From Zero to Kusto Hero at 30.000 ft

Special thanks to Fabric and Power BI Team at

Microsoft

This Summit presented to you by

RADACAD

Power BI & Fabric SUMMIT

Brian Bønk Rueløkke

Principal & Enterprise architect, Data & AI

Fellowmind

https://linkedin.com/in/brianbonk
https://brianbonk.dk
https://github.com/brianbonk

MVP Microsoft Most Valuable Professional

Microsoft
FastTrack Recognized
Solution Architect
Power BI
2022 >>

Microsoft
Certified Trainer
Data Platform

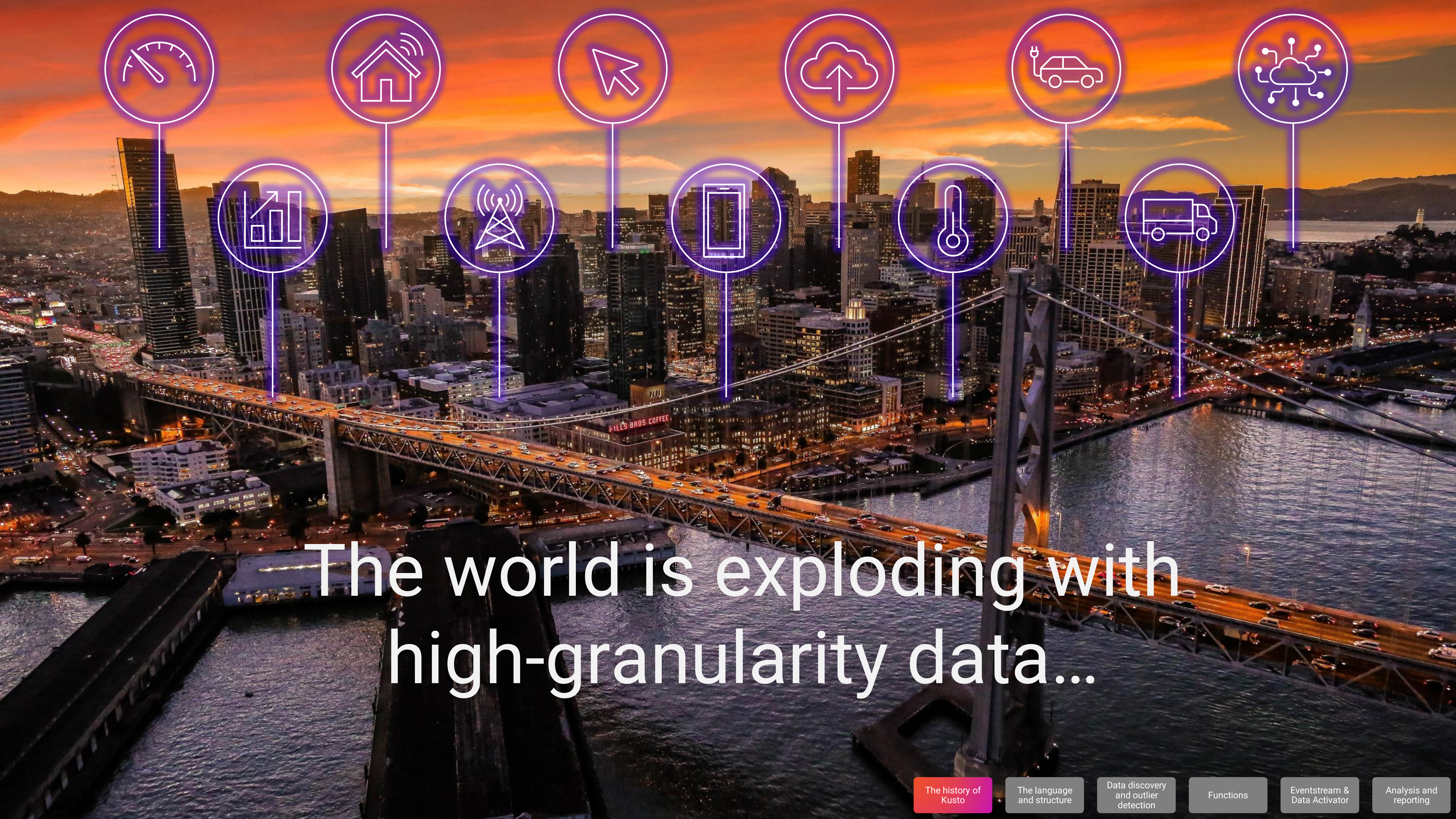
2018 >>

Agenda

- The history of Kusto
- The language and structure
- Data discovery and outlier detection
- Functions
- Eventstream & Data Activator
- Analysis and reporting

