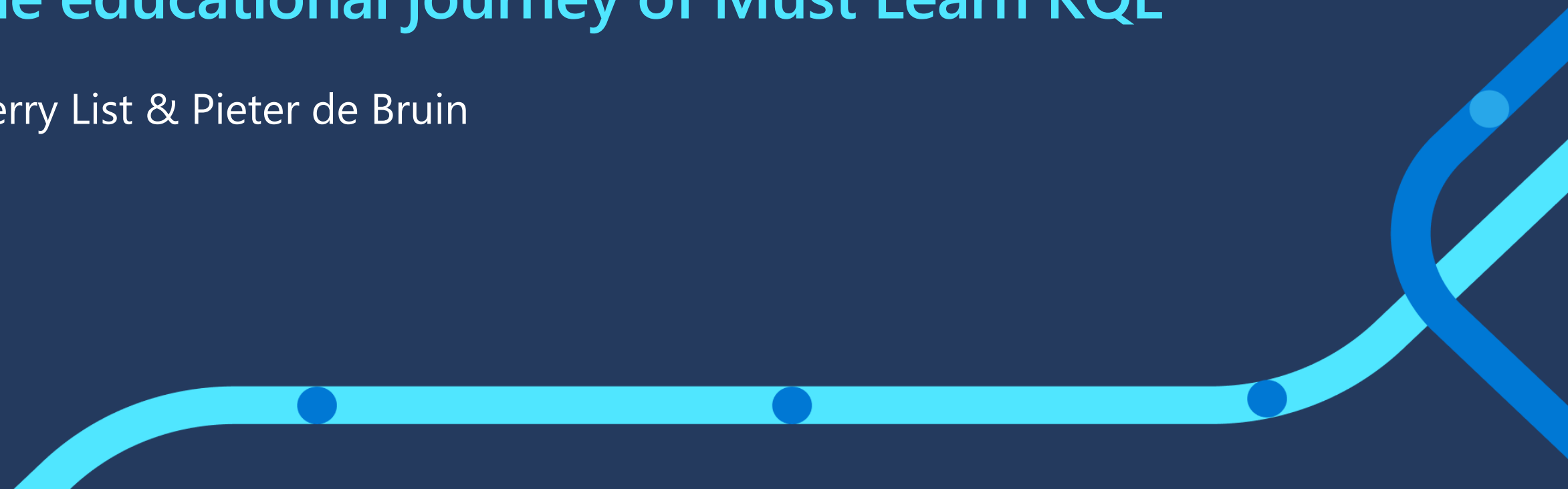
Microsoft

DEVELOPER RELATIONS | CONTENT & LEARNING

From enthusiast to authority: The educational journey of Must Learn KQL

Sherry List & Pieter de Bruin



Hello

Sherry List

Senior Program Manager, Microsoft

@sherrrylst

Pieterd de Bruin

Senior Program Manager, Microsoft

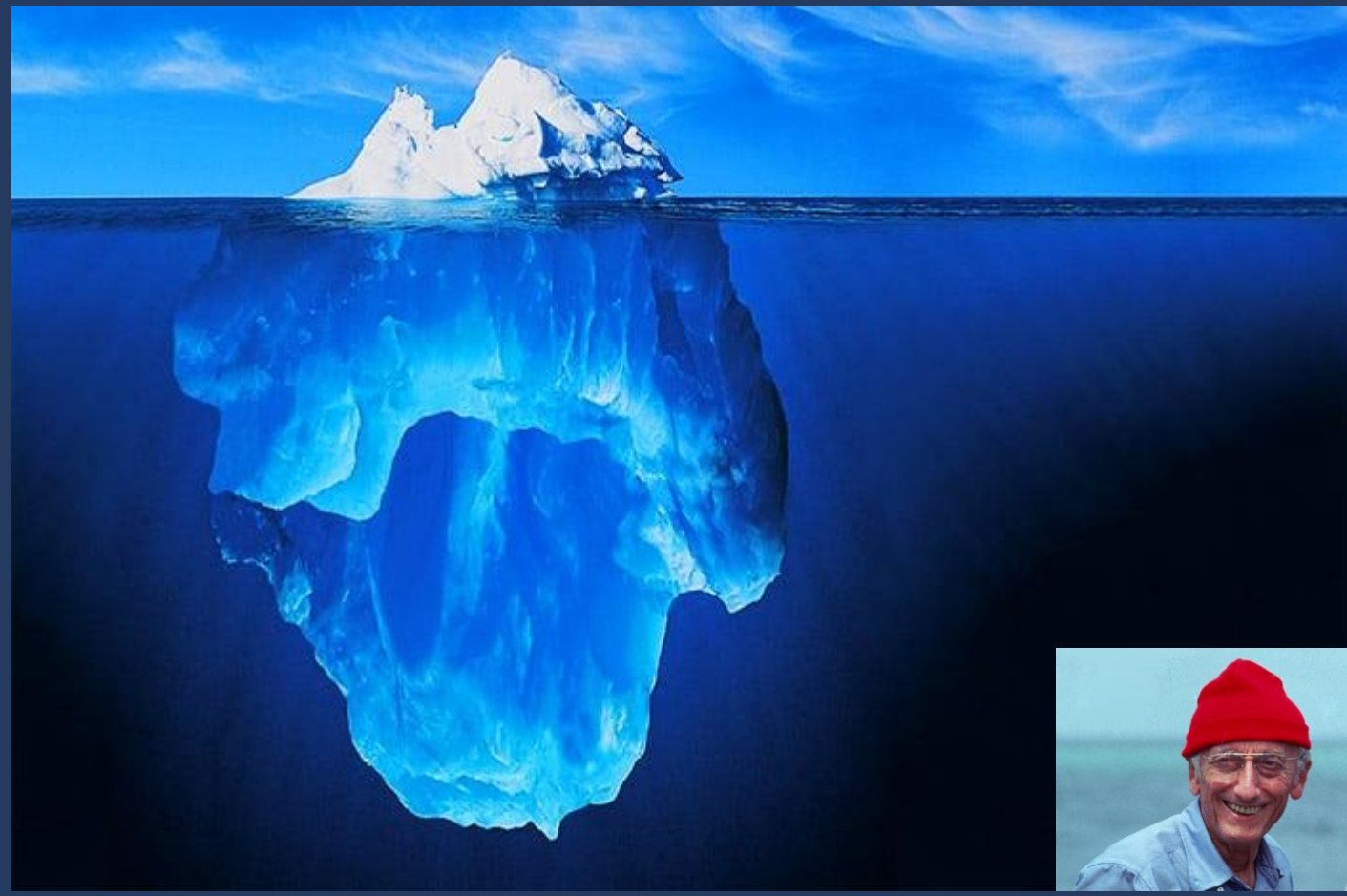
@pieter_de_bruin

Agenda

- What is Kusto Query Language?
- Where to use it?
- Storytime: MustLearnKQL
- Questions & answers

Why Kusto Query Language?

- High volume/velocity/variance data +
- queryable +
- managed +
- optimized +
- interactive ad-hoc queries



Where KQL is used

- Data Explorer
- Resource graph
- Log Analytics / Monitor
- Sentinel, Defender, etc

