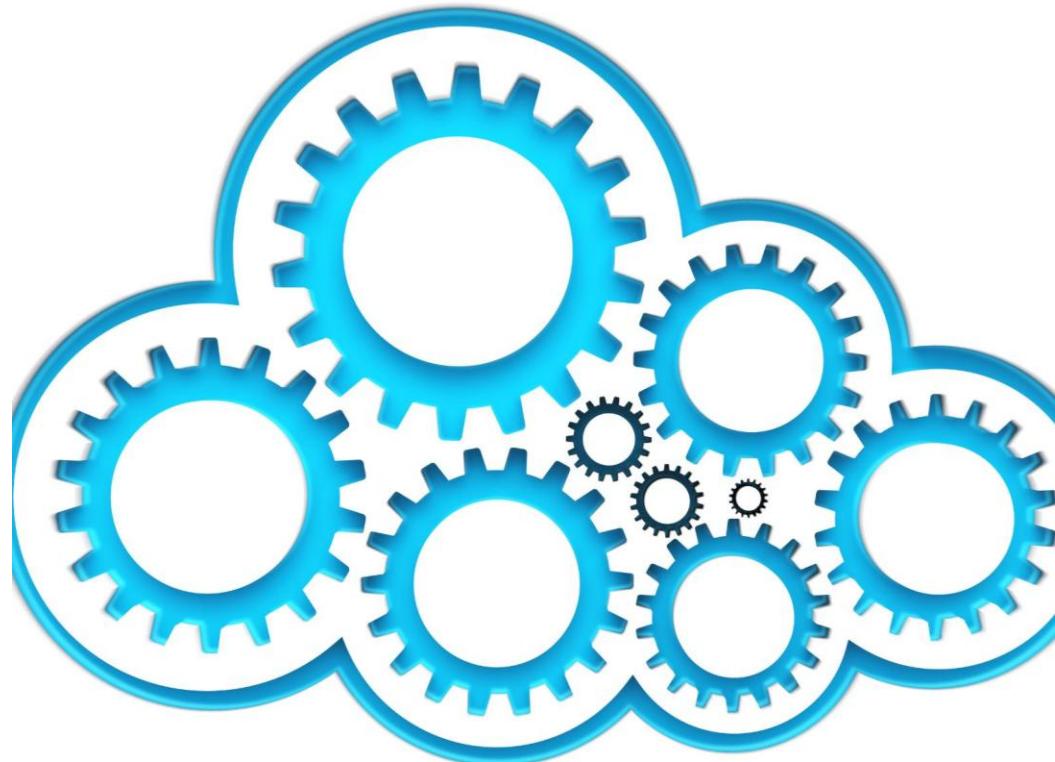
Stosowanie najlepszych praktyk jest niezbędne do zwiększenia wydajności zapytań i analizy danych.

## Unikanie zbędnych operacji

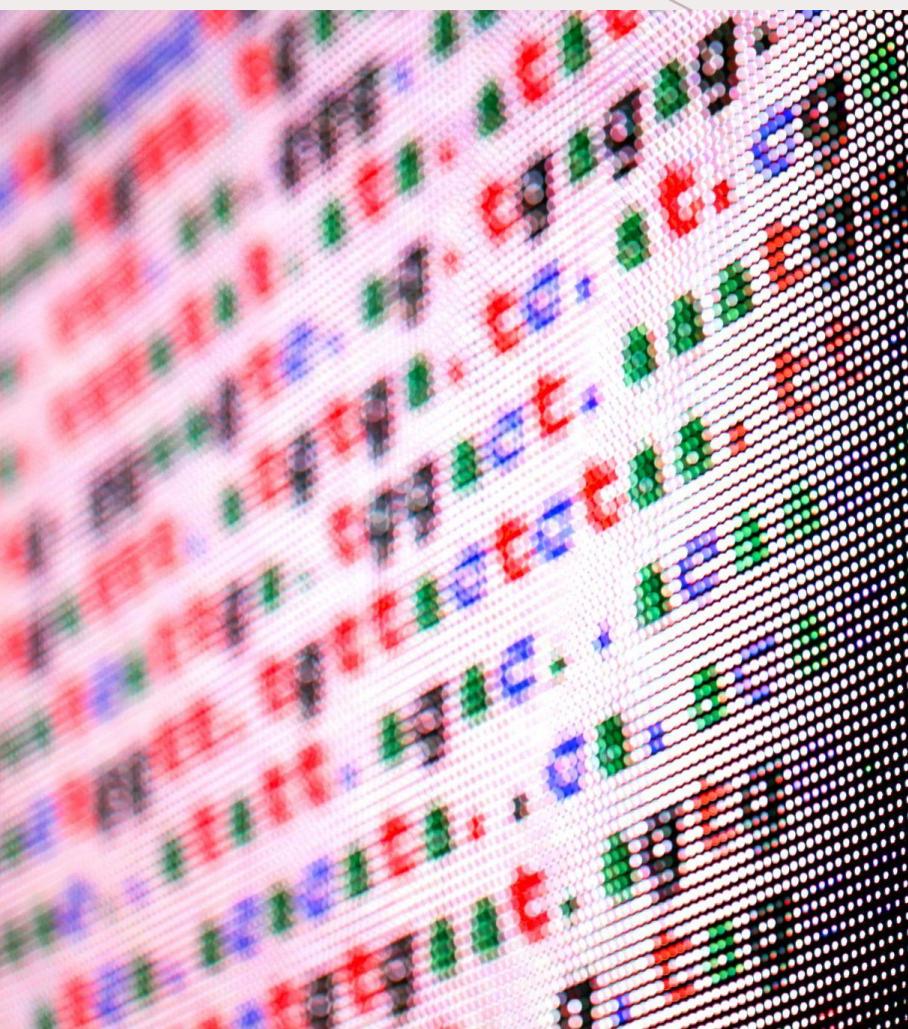
Unikanie niepotrzebnych operacji przyspiesza działanie zapytań i zmniejsza obciążenie systemu.