Jaques Cousteau
1910-1997

Jaques Cousteau 1910-1997



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

It all starts with data

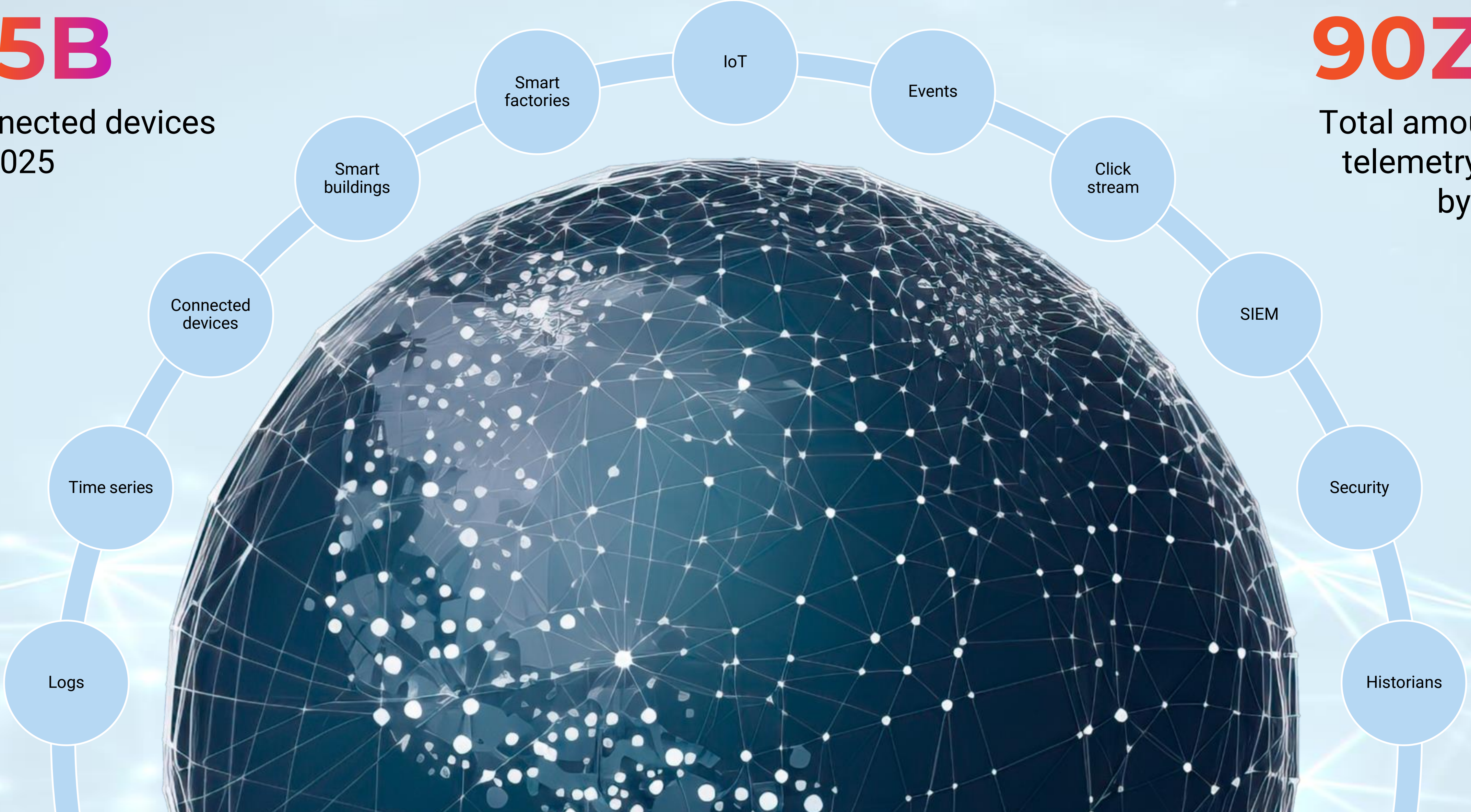
Telemetry – a key data for digital transformation