Collect

Detect

Analytics

Hunting

Intelligence

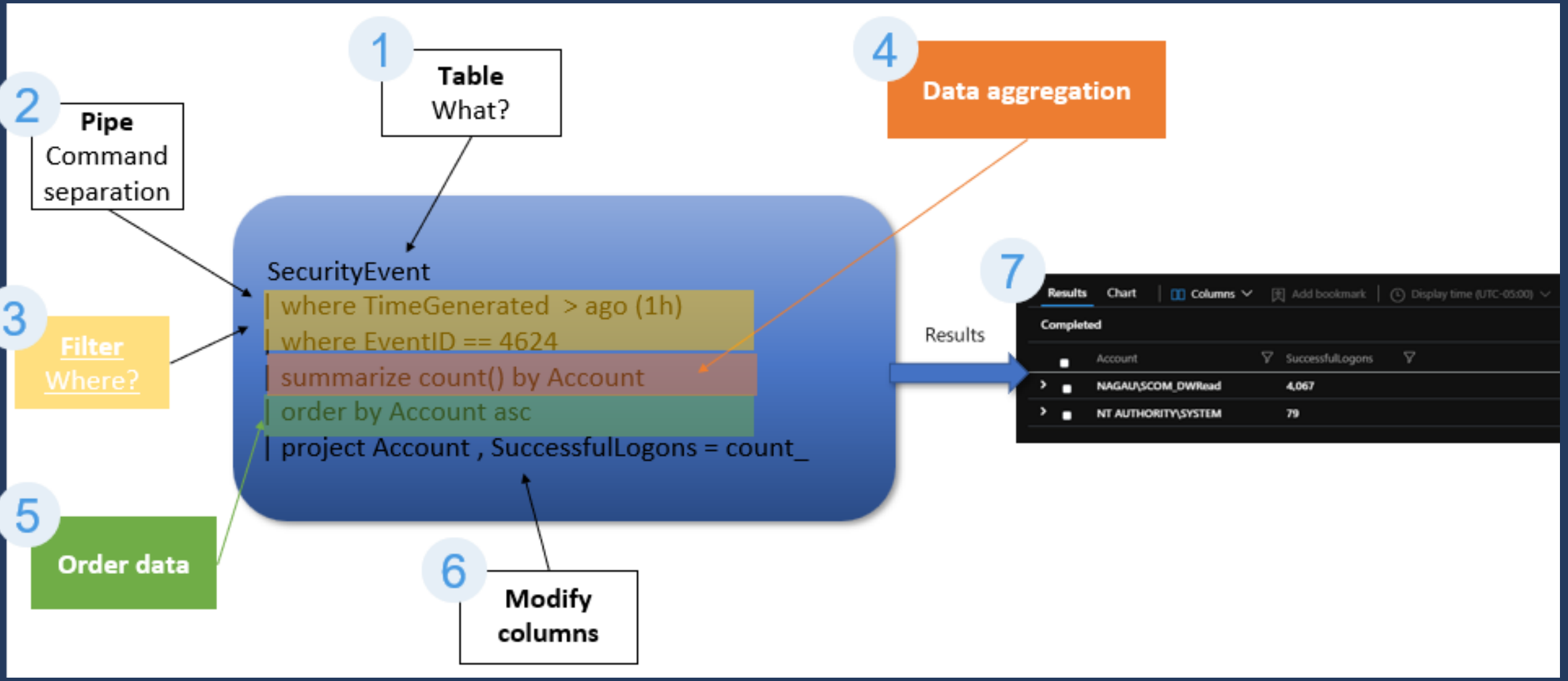
Investigate

Incidents

Respond