## Indeksowanie danych

Zastosowanie odpowiednich indeksów jest kluczowe dla zwiększenia szybkości wyszukiwania i przetwarzania danych.



# DEBUGOWANIE I TESTOWANIE ZAPYTAŃ



## Znaczenie debugowania

Debugowanie zapytań KQL jest kluczowe dla poprawnego analizowania danych, co pozwala na skuteczniejsze podejmowanie decyzji.

## Narzędzia do testowania

Użytkownicy powinni znać narzędzia, które pomagają w identyfikowaniu błędów w zapytaniach i ich optymalizacji.

## Optymalizacja zapytań

Optymalizacja zapytań pozwala na zwiększenie ich wydajności, co jest istotne dla efektywnej analizy danych.

# PRAKTYCZNE WSKAZÓWKI I PORADY

## Zrozumienie KQL

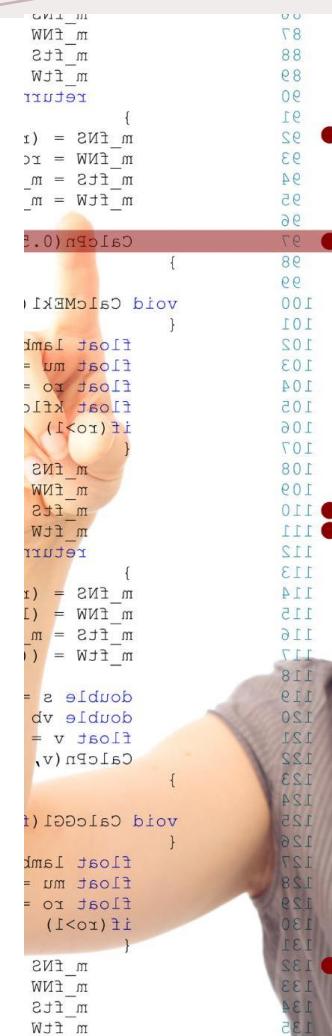
Kluczowe jest zrozumienie składni KQL, aby skutecznie analizować dane i uzyskiwać precyzyjne wyniki.

## Optymalizacja zapytań

Optymalizacja zapytań w KQL pomaga w zwiększeniu wydajności i skróceniu czasu odpowiedzi, co jest kluczowe dla skutecznej pracy z danymi.

## Wizualizacja wyników

Dobre wizualizacje wyników analizy danych są istotne dla łatwego zrozumienia i interpretacji wyników.



# OPTYMALIZACJA WYDAJNOŚCI ZAPYTAŃ



## Techniki optymalizacji

Wykorzystanie technik optymalizacji, takich jak ograniczanie zakresu danych, jest kluczowe w poprawie wydajności zapytań.

## Operatorzy w KQL

Zastosowanie odpowiednich operatorów w zapytaniach KQL może znacząco wpływać na czas odpowiedzi oraz efektywność pracy z danymi.

# BEZPIECZEŃSTWO I ZARZĄDZANIE DOSTĘPEM



## Kluczowe zasady bezpieczeństwa

Zasady bezpieczeństwa danych są niezbędne do ochrony wrażliwych informacji przed nieautoryzowanym dostępem.

## Mechanizmy zarządzania dostępem

KQL oferuje różne mechanizmy zarządzania dostępem, które pomagają w kontrolowaniu, kto ma dostęp do danych.

## Ochrona wrażliwych informacji

Ochrona wrażliwych informacji wymaga ścisłego przestrzegania zasad dostępu przez wszystkich użytkowników.

# NAJCZĘŚCIEJ POPEŁNIAНЕ BŁĘDY I JAK ICH UNIKAĆ

## Błędy w składni KQL

Nieprawidłowa składnia KQL może prowadzić do błędnych wyników. Ważne jest, aby zrozumieć zasady poprawnej składni.

## Zrozumienie danych

Nieznajomość struktury danych może prowadzić do błędnych wniosków. Zrozumienie kontekstu danych jest kluczowe.

## Testowanie zapytań

Niezapewnienie testowania zapytań KQL może prowadzić do nieefektywnych wyników. Testowanie jest ważnym krokiem w procesie analizy.



# 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 rozwiązanie 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](mailto: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/>

