From Zero to Kusto Hero

A unified analytics solution for the era of AI

Brian Bønk

Senior Principal, Microsoft MVP

Intellishore

https://aka.bi/follow

https://kql.how

https://dcode.bi

https://aka.bi/slides

Microsoft MVP Most Valuable Professional

Microsoft

FastTrack Recognized
Solution Architect
Power BI
2022 >>

Microsoft

Certified Trainer
Data Platform

2018 >>

The history of Kusto

Azure Sentinel

Log Analytics

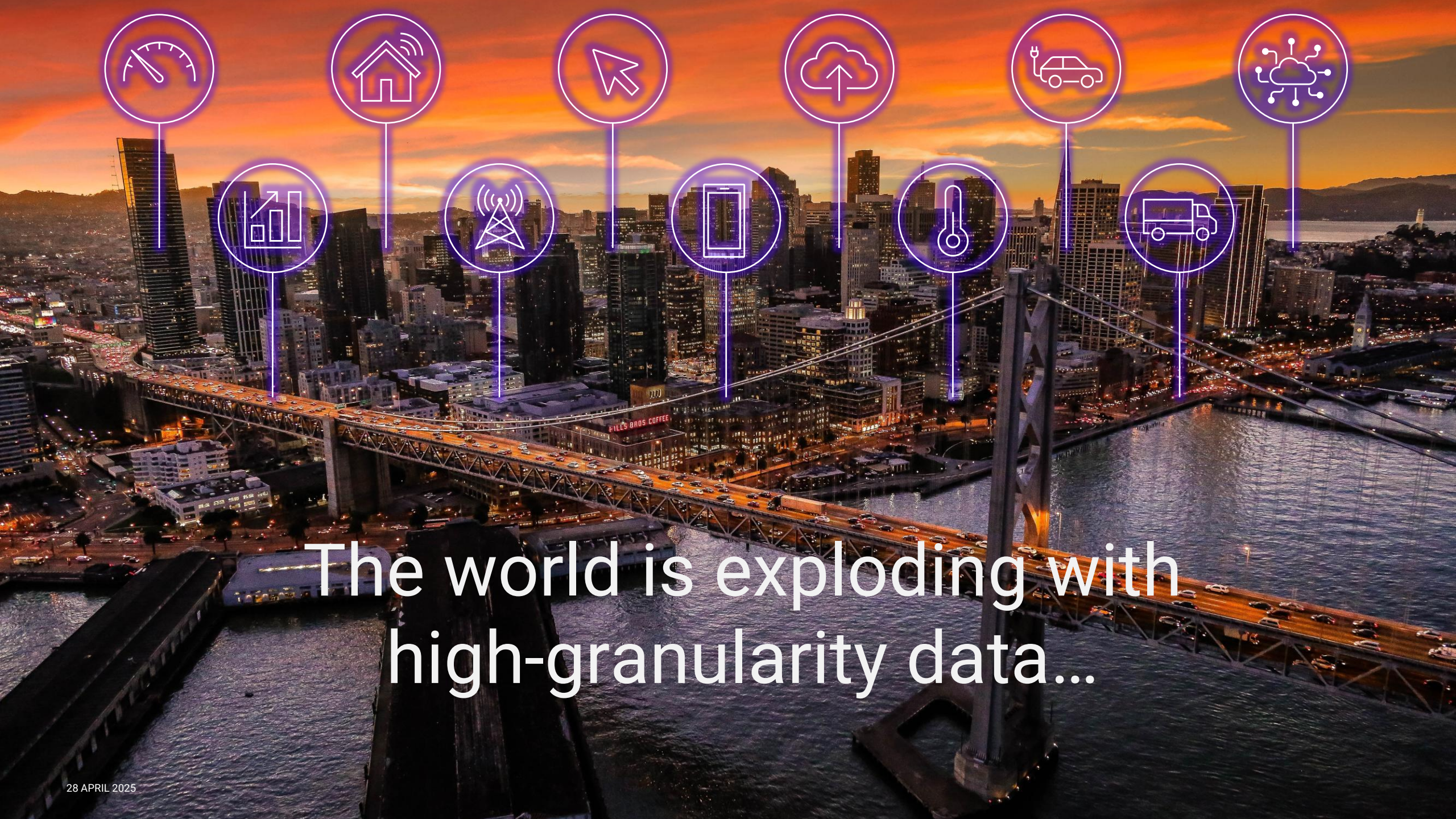
