PASS 24
Data Community Summit

From Junior Detective to Senior Data Sleuth – Threat hunting with Fabric

Brian Bønk

He/Him

Senior Principal, Data Platform MVP

Intellishore

Brian

Bønk

he/him

Senior Principal, Data Platform MVP

Intellishore

Been working within the sphere of data for more than two decades.

Currently helping the Intellishore company in Denmark to the next level within the Microsoft data platform.

Love meeting new people and help them be better tomorrow.

/in/brianbonk

https://dcode.bi

The learning path – Fabric Real-Time Intelligence

Real World Uses for Fabric Real-Time Intelligence: An Introduction

Nov 6 – 9:45 AM

Marthe Moegen & Frank Geisler

Real-Time Hub: Starting Point of Real-Time Intelligence in Fabric

Nov 6 – 11:15 AM

Matt Gordon & Devang Shah

From Junior Detective to Senior Data Sleuth: Threat Hunting with Fabric

Nov 6 – 2:00 PM

Brian Bønk

Take Real-Time Action on Your Real-Time Data

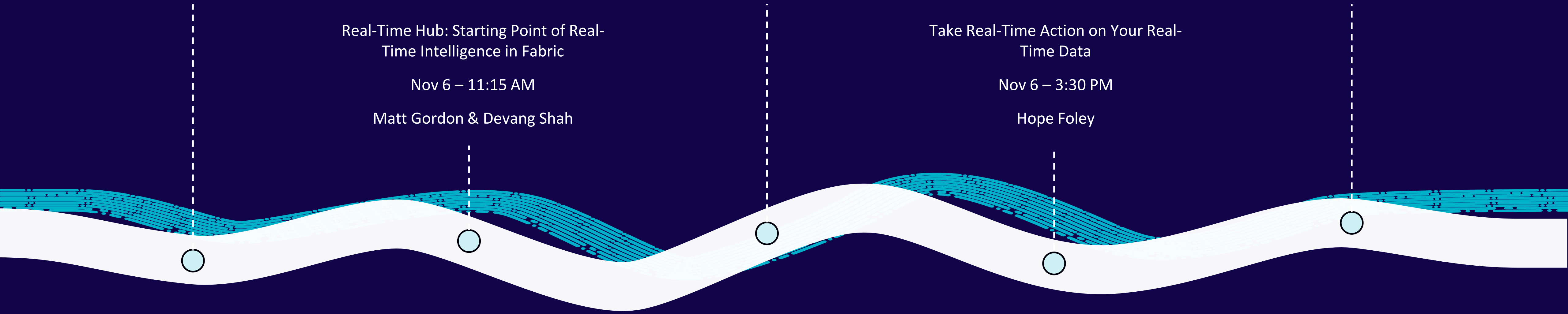
Nov 6 – 3:30 PM

Hope Foley

Securing and Automating Your Fabric Real-Time Intelligence Assets

Nov 7 – 9:45 AM

Johan Brattås



