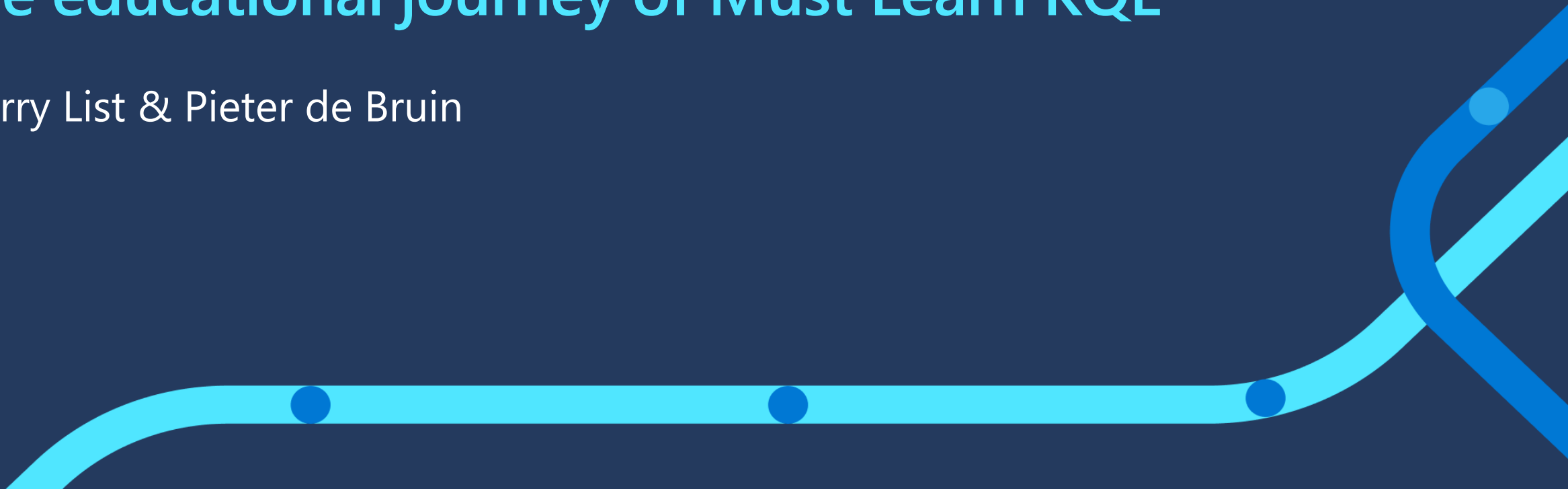




DEVELOPER RELATIONS | CONTENT & LEARNING

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

Sherry List & Pieter de Bruin



Hello



Sherry List

Senior Program Manager, Microsoft



@sherrylst



Pieterd de Bruin

Senior Program Manager, Microsoft



@pieter_de_bruin

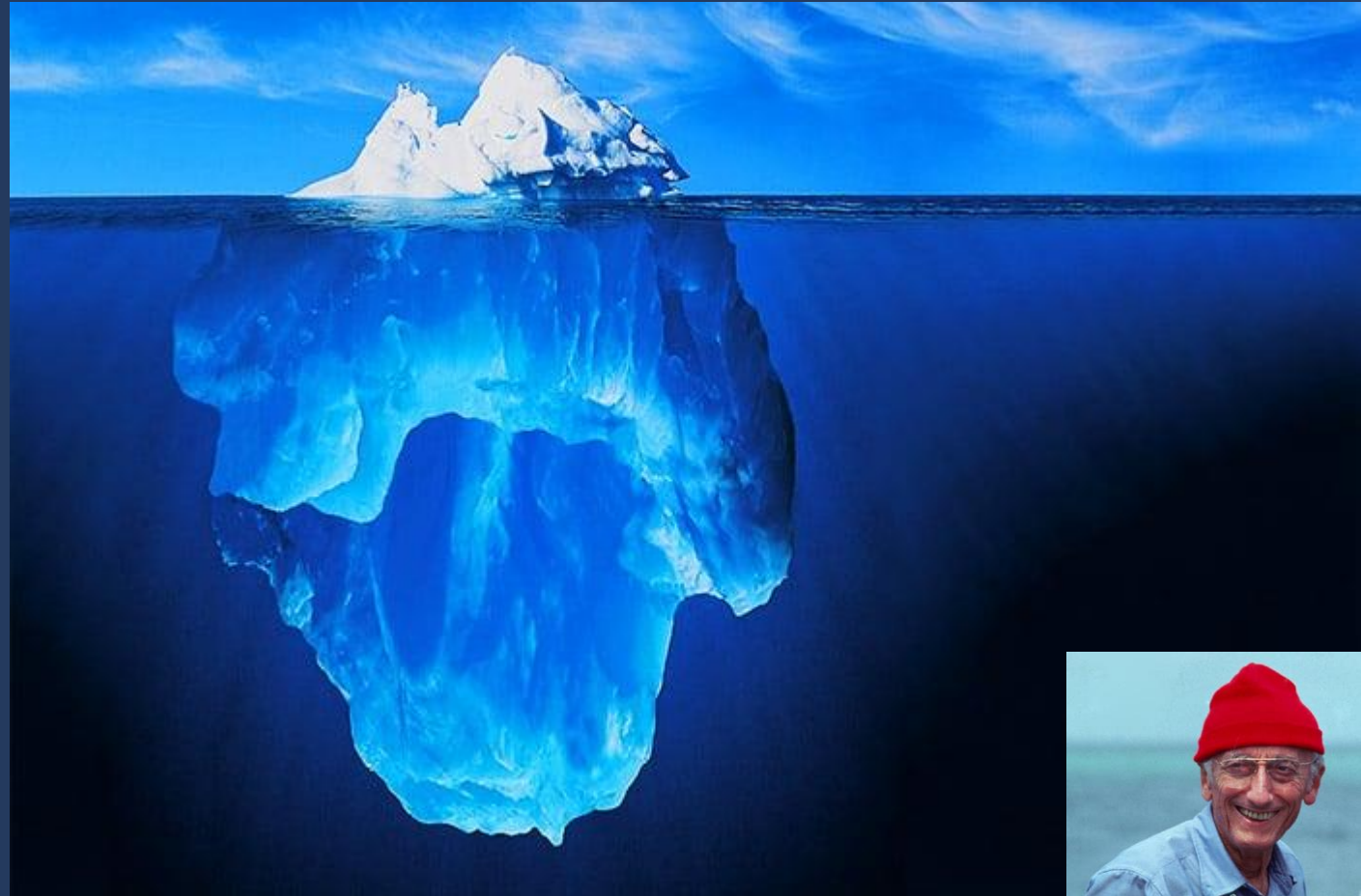
Agenda



- 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



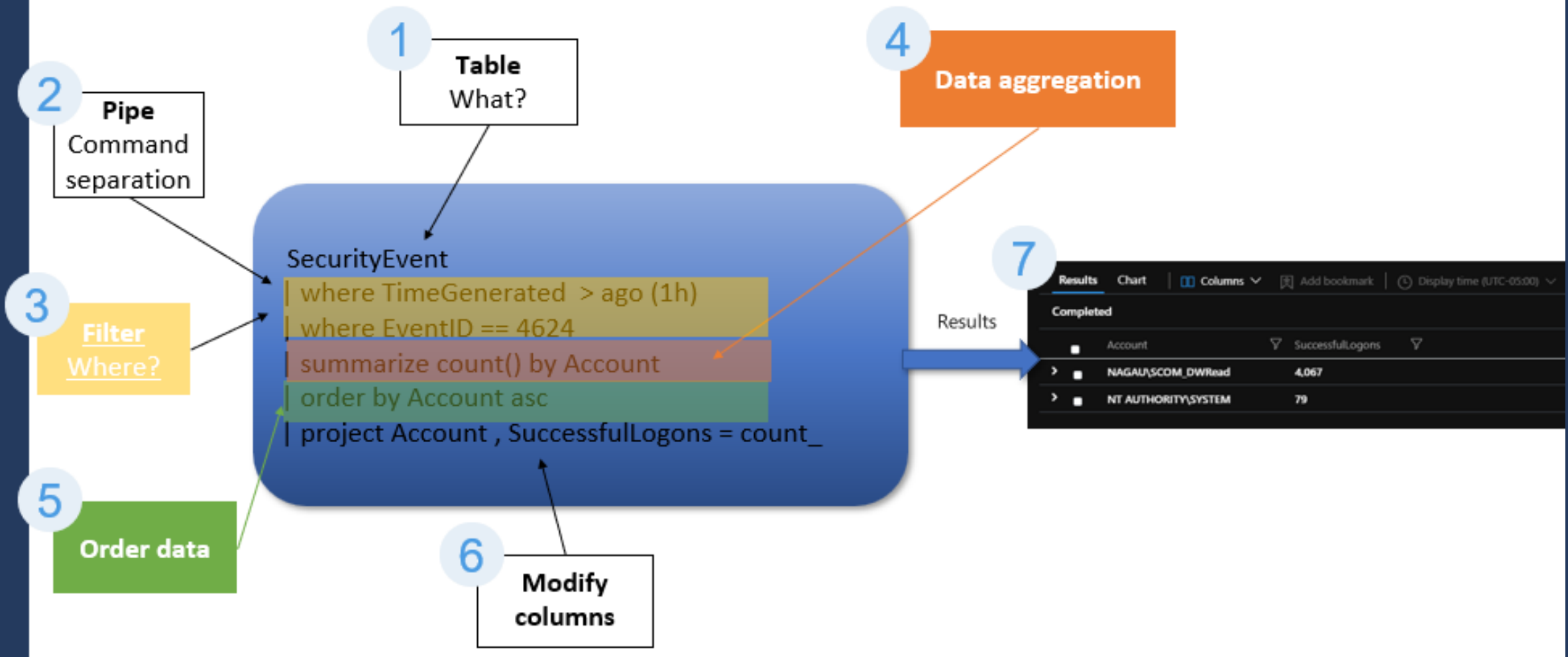
Incidents

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

1 Does it exist?

Run Time range: Last 4 hours Save Share + New alert rule Export Pin to dashboard Format query

1 search "rodtrent"

Results Chart Columns Add bookmark Display time

Completed. Showing results from the last 4 hours.

TimeGenerated [Local Time]	Stable	Computer