Real-Time Analytics

Azure resource graph

Microsoft 365 Defender

CMPivot

CMPivot

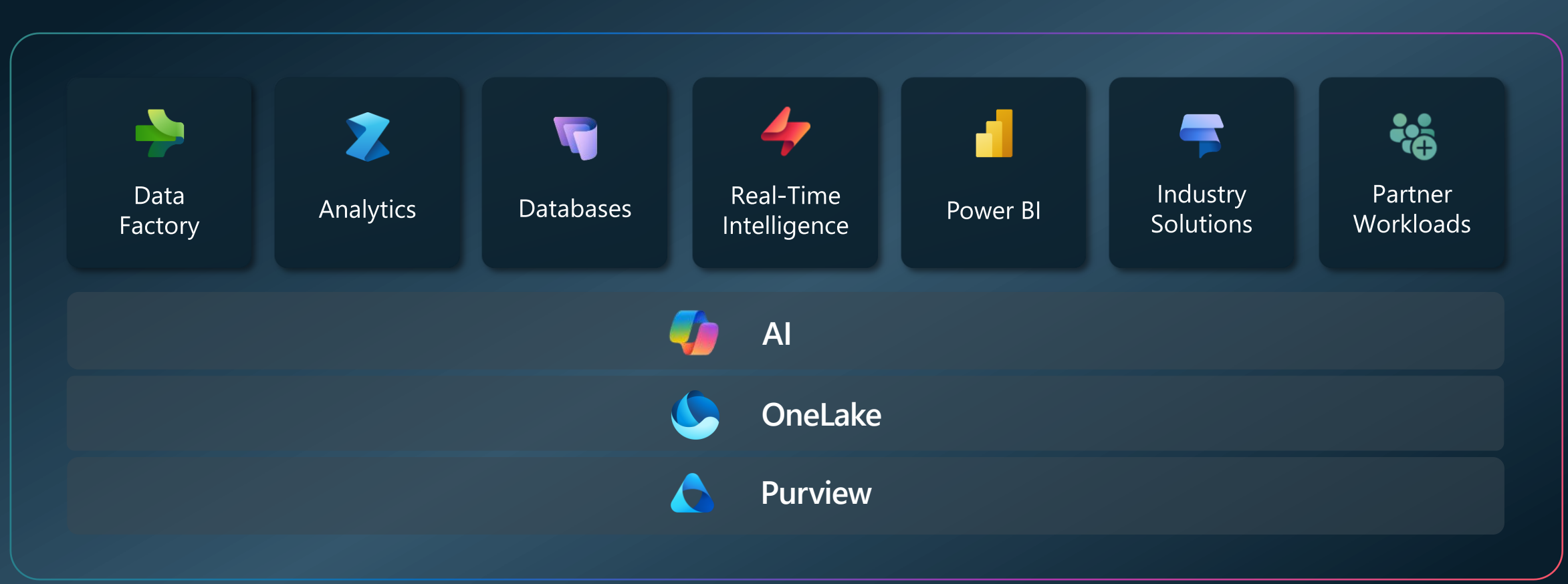


The world is exploding with high-granularity data...

Digital transformation

Cybersecurity
Asset tracking and management
Predictive maintenance
Supply chain optimization
Customer experience
Energy management
Inventory management
Quality control
Environmental monitoring
Fleet management
Health and safety

