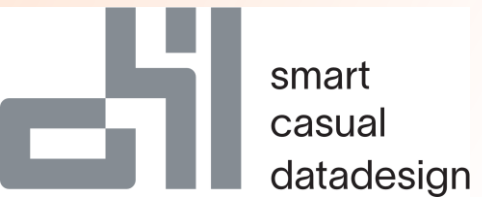


Kusto

An introduction





Brian Bønk Rueløkke

Principal & Enterprise architect, Data & AI

Fellowmind

 <https://linkedin.com/in/brianbonk>

 <https://brianbonk.dk>

 <https://github.com/brianbonk>



FastTrack Recognized
Solution Architect
Power BI
2022 >>



Certified Trainer
Data Platform

2018 >>



**REAL-TIME
ANALYTICS &
KUSTO**



REAL-TIME ANALYTICS & KUSTO

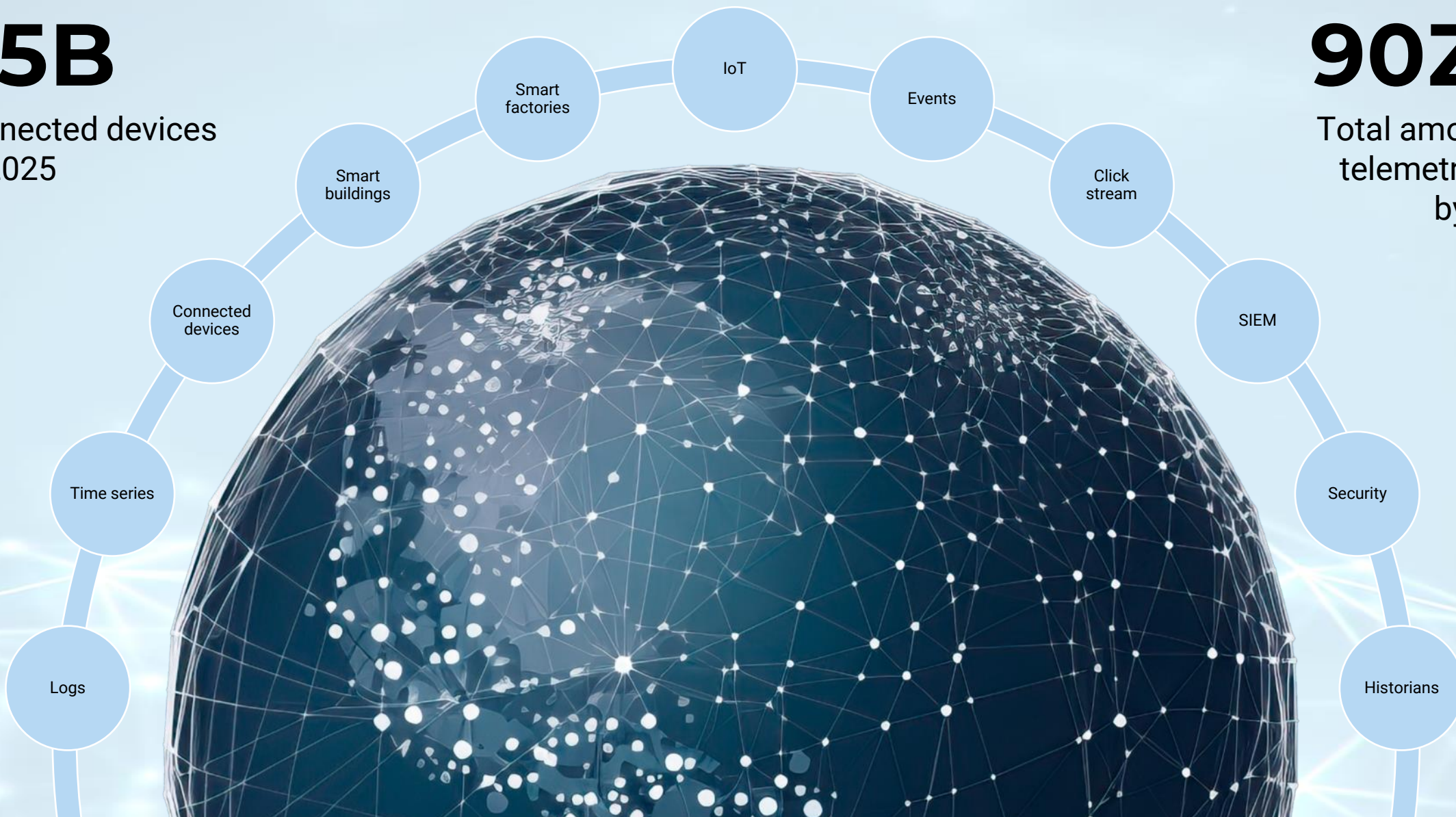


The world is exploding with high-granularity data and the need for faster loads are increasing



75B

Connected devices
by 2025



90ZB

Total amount of
telemetry data
by 2025

An underwater photograph showing a deep blue sea with sunlight rays filtering down from the surface. Several dark-colored fish are swimming in the center, flanked by steep, rocky cliffs covered in coral and marine life. The scene is serene and mysterious.