From Junior Detective to Senior Data Sleuth: Threat Hunting with Fabric

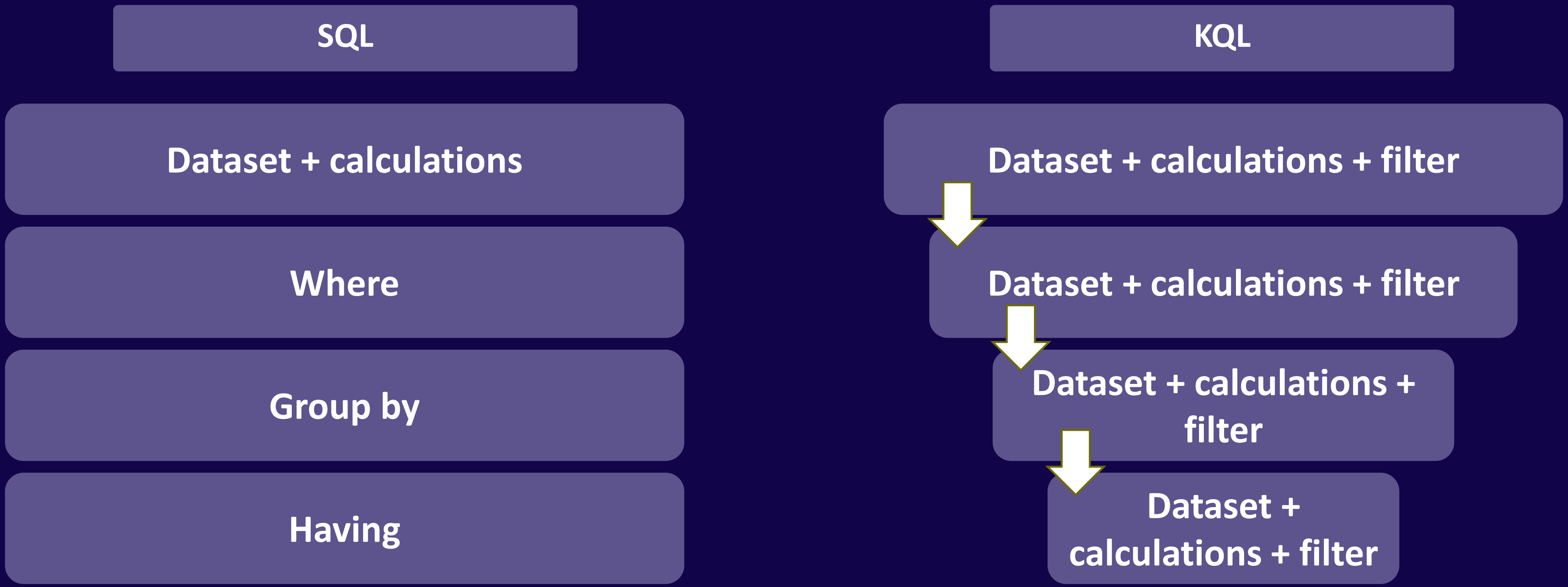
Introduction to the KQL language

Your first KQL script – you already know it

Adding insights and outliers

The graph perspective

Introduction to the KQL language



SQL

Dataset + calculations

Where

Group by

Having

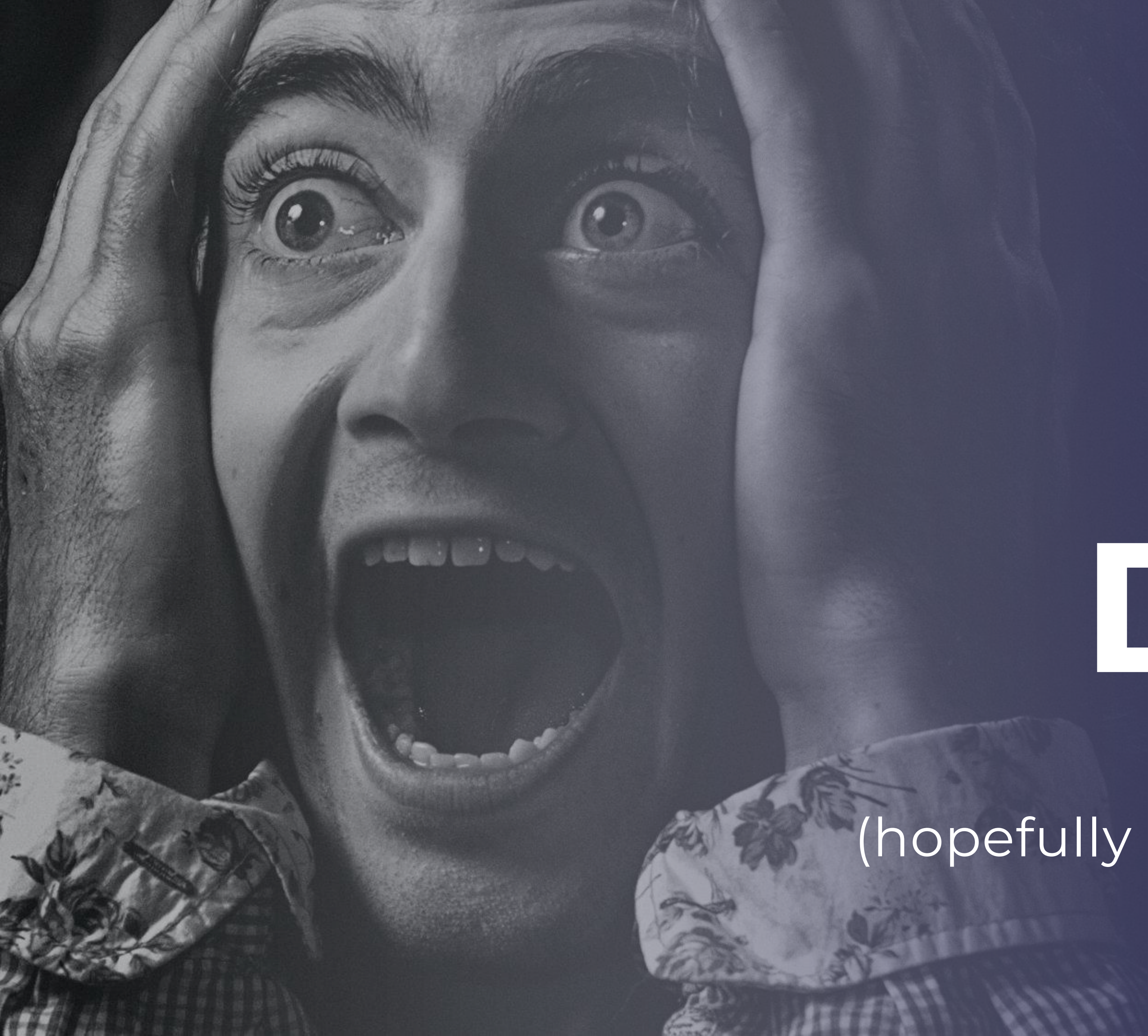
KQL

Dataset + calculations + filter

Dataset + calculations + filter

Dataset + calculations + filter

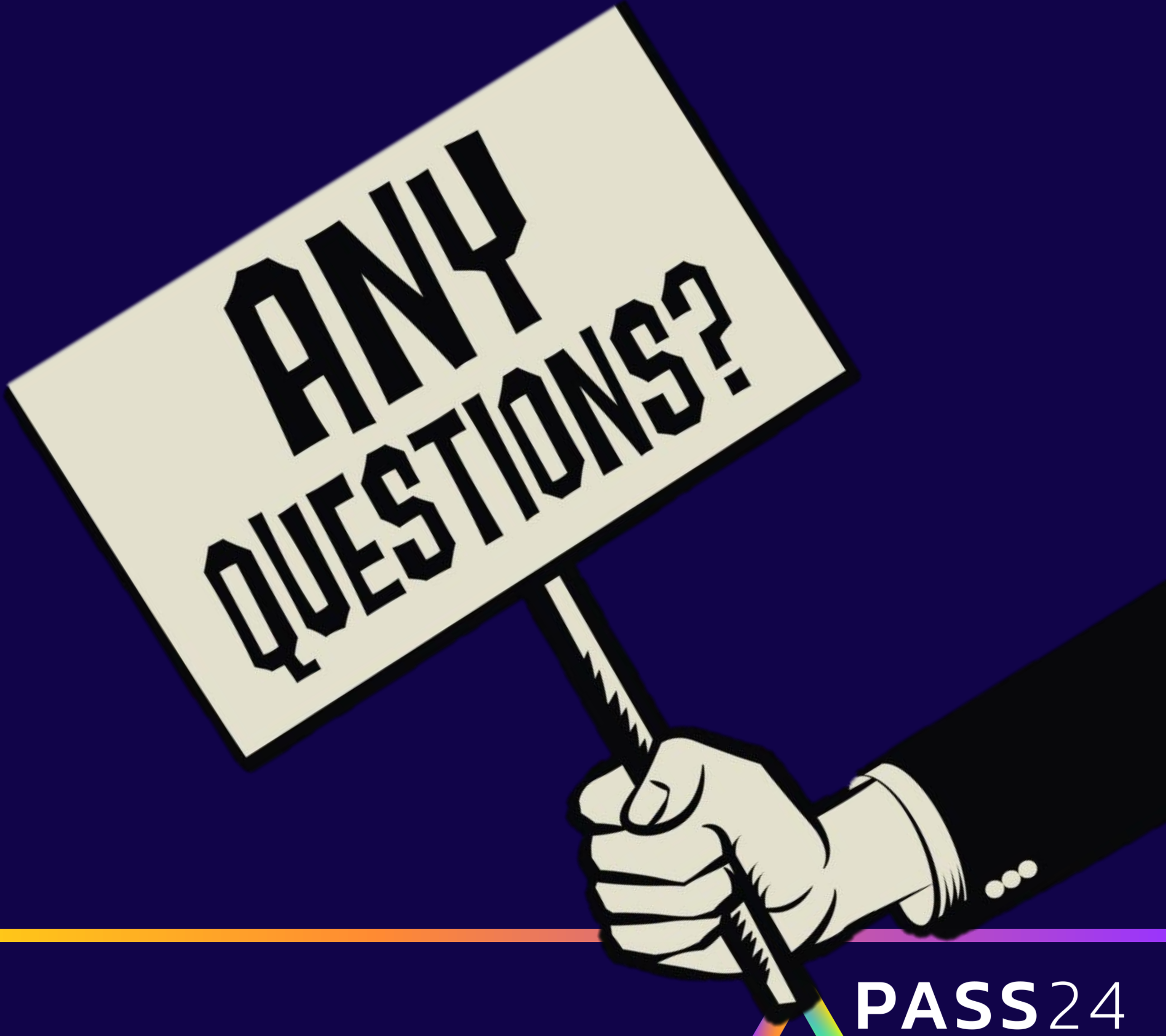
Dataset + calculations + filter



DEMO

Live coding
(hopefully no demo-ghost 👻)