Telemetry – a key data for digital transformation

Telemetry – a key data for digital transformation

75B

Connected devices by 2025



Logs

Time series

Connected devices

Smart buildings

Smart factories

IoT

Events

Click stream

SIEM

Security

Historians

90ZB

Total amount of telemetry data by 2025

The history of Kusto

Azure Sentinel

Log Analytics

Real-Time Analytics

Azure resource graph

Microsoft 365 Defender

CMPivot

CMPivot

The language and structure

KQL: Kusto Query Language

SQL	KQL
select * from NYCTaxi	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

SQL

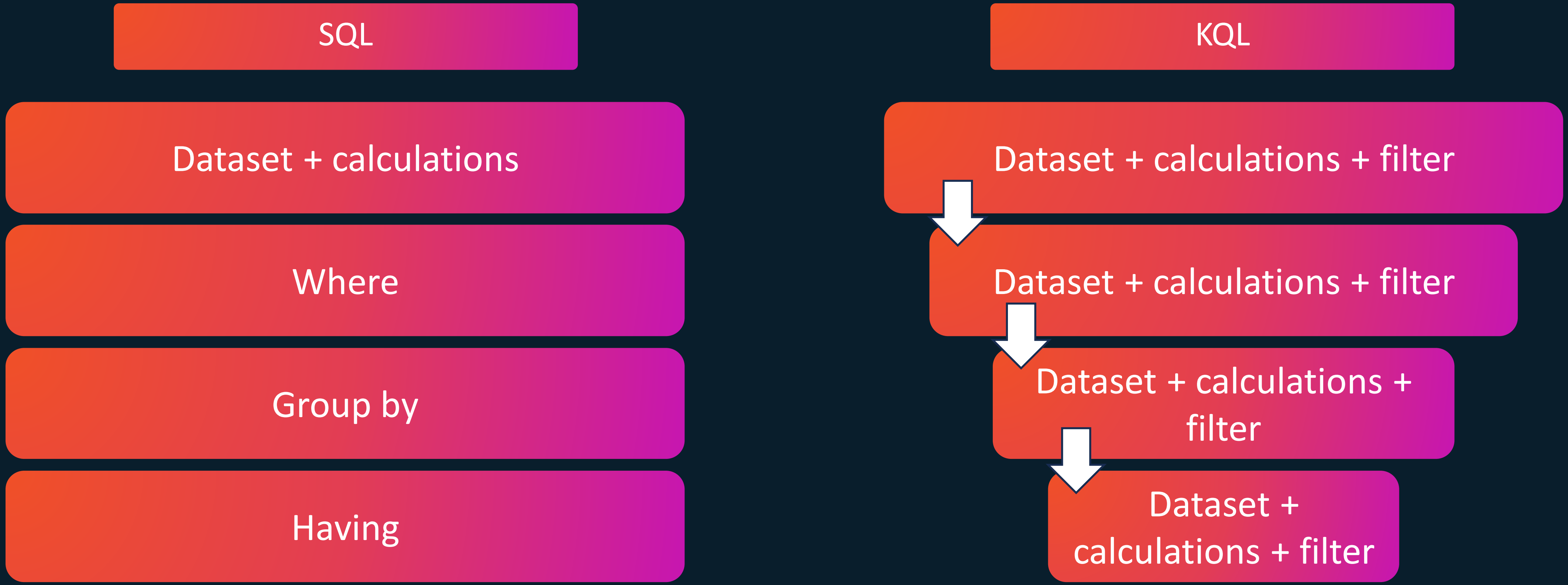
```
select
   sum(passenger_count) as SumPassenger
   ,VendorID
from NYCTaxi
group by VendorID
```