DIVE INTO HISTORY



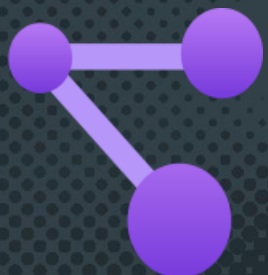
Azure Sentinel



Log Analytics



Real-Time Analytics



Azure resource
graph



Microsoft 365
Defender

CMPIVOT

CMPIVOT



Jacques Cousteau
1910-1997



Jaques Cousteau
1910-1997

KQL database

Key capabilities

Unlimited Scale
(query, ingestion
and storage)

Any data source

Any data format

Structured
Semi-structured
Free-text

Real-time
transformation of
complicated data
structures

Streaming analytics
in Near-Real-Time

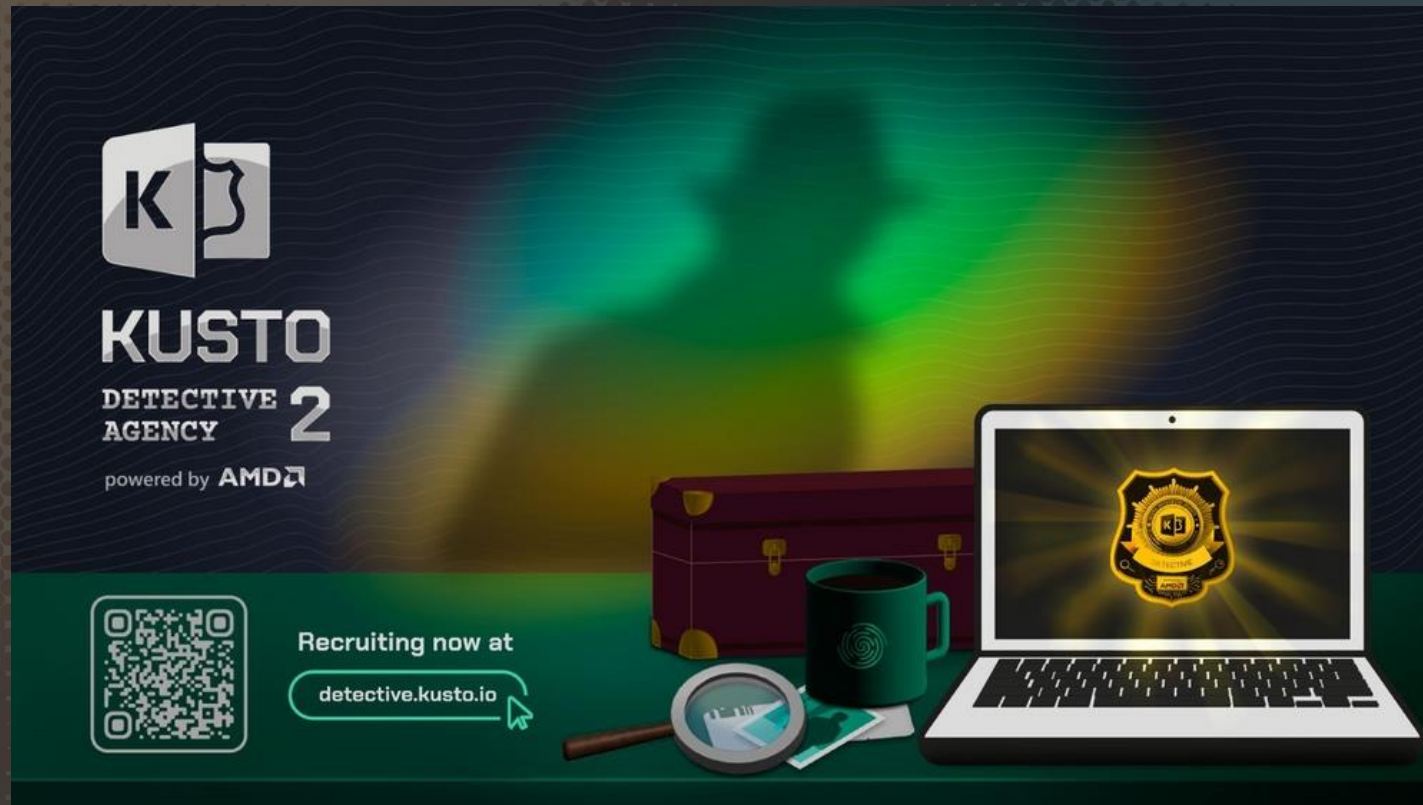
High performance
Low latency
High freshness

