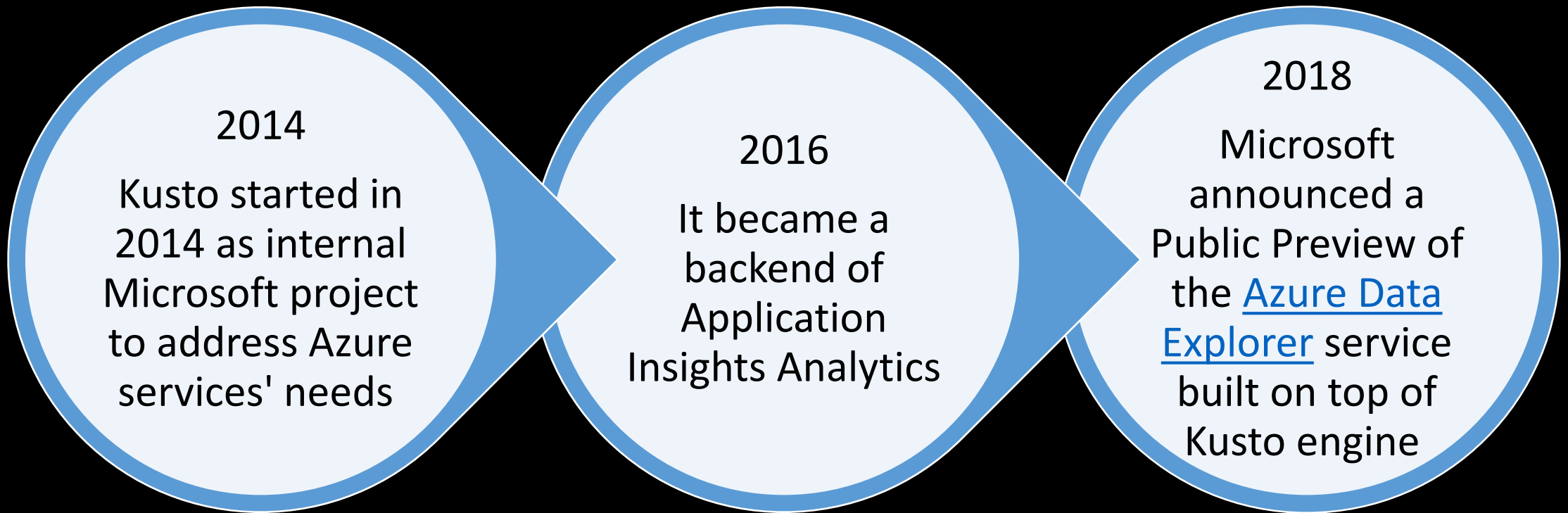
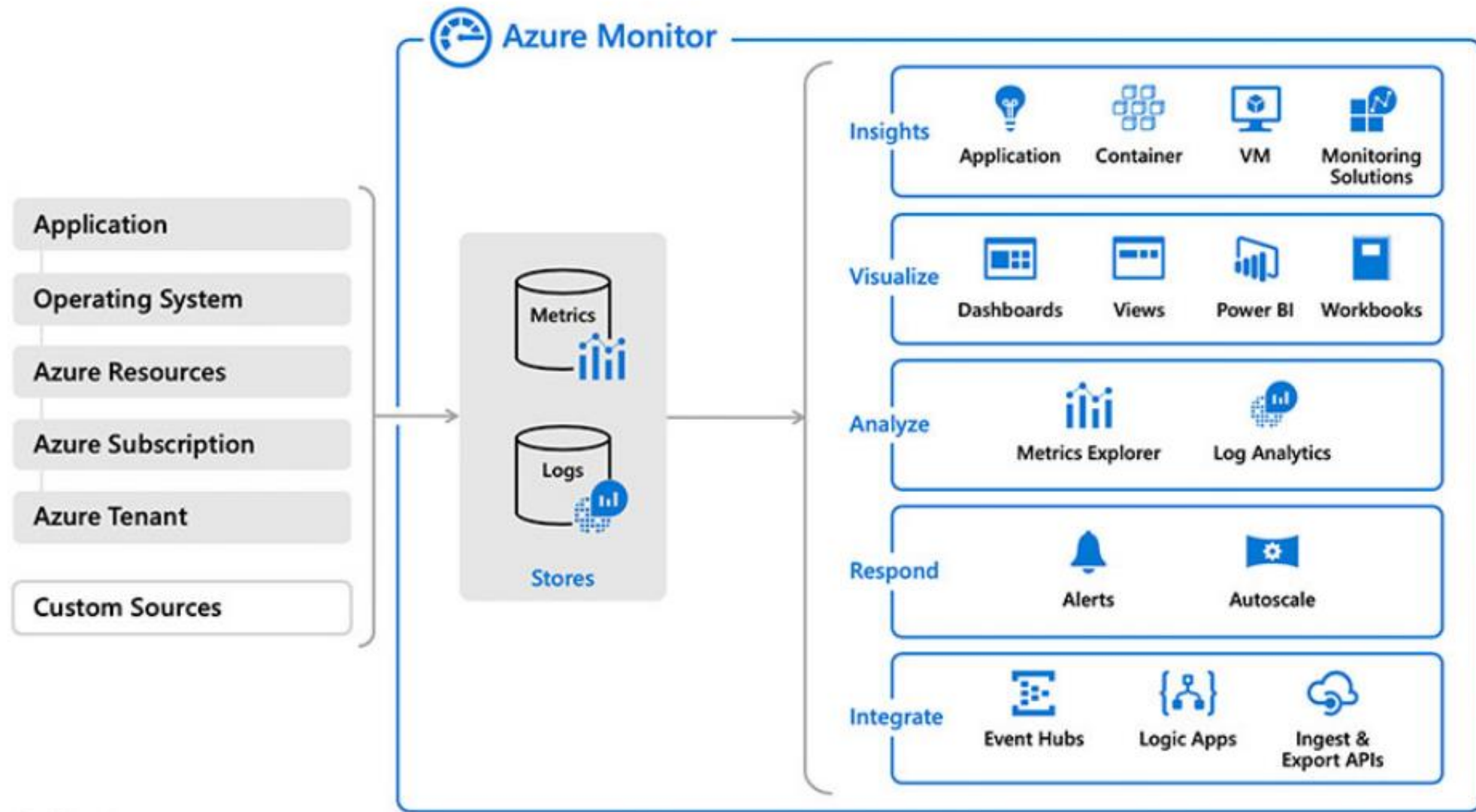