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



SQL

Dataset + calculations

Where

Group by

Having

KQL

Dataset + calculations + filter

Dataset + calculations + filter

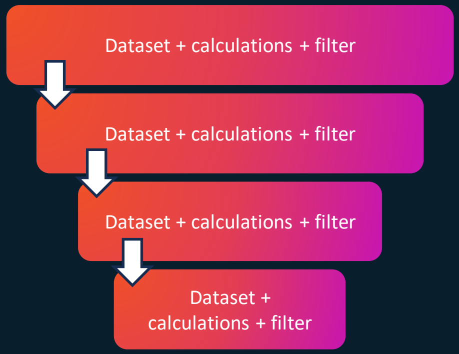
Dataset + calculations + filter

Dataset + calculations + filter

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

The language and structure

KQL



Dataset + calculations + filter

Dataset + calculations + filter

Dataset + calculations + filter

Dataset + calculations + filter

```
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

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

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.

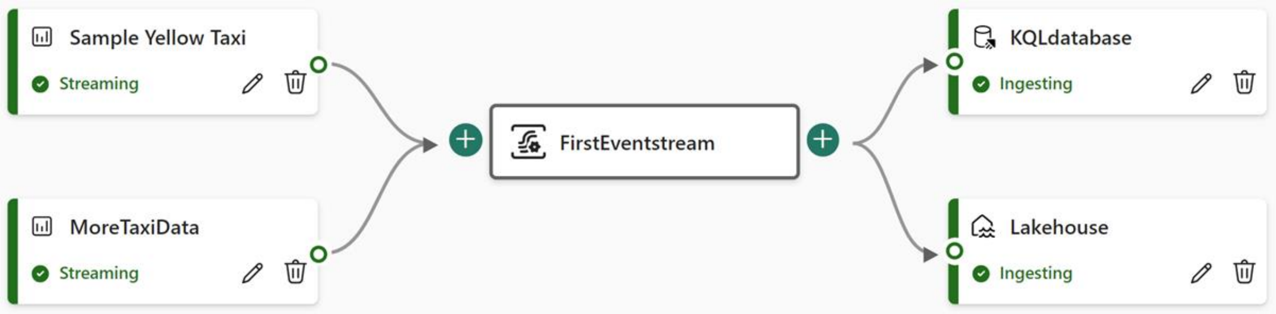
```
.create-or-alter function GetSysLogs(TimeWindow:string , Bucket:string )
{
cluster('help').database('SampleLogs').RawSysLogs
| where timestamp > ago(totimespan(TimeWindow))
| summarize LogCount=count() by name, bin(timestamp, totimespan(Bucket))
| order by timestamp asc
}

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

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

Eventstream and Data Activator

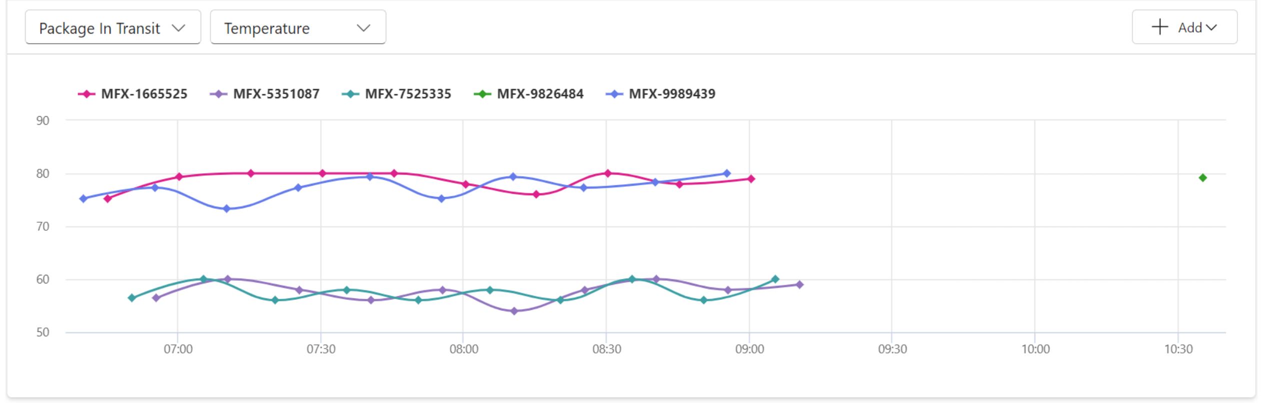
Eventstream

The brand-new 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.