Introduction to the KQL language



Your first KQL script – you already know it

DEMO

Live coding
(hopefully no demo-ghost 👻)

Your first KQL script – you already know it

Adding insights and outliers

Aggregations and calculations

The summarize function is the key

String manipulation

Use the parse_where

Forecast

series_decompose_forecast()

Outliers

series_outliers()

DEMO

Live coding
(hopefully no demo-ghost 👻)

Adding insights and outliers

Aggregations and calculations

The summarize function is the key

String manipulation

Use the parse_where

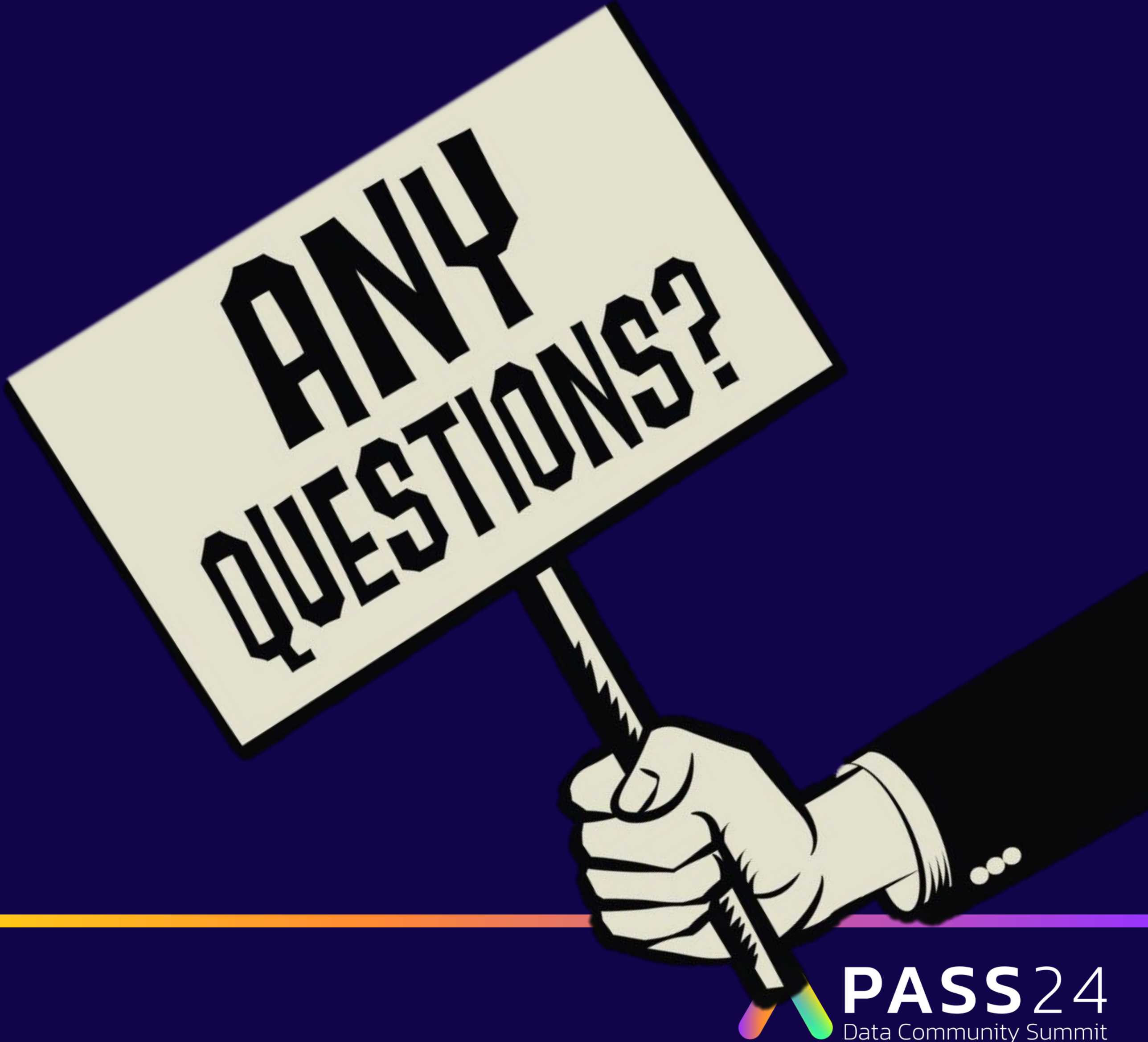
Forecast

series_decompose_forecast()