Microsoft Fabric

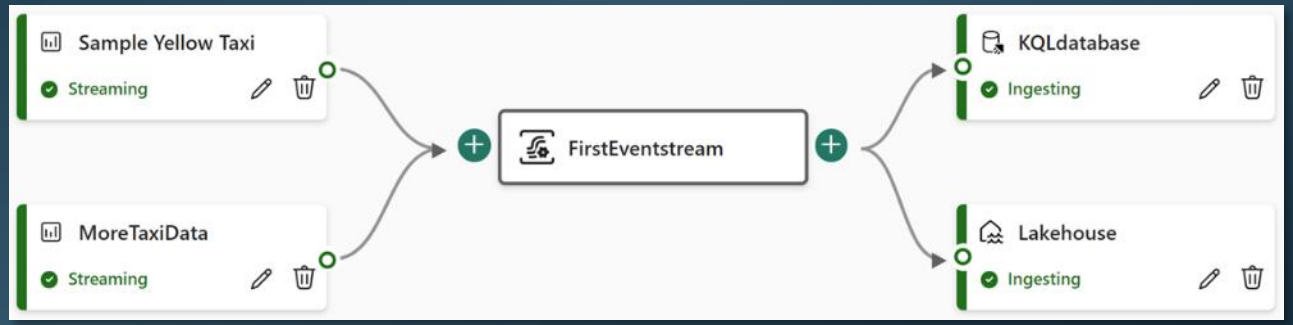



Event Ingestion
Real-Time Analytics
Real-Time AI
Real-Time Dashboards
Real-Time Rules
Event-Driven Actions
Data Factory
Data Engineering
Data Warehouse
Data Science
Real-Time intelligence
Power BI
SQL
Real-Time hub
OneLake
AI

Streaming data with ease

EVENTSTREAM

The event stream service, leverages the ability to get data from several sources of streaming data and save it to a wide variety of destinations, including OneLake, KQL databases and Azure services.



The service computes the data once and can pipe it out to several destinations at once. All configured and maintained from within the Microsoft Fabric portal and “coded” with your mouse.

Imagine scenarios of IoT devices loading data to both the data warehouse and other 3-rd party destinations – this can now be done using the low-code approach from Event Stream.