Timeseries database

Everything is
indexed and
partitioned

<https://dataexplorer.azure.com/freecluster>

<https://detective.kusto.io>





THE FABRIC EXPERIENCE



Microsoft Fabric

Get data



Data Factory

Prepare data



Synapse Data Engineering



Synapse Data Warehouse



Synapse Data Science



Synapse Real-Time Analytics

Use data



Data Activator



Power BI

Store data



OneLake



Microsoft Fabric

Get data



Data Factory



Synapse Data
Engineering



Synapse Data
Warehouse



Synapse Data
Science



Synapse Real-Time
Analytics



Data Activator



Power BI

Prepare data

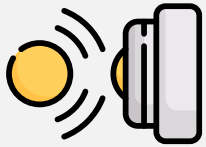
Store data



OneLake



Microsoft Fabric



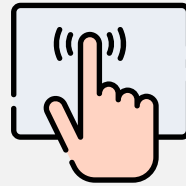
Event
ingestion



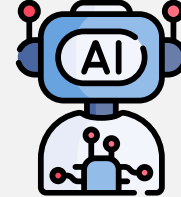
Real-Time
analytics



Real-Time
dashboards



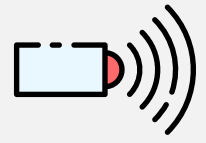
Real-Time
triggers



Real-Time
AI



Real-Time
applications



Event driven
actions

Get data



Data Factory

Prepare data



Synapse Data
Engineering



Synapse Data
Warehouse



Synapse Data
Science

Use data



Synapse Real-Time
Analytics



Data Activator



Power BI



DEMONSTRATION

The language and structure

SQL

Dataset + calculations

Where

Group by

Having

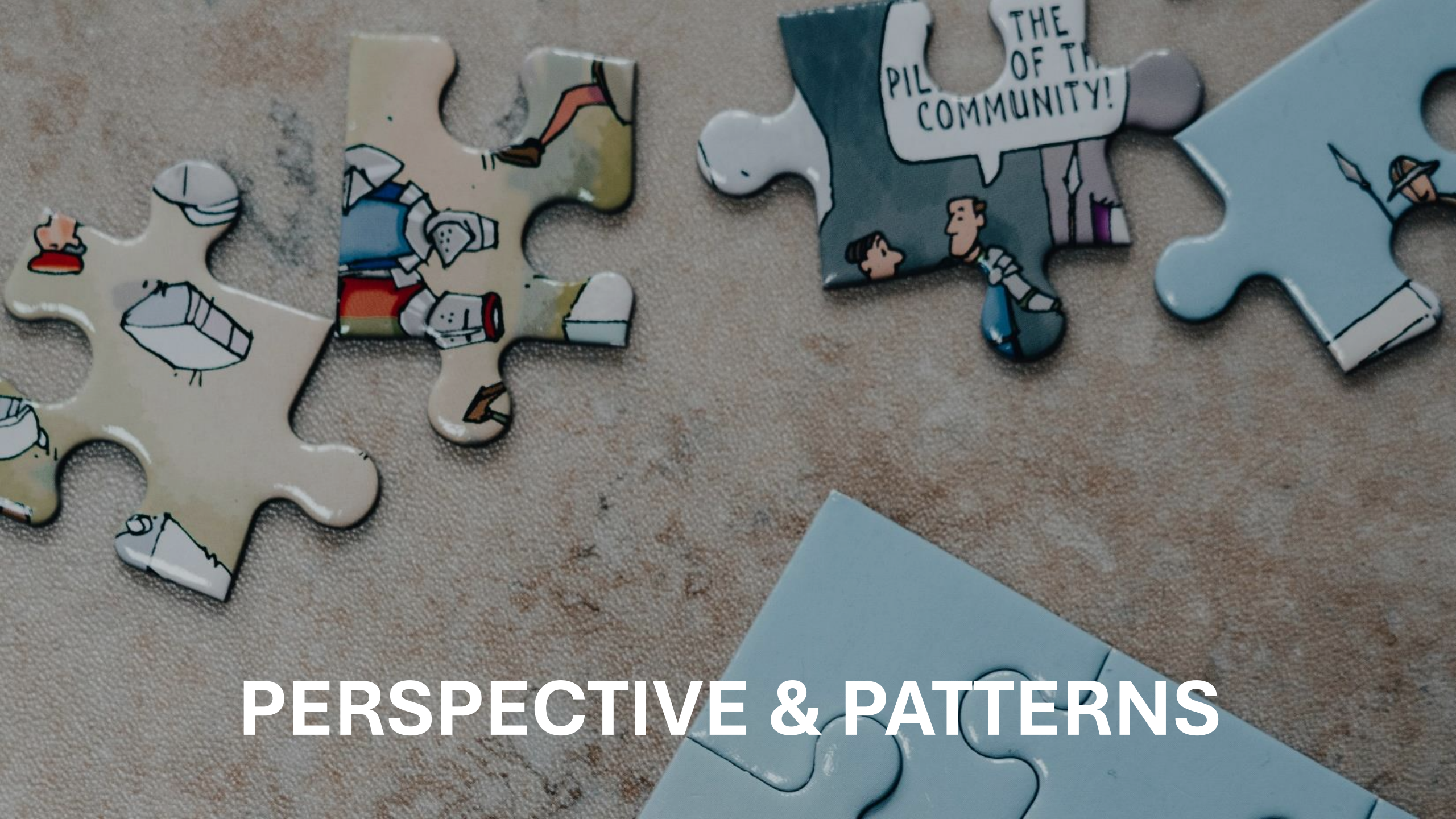
KQL

Dataset + calculations + filter

Dataset + calculations + filter

Dataset + calculations +
filter

Dataset +
calculations + filter



PERSPECTIVE & PATTERNS

Sources



Eventstream



Pipeline



Shortcuts &
External tables



Eventhouse



KQL Database



Tables

Bronze



KQL Database



Tables

Silver



Update
policies



Shortcuts & External tables

```
//External tables - shortcuts
//connect to operational Database with external table Address

.create external table products (AddressID: int, StreetName: string, City: string)
kind=sql
table=[SalesLT.Address]
(
    h@'Server=tcp:adxdemo.database.windows.net,1433;Initial Catalog=aworks;User
Id=sqlread;Password=ChangeYourAdminPassword1'
)
With
(
createifnotexists = true
)
```

Update policies

```
.create function ifnotexists with (docstring = 'Add ingestion time to raw data')
