Kusto Query Language From Scratch

INTRODUCTION

Robert C. Cain, MVP
OWNER, ARCANE TRAINING AND CONSULTING
@arcanecode www.arcanecode.com

Agenda

- Introduction
- 80% of the Operators You'll Ever Use
- Scalar Operators
- Advanced Aggregations
- Working with Datasets
- Time Series
- Machine Learning
- Exporting Data
- Summary

What is KQL

KQL – The Kusto Query Language

Kusto Engine

Where to use KQL

Azure Log Analytics

Azure Application Insights

Windows Defender Advanced Threat Protection

Azure Security Center

Demo Platforms

Log Analytics - https://aka.ms/LADemo

Application Insights - https://aka.ms/AIAnalyticsDemo

ATP – https://aka.ms/WinDefATP

Demo

Using the Log Analytics Demo Portal

Summary

Introduction

80% of the Operators You'll Ever Use

Scalar Operators

Advanced Aggregations

Working with Datasets

Time Series

Machine Learning

Exporting Data

Summary

Summary

Introduction

80% of the Operators You'll Ever Use

Scalar Operators

Advanced Aggregations

Working with Datasets

Time Series

Machine Learning

Exporting Data

Summary