Kusto - Azure Monitor Log Queries

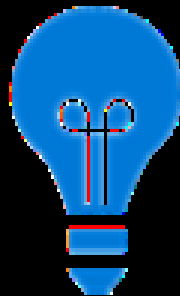
Taioab Ali





WHERE TO USE KQL

- **Azure Log Analytics**
- **Azure Application Insights**
- **Windows Defender**
- **Advanced Threat Protection**
- **Azure Security Center**



Not another one, can I use tsql?

- Azure Monitor – NO
- Azure Data Explorer - YES

While [SQL queries](#) to Kusto are supported, the primary means of interaction with Kusto is through the use of the [Kusto query language](#) to send data queries, and through the use of [control commands](#) to manage Kusto entities, discover metadata, etc.

How can I learn?

Check the reference slide

Demo environment

- <https://aka.ms/LADemo>
- <https://aka.ms/AIAnalyticsDemo>
- <https://aka.ms/WidDevATP>

Reference

- [Azure Monitor overview](#)
- [Pluralsight course 'Kusto Query Language \(KQL\) from Scratch](#) by Robert Cain
- [Get started with log queries in Azure Monitor](#)
- [Common Query Samples](#)
- [Write queries for Azure Data Explorer](#)
- [SQL to Azure Monitor log query cheat sheet](#)
- [SQL to Analytics Language cheat sheet](#)
- [Azure AD Log Analytics KQL queries via API with PowerShell](#)
- [Operations Management Suite 101: Log Analytics Queries 101](#)
- [Log Analytics Advanced Queries](#) by Marc Kean





@SqlWorldWide



linkedin.com/in/taiojali



sqlworldwide.com



taioa@sqlworldwide.com

Work

- Microsoft MVP – Data Platform
- 13 years as DBA
- MCSE Data Management and Analytics

Outside Work

- Running—One 26.2 and Many 13.1
- Shuttling 3 kids

Giving Back

- Organizer @SqlSaturdayBoston and Co-organizer NESQL UG
- Frequent speaker local user groups, SQL Saturdays & Virtual groups
- Answering questions at #sqlhelp & dba.stackexchange
- Blog at sqlworldwide.com