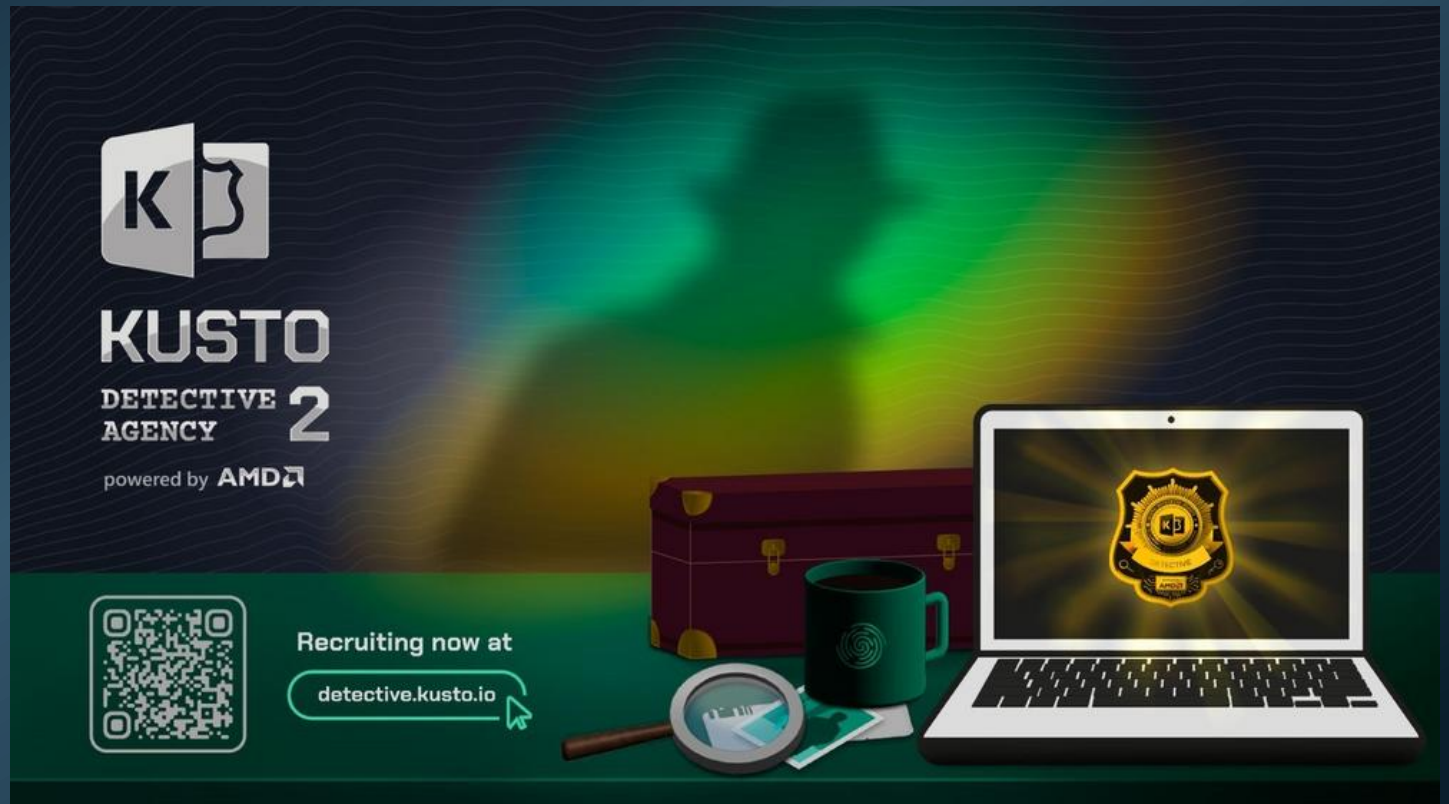
KQL database
Key capabilities

Unlimited Scale (query, ingestion and storage)	Any data source	Any data format
Structured Semi-structured Free-text	Real-time transformation og complicated data strcutures	Streaming analytics in Near-Real-Time
High performance Low latency High freshness	Timeseries database	Everything is indexed and partitioned