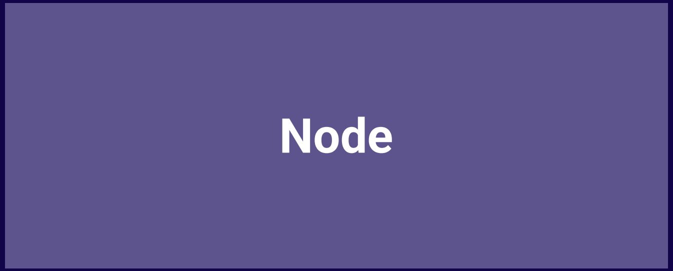
Outliers

series_outliers()

Adding insights and outliers



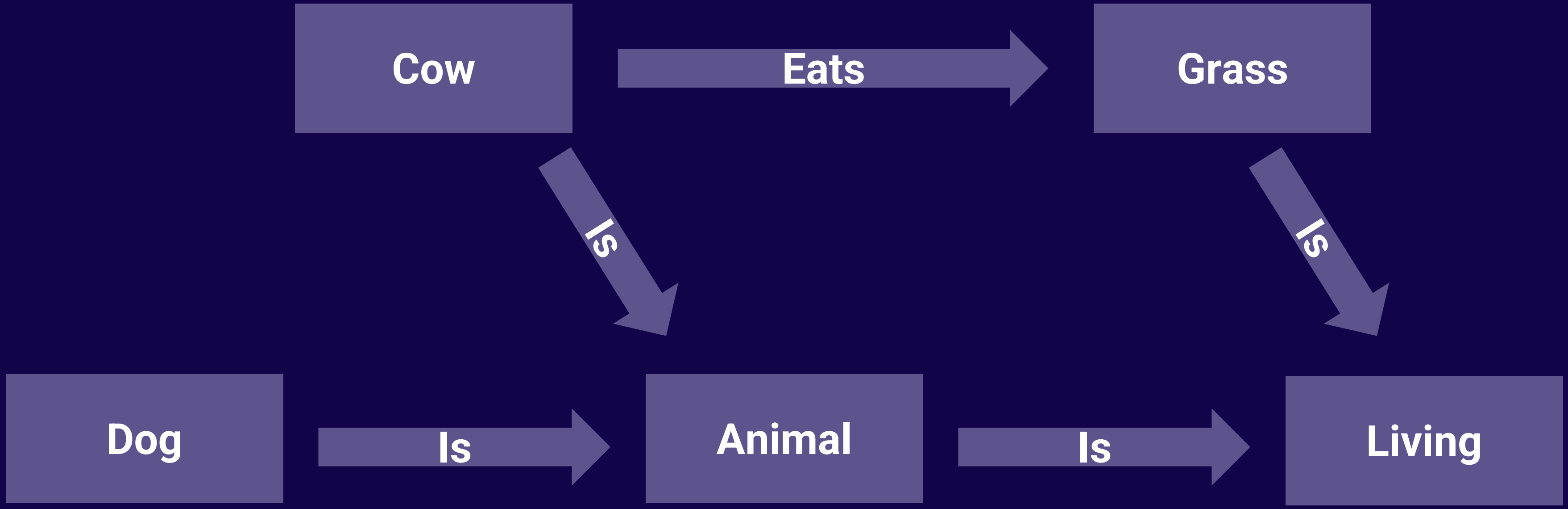
The graph perspective



A node is an object in a problem or process.

An edge is the connection “actions” between two nodes

The graph perspective



Introduction to the KQL language

Your first KQL script – you already know it

Adding insights and outliers

The graph perspective

Here is our missing, if we choose to accept it

The entire network has been infected, and we need to find the path of infection....

Where did the virus enter and how did it spread to the entire company?

Your mission is to find the entry point and crawl your way through the network and find the last machine in the chain....

LET’S DO IT

Feedback

Thank you

Go get them!

Brian Bønk

/in/brianbonk

https://dcode.bi