Automation

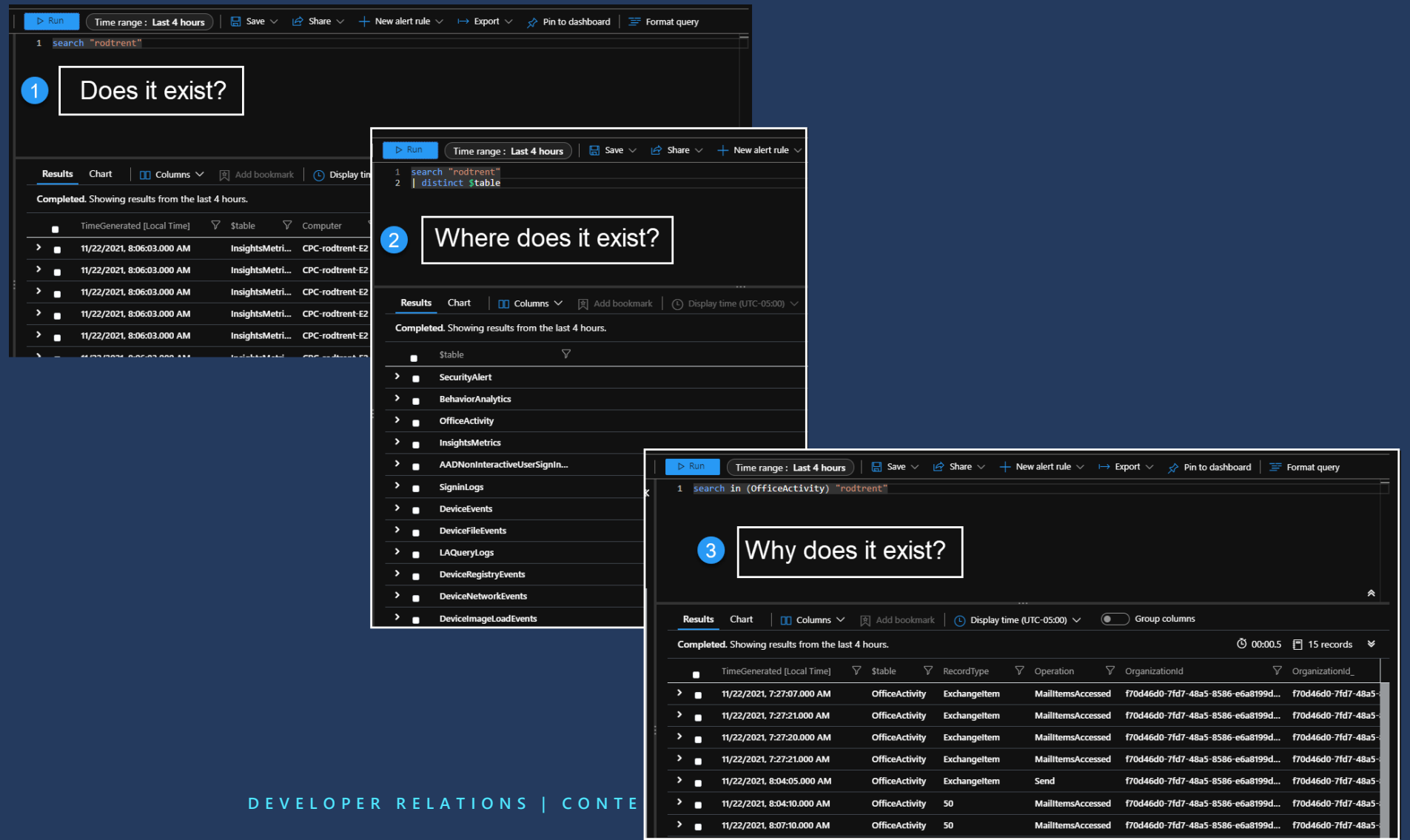
How KQL works



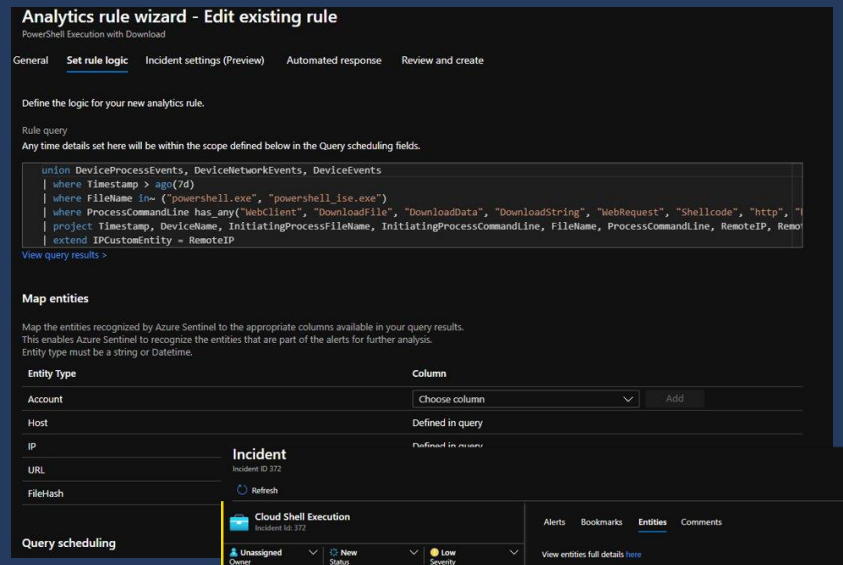
What did you just learn?