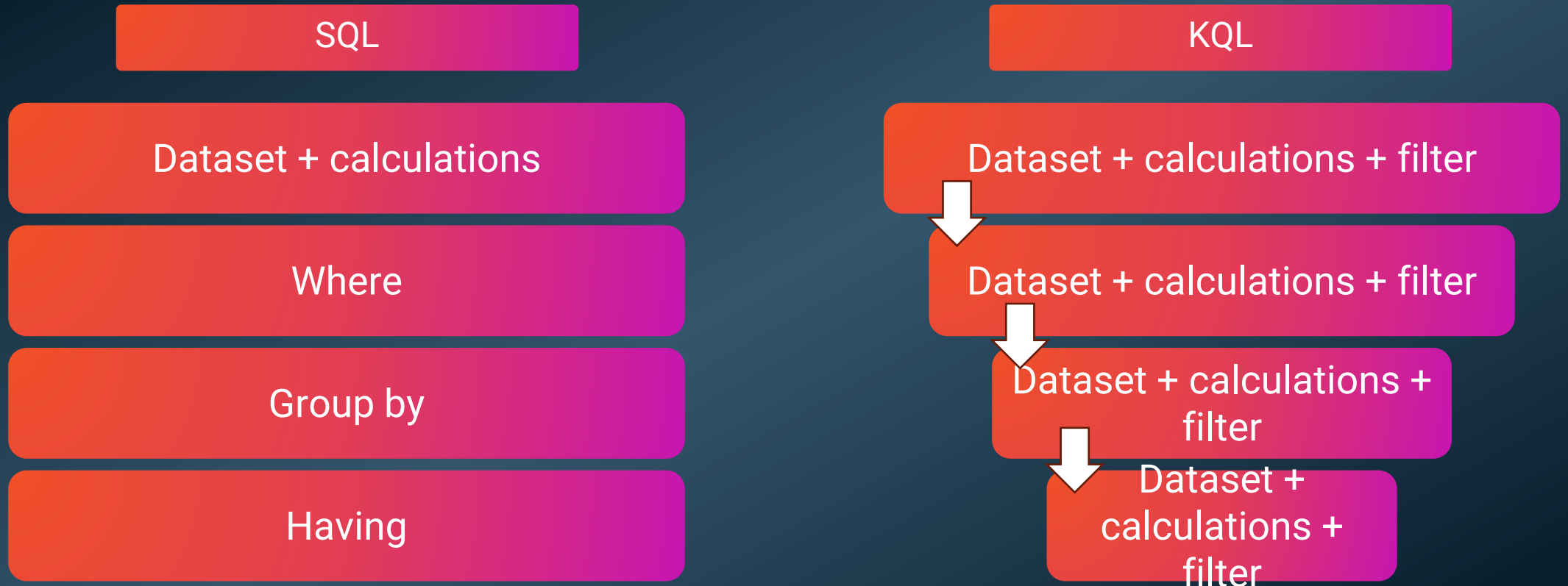
Get started for free

https://dataexplorer.azure.com/freecluster

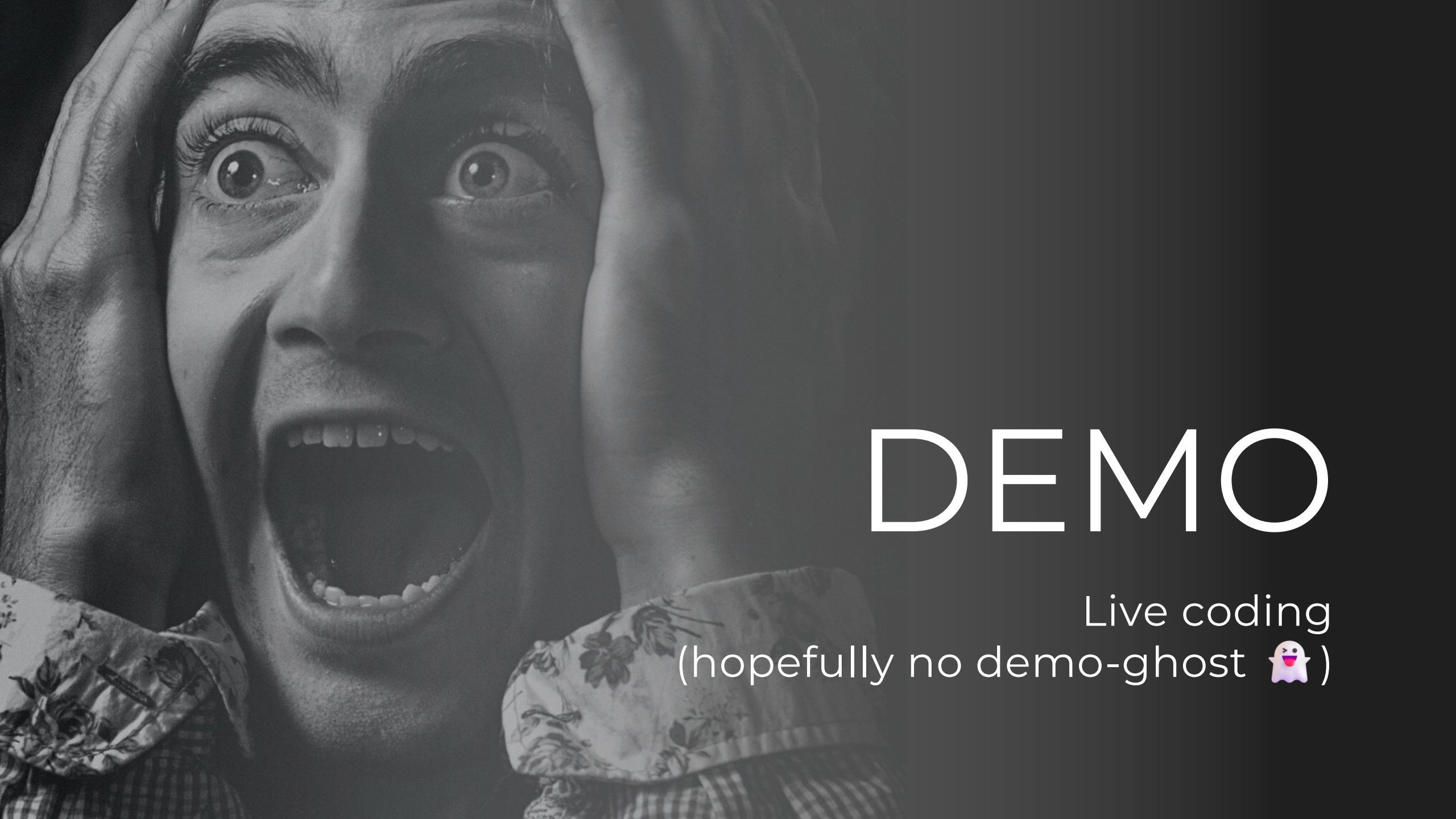
https://detective.kusto.io



The language and structure



SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn



DEMO

Live coding
(hopefully no demo-ghost 👻)

The language and structure

KQL: Kusto Query Language

SQL

```
select * from NYCTaxi
```

KQL

```
NYCTaxi
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

SQL

```
select * from NYCTaxi
where VentorID = 2
```

KQL

```
NYCTaxi
| where VendorID == 2
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