ParseAddress ( ) { Address | extend IngestionDate = ingestion_time() }.alter table SilverAddress policy
update@[{"Source": "Address", "Query": "ParseAddress", "IsEnabled" : true,
"IsTransactional": true }]
```



Shortcuts & External tables

```
//External tables - shortcuts

//connect to operational Database with external table Product

.create external table products (ProductID: int, ProductNumber: string, Name: string)
kind=sql
table=[SalesLT.Product] (
    h@'Server=tcp:adxdemo.database.windows.net,1433;Initial Catalog=aworks;User Id=sqlread;Password=ChangeYourAdminPassword1'
)
With (
    createifnotexists = true )
```

Update policies

```
.create function ifnotexists
with (docstring = 'Add ingestion time to raw data')
ParseAddress ()
{
    Address
    | extend IngestionDate = ingestion_time()
}
```








Update policies



```
.create function ifnotexists
with (docstring = 'Add ingestion time to raw data')
ParseAddress ()
{
Address
| extend IngestionDate = ingestion_time()
}


.alter table
SilverAddress
policy update @' [{"Source": "Address", "Query":
"ParseAddress", "IsEnabled" : true, "IsTransactional":
true } ]'
```


Sources

 
Eventstream

 
Pipeline

 
Shortcut

 Eventhouse


 KQL Database



Tables

Bronze

Update
policies

 KQL Database



Tables

Silver



Materialized
views

Gold





Materialized views



```
//GOLD LAYER
//use materialized views to view the latest changes in
the tables


.create materialized-view with (backfill=true) GoldAddress
on table SilverAddress
{
SilverAddress
| summarize arg_max(IngestionDate, *) by AddressID
}
```


Sources

 
Eventstream

 
Pipeline

 
Shortcut

 Eventhouse


 KQL Database



Tables

Bronze

Update
policies

 KQL Database



Tables

Silver



Materialized
views

Gold

Real-Time
Dashboard
(on roadmap)





Sub 1 second

THANK YOU!

Brian Børnk Rueløkke

Principal & Enterprise architect, Data & AI

Fellowmind



 <https://linkedin.com/in/brianbonk>

 <https://brianbonk.dk>

 <https://github.com/brianbonk>



 **Microsoft**
FastTrack Recognized
Solution Architect
Power BI
2022 >>

 **Microsoft**
Certified Trainer
Data Platform
2018 >>