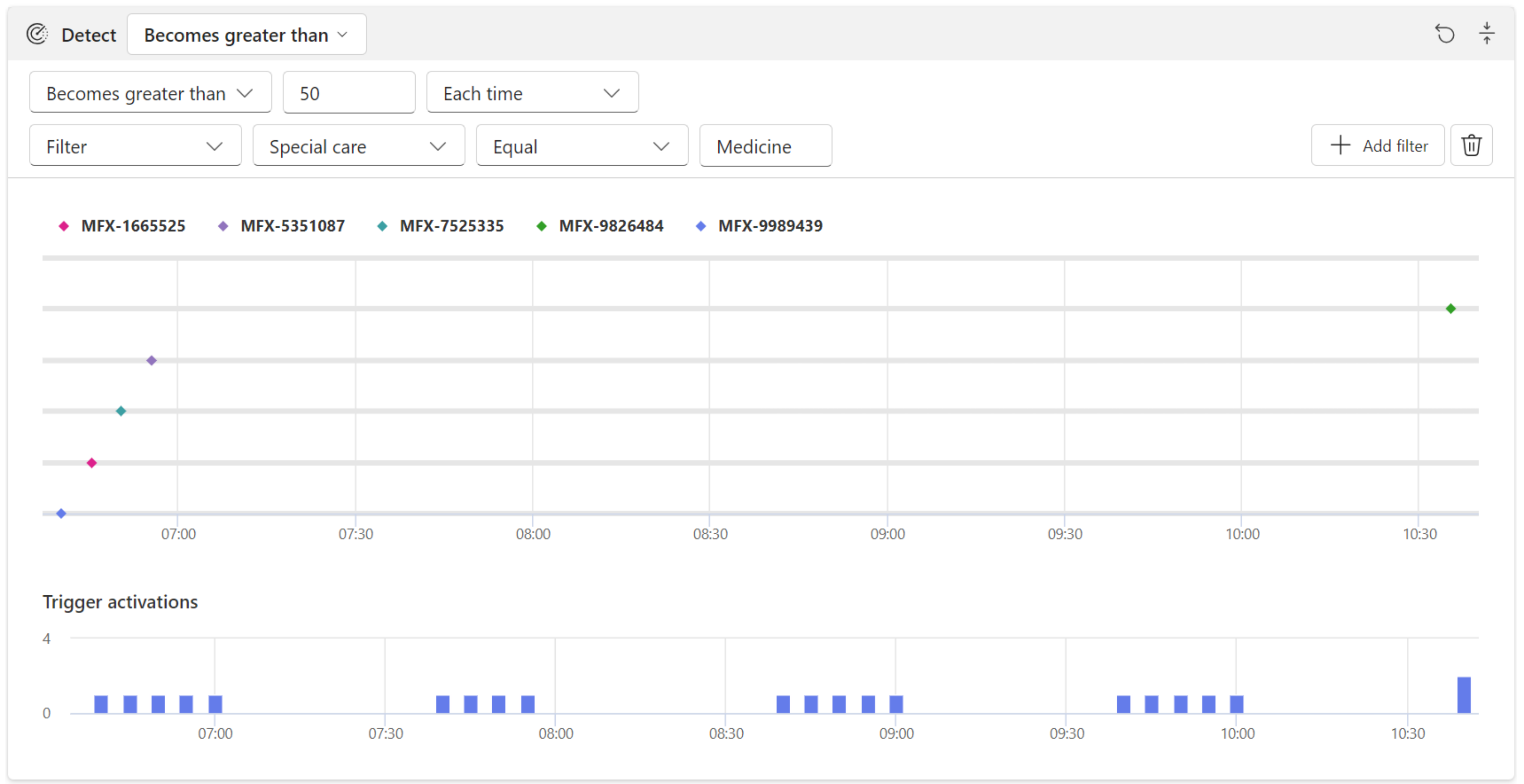
Data Activator

Activeli listens to your data from either the Eventstream service or a Power BI dataset.
Can react to values outside of defined boundaries and, for now, send an e-mail for a Teams message.