SQL

```
select * from NYCTaxi
where VentorID = 2
order by passenger_count
```

KQL

```
NYCTaxi
| where VendorID == 2
| order by passenger_count
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

SQL

```
select count(*) from
NYCTaxi
```

KQL

```
NYCTaxi
| count
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

SQL

```
select
    passenger_count
    ,VendorID
    ,trip_distance
from NYCTaxi
```

KQL

```
NYCTaxi
| project passenger_count, VendorID, trip_distance
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

SQL

```
select
    passenger_count
    ,VendorID
    ,trip_distance
    ,total_amount / passenger_count as AmtPsngr
from NYCTaxi
```

KQL

```
NYCTaxi
| extend AmtPsngr = total_amount / passenger_count
| project passenger_count, VendorID, trip_distance,
AmtPsngr
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

SQL

```
select
    sum(passenger_count) as SumPassenger
    ,VendorID
from NYCTaxi
group by VendorID
```

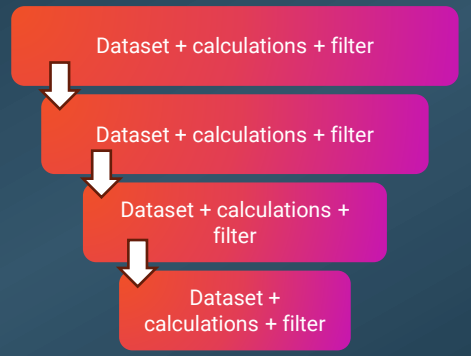
KQL

```
NYCTaxi
| summarize SumPassenger = sum(passenger_count) by
VendorID
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

The language and structure

KQL




```
NYCTaxi
| where passenger_count > 1
| project passenger_count, total_amount, VendorID, fare_amount
| extend AmtPsngr = total_amount / passenger_count
| where AmtPsngr > 10
| summarize TotalAmount = sum(total_amount), AvgAmtPsngr = avg(AmtPsngr) by VendorID
| where VendorID  <> 1
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

Forget everything you know about

query performance vs data types
&
data modelling best practices

Data modelling Kusto in Power BI

- Single table reporting can be a good option, if you can include all columns from dimensions to the table
- M:M relations are hard to avoid, but not a big deal → all queries will be translated to KQL
- All dimensions must be tagged with “IsDimension=true”
- Dimensions can be imported if they are <1 mio rows.
- INTEGER and DECIMAL er slow joins compared to STRING