11/22/2021, 8:06:03.000 AM	InsightsMetri...	CPC-rodtrent-E2
11/22/2021, 8:06:03.000 AM	InsightsMetri...	CPC-rodtrent-E2
11/22/2021, 8:06:03.000 AM	InsightsMetri...	CPC-rodtrent-E2
11/22/2021, 8:06:03.000 AM	InsightsMetri...	CPC-rodtrent-E2
11/22/2021, 8:06:03.000 AM	InsightsMetri...	CPC-rodtrent-E2

2 Where does it exist?

Run Time range: Last 4 hours Save Share + New alert rule

1 search "rodtrent"
2 distinct \$table

Results Chart Columns Add bookmark Display time (UTC-05:00)

Completed. Showing results from the last 4 hours.

Stable
SecurityAlert
BehaviorAnalytics
OfficeActivity
InsightsMetrics
AADNonInteractiveUserSignin...
SigninLogs
DeviceEvents
DeviceFileEvents
LAQueryLogs
DeviceRegistryEvents
DeviceNetworkEvents
DeviceImageLoadEvents

3 Why does it exist?

Run Time range: Last 4 hours Save Share + New alert rule Export Pin to dashboard Format query

1 search in (OfficeActivity) "rodtrent"

Results Chart Columns Add bookmark Display time (UTC-05:00) Group columns

Completed. Showing results from the last 4 hours. 00:00.5 15 records

TimeGenerated [Local Time]	Stable	RecordType	Operation	OrganizationId	OrganizationId_
11/22/2021, 7:27:07.000 AM	OfficeActivity	ExchangeItem	MailItemsAccessed	f70d46d0-7fd7-48a5-8586-e6a8199d...	f70d46d0-7fd7-48a5-
11/22/2021, 7:27:21.000 AM	OfficeActivity	ExchangeItem	MailItemsAccessed	f70d46d0-7fd7-48a5-8586-e6a8199d...	f70d46d0-7fd7-48a5-
11/22/2021, 7:27:20.000 AM	OfficeActivity	ExchangeItem	MailItemsAccessed	f70d46d0-7fd7-48a5-8586-e6a8199d...	f70d46d0-7fd7-48a5-
11/22/2021, 7:27:21.000 AM	OfficeActivity	ExchangeItem	MailItemsAccessed	f70d46d0-7fd7-48a5-8586-e6a8199d...	f70d46d0-7fd7-48a5