

# Kusto Query Language From Scratch

---

## INTRODUCTION



**Robert C. Cain, MVP**

OWNER, ARCANE TRAINING AND CONSULTING

@arcanecode [www.arcanecode.com](http://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



**Powered by Kusto**

**KQL – The Kusto Query Language**  
**Kusto Engine**



# Where to use KQL



Application Insights

Windows Defender Security Center



Azure Log Analytics

App Insights Data

Windows Defender  
Advanced Threat  
Analytics

Azure Server Logs



# Demo Platforms



Azure Log Analytics

<https://aka.ms/LADemo>



Application Insights

<https://aka.ms/AIAalyticsDemo>

Windows Defender Security Center

<http://bit.ly/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