Eventstream and Data Activator

Data Activator



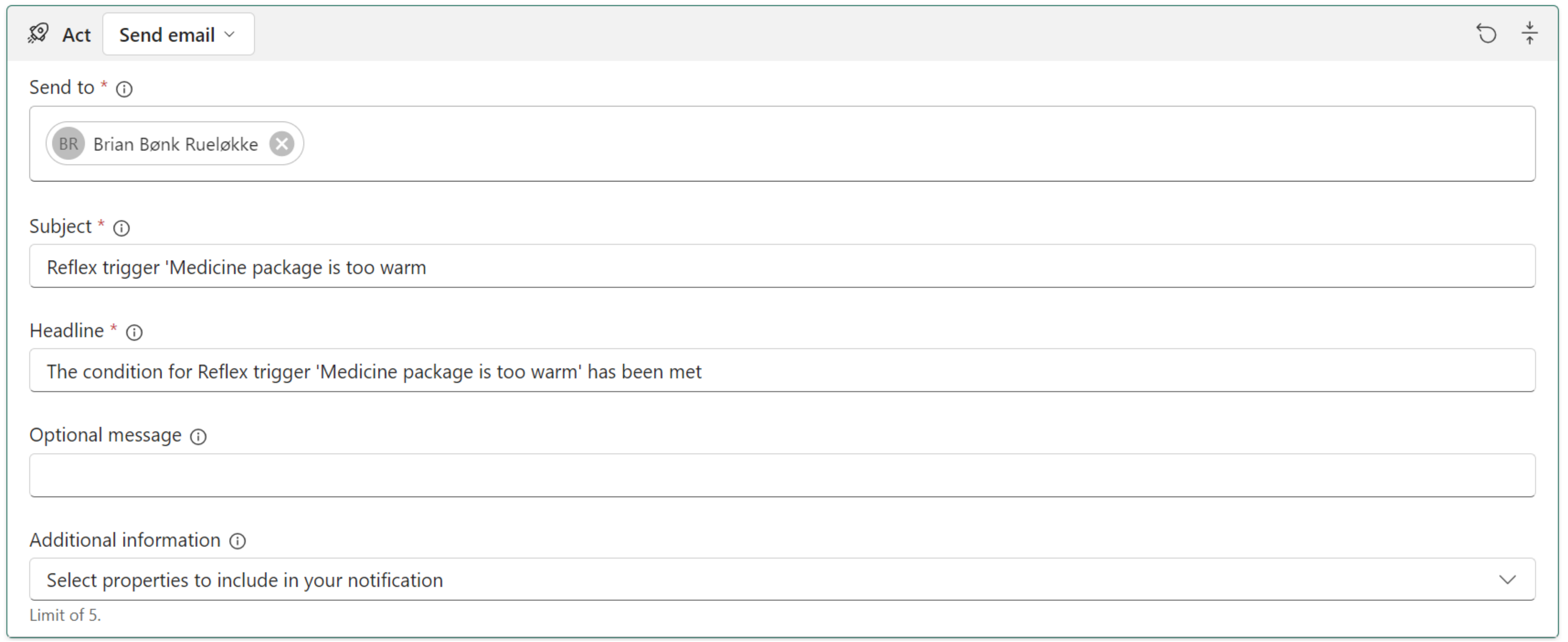
Detect: Becomes greater than

Becomes greater than | 50 | Each time

Filter | Special care | Equal | Medicine

Eventstream and Data Activator

Data Activator



Send to *

BR Brian Bønk Rueløkke

Subject *

Reflex trigger 'Medicine package is too warm

Headline *

The condition for Reflex trigger 'Medicine package is too warm' has been met

Optional message

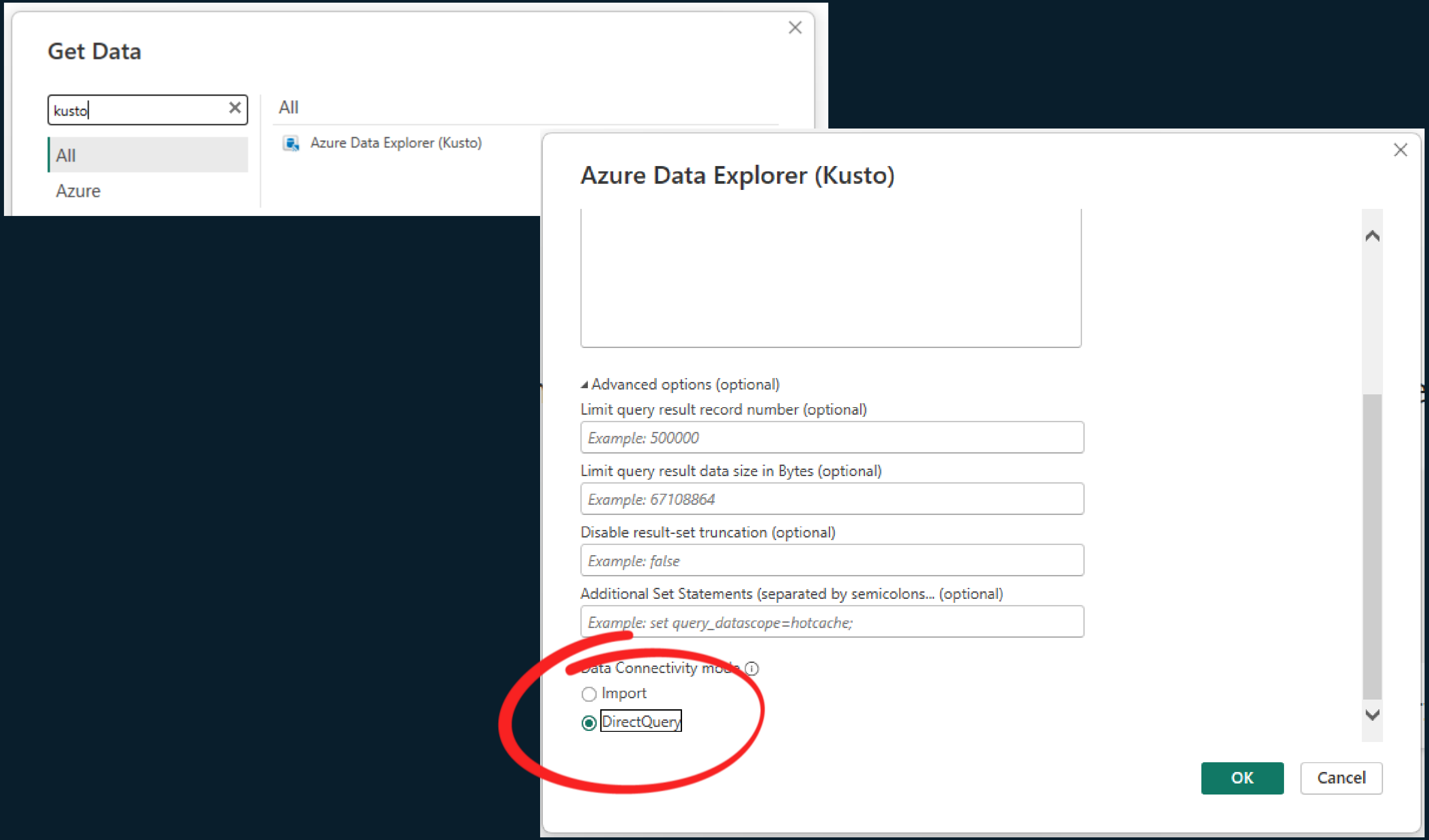
Additional information

Select properties to include in your notification

Limit of 5.

Analysis and reporting

Power BI



Get Data

kusto

All

Azure

All

Azure Data Explorer (Kusto)

Azure Data Explorer (Kusto)

▴ Advanced options (optional)

Limit query result record number (optional)

Example: 500000

Limit query result data size in Bytes (optional)

Example: 67108864

Disable result-set truncation (optional)

Example: false

Additional Set Statements (separated by semicolons... (optional)

Example: set query_datascope=hotcache;