Harness the Power (BI) of Kusto

Let Power BI build the KQL

- In Power Query
- Using DAX

Or build a Kusto function

Functions

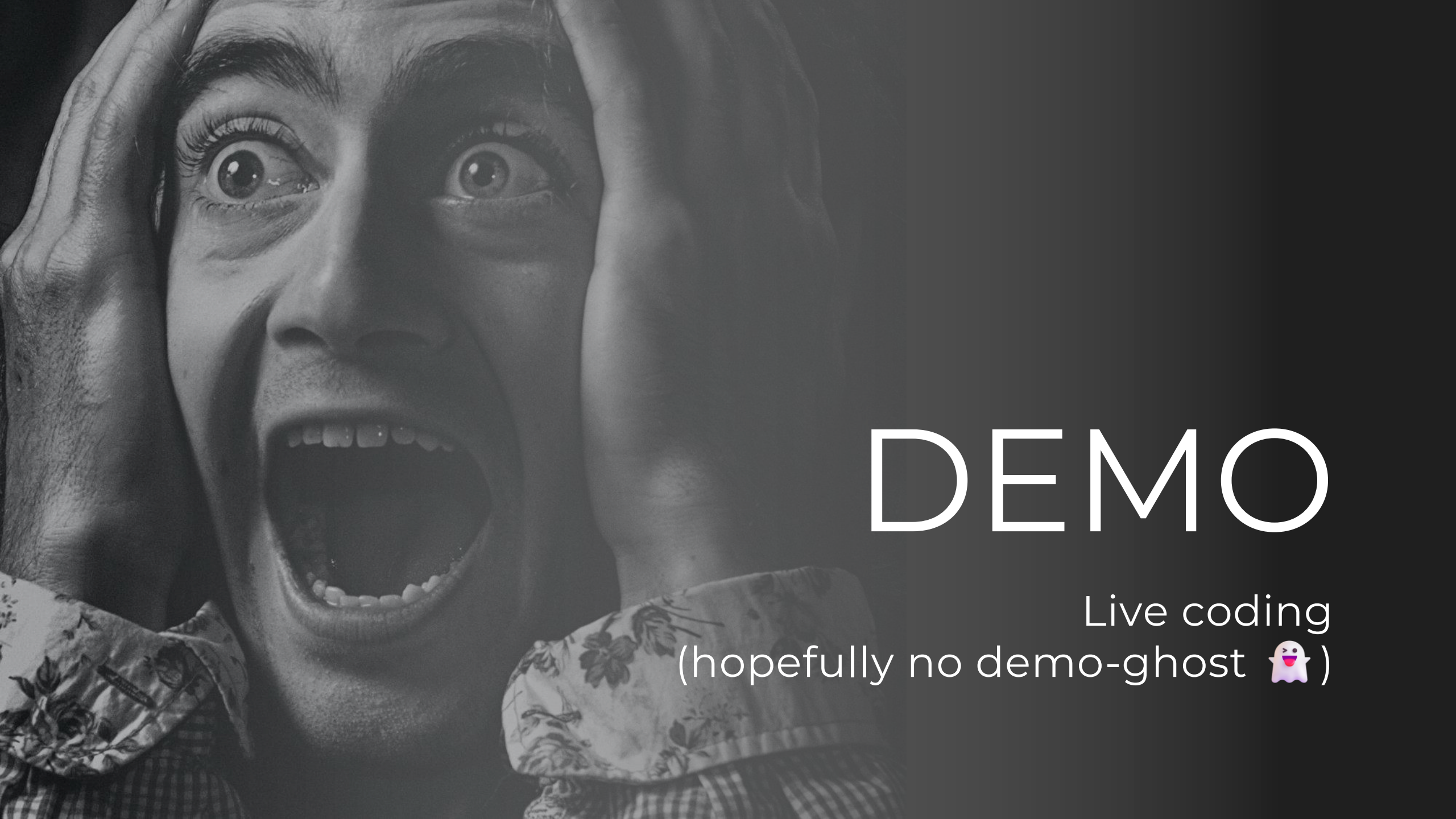
Functions in Kusto is equivalent to a stored procedure in the SQL world.

With additional functionality to be able to go outside of the cluster and service and ask for data from a different place in the world.

```
.create-or-alter function GetSysLogs(TimeWindow:string , Bucket:string )
{
cluster('help').database('SampleLogs').RawSysLogs
| where timestamp > ago(totimespan(TimeWindow))
| summarize LogCount=count() by name, bin(timestamp, totimespan(Bucket))
| order by timestamp asc
}

// to execute the function
GetSysLogs('5d','1h')
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn



DEMO

Live coding
(hopefully no demo-ghost 👻)

Data discovery and outlier detection

Data discovery is what we've just been through – use select statements and filter your data to find and explore the data given to you.

RENDERING!!

```
NYCTaxi
| where tpep_pickup_datetime between (datetime(2009-01-01)..datetime(2015-01-01))
| extend PickUpdate = startofday(tpep_pickup_datetime)
| summarize SumPsngrCount = sum(passenger_count) by PickUpdate
| project PickUpdate, SumPsngrCount
| render  timechart
    with(
        title = "timechart"
        ,xtitle = "Time"
        ,ytitle = "Fares"
    )
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