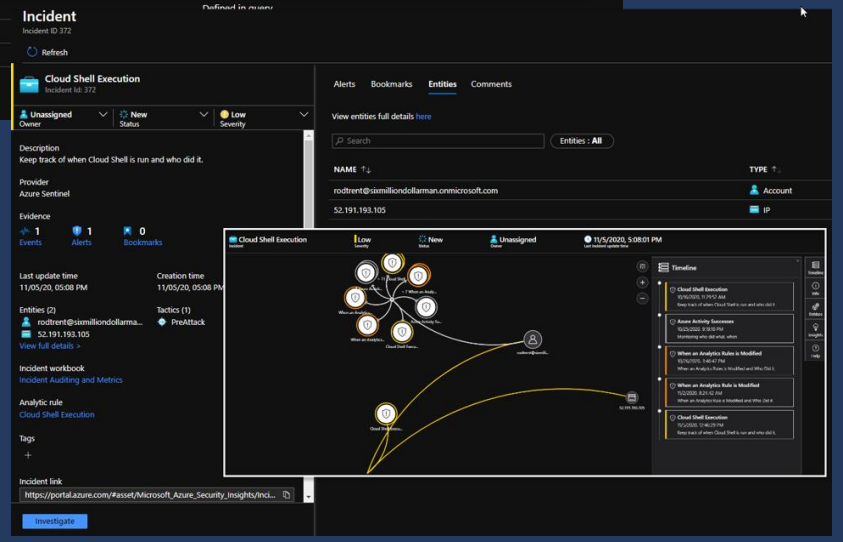
- Where
- Take/limit - returns a specific number of arbitrary rows
- Count,
- Summarize
- Render
- Distinct
- Extend
- Project
- Sort/order
- Let
- Union
- Join

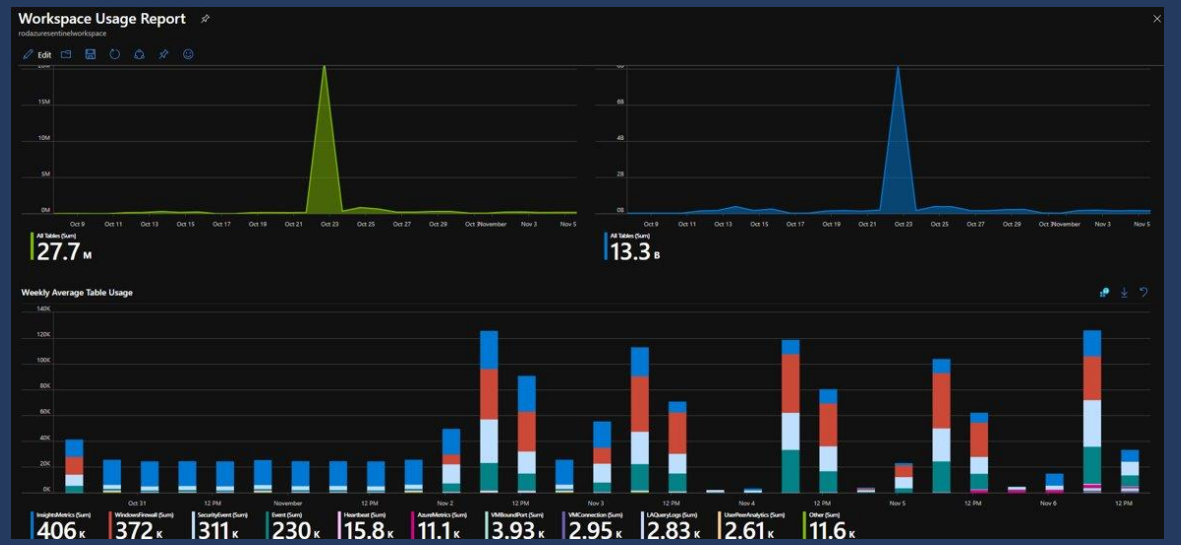
Querying on steroids

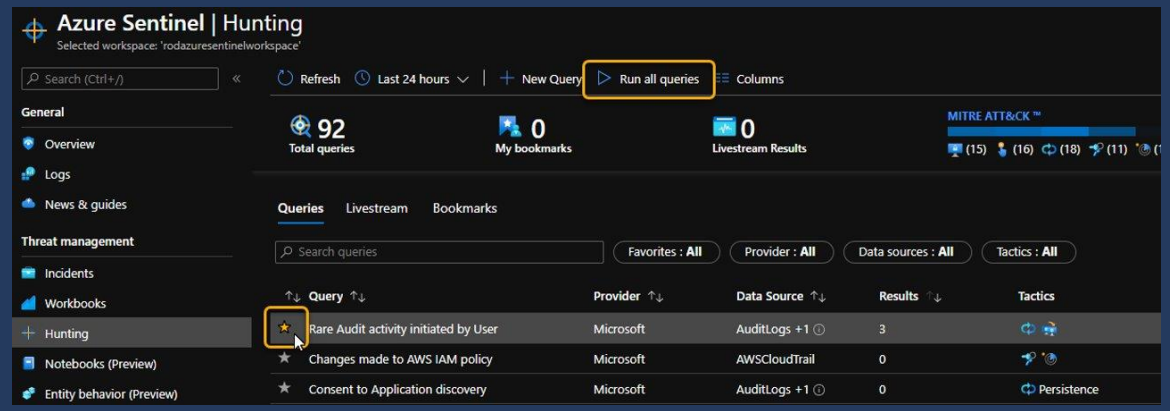


KQL at the core of Sentinel









Story time:

Must Learn KQL

http://aka.ms/MustLearnKQL

Microsoft Security

Rod Trent

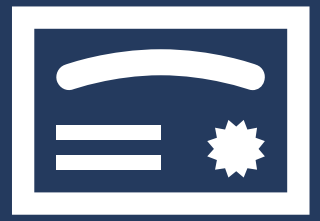
Cloud Security Advocate @ Microsoft

@rodtrent

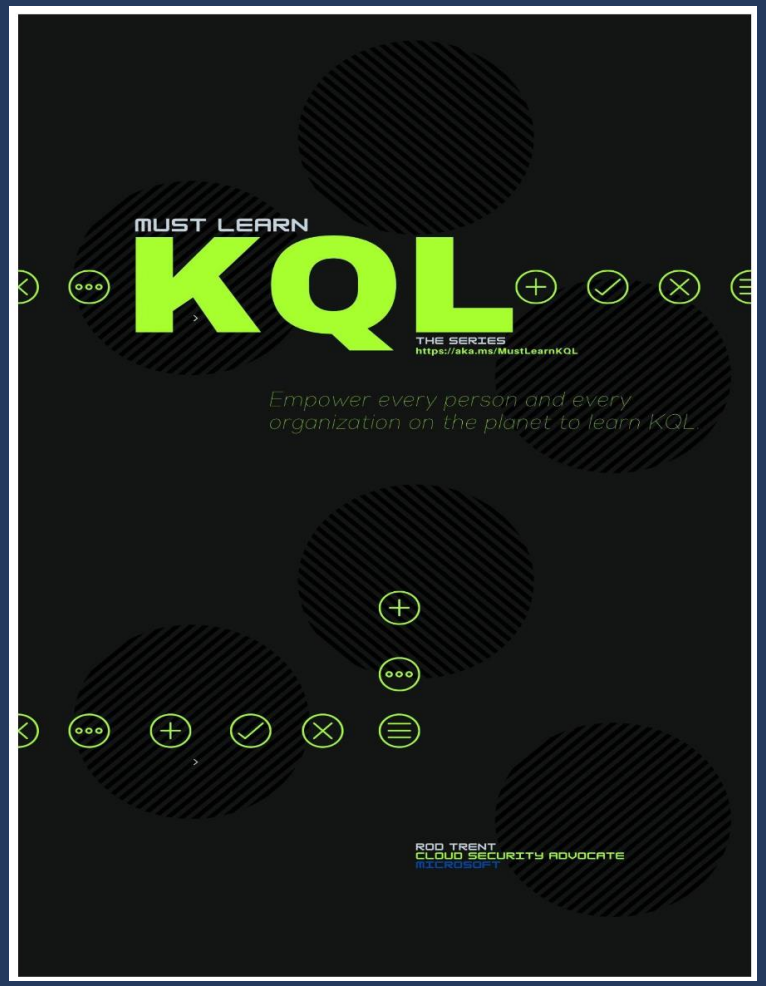
https://www.linkedin.com/in/rodtrent/

aka.ms/RodsBlog

MustLearnKQL



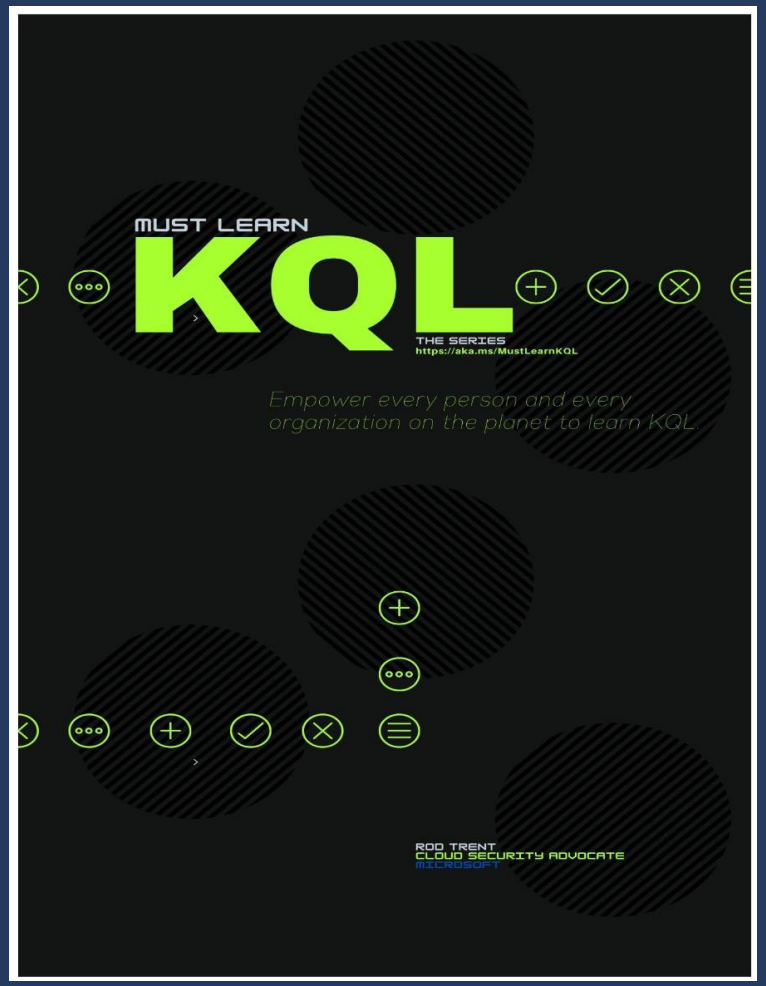
e-book



Free e-book

https://cda.ms/4rg

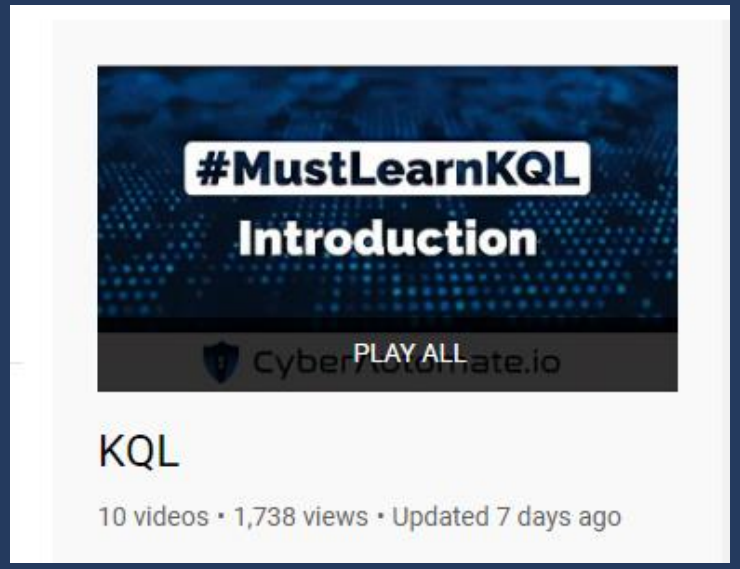
Book



Book

https://cda.ms/4rg

Video



YouTube Channel

https://cda.ms/3Jx

Must Learn KQL Community!

- #mustlearnkql on Instagram & TikTok
- Merch Store: https://cda.ms/3Dy

  (Love the series so much you want a coffee mug? There's now a merch store where all proceeds go to St. Jude Children's Research Hospital.)
- Weekly Tweets

From Must Learn KQL Community

"Super fun series and easy to follow explanations. Thank you for this!"

"I am happy to say I just passed the Must Learn KQL assessment with an 80% score. The book was a lot of fun and I am already going through the Advanced KQL-series as well."

"I stumbled across your MustLearnKQL blog just yesterday night and I got addicted to it right from the first instance. So, I read all parts today and made the test. "

"I hope you are well. I would like to thank you for creating such a great KQL learning series. "

Stats

- 11,000 unique and returning visitors
- Assessments taken: Over 3,000
- Certificates: 1,009
- GitHub traffic(Avg per week): 2,000 visitors/980 unique
- GitHub Fork: 61 times

Why this story?

- Be proactive
- Share your opinion
- Grow through the community

Q&A

Thank you