Data Connectivity mode ⓘ

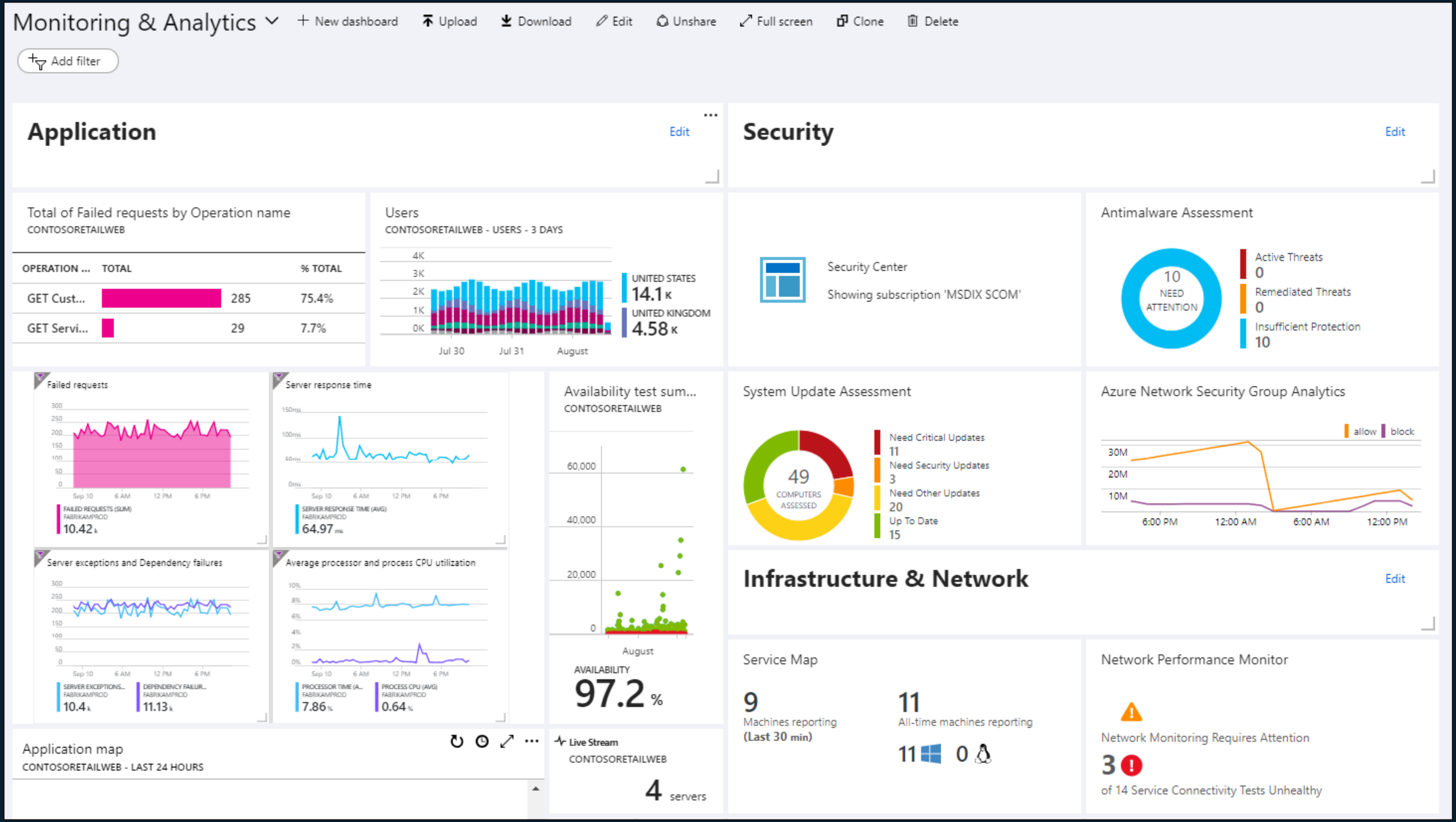
○ Import

● DirectQuery

Analysis and reporting

Real-Time Analytics

Dashboards in RTA - planned - to come…



Total of Failed requests by Operation name
CONTOSORETAILWEB

OPERATION ...	TOTAL	% TOTAL
GET Cust...	285	75.4%
GET Servi...	29	7.7%

Image from James Westall

Summary

- The history of Kusto
- The language and structure
- Data discovery and outlier detection
- Functions
- Eventstream & Data Activator
- Analysis and reporting

Thank you

Connect with me at:

https://linkedin.com/in/brianbonk
https://brianbonk.dk
https://github.com/brianbonk

Stay on-line for the Q&A sesssion

Power BI & Fabric SUMMIT