Data discovery and outlier detection

Outliers

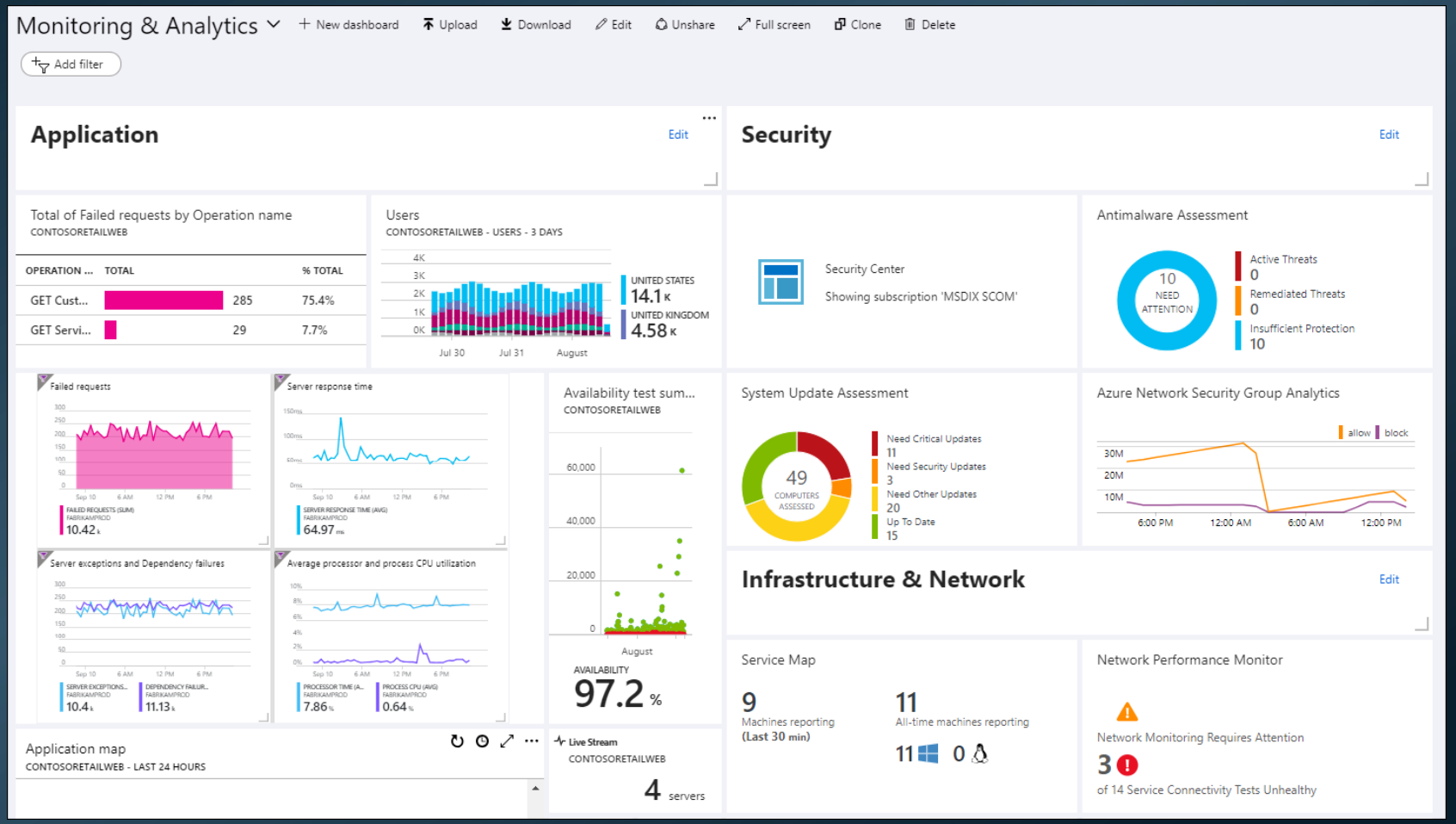
series_outliers() - LINK
series_decompose() - LINK
series_decompose_anomalies() - LINK
series_decompose_forecast() - LINK

```
range x from 0 to 364 step 1
| extend t = datetime(2023-01-01) + 1d*x
| extend y = rand() * 10
// generate a sample series with outliers at first day of each month
| extend y = iff(monthofyear(t) != monthofyear(prev(t)), y+20, y)
| summarize t = make_list(t), series = make_list(y)
| extend outliers=series_outliers(series)
| extend pos_anomalies = array_iff(series_greater_equals(outliers, 1.5), 1, 0)
| render anomalychart with(xcolumn=t, ycolumns=series, anomalycolumns=pos_anomalies)
```

SQL to Kusto query translation - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

Analysis and reporting

Dashboards in RTA – a free offering



Real-Time Intelligence

[Image from James Westall]

Thank you

https://aka.bi/follow
https://kql.how
https://dcode.bi
https://aka.bi/slides

Microsoft MVP
Microsoft Most Valuable Professional

Microsoft
FastTrack Recognized
Solution Architect
Power BI
2022 >>

Microsoft
Certified Trainer
Data Platform
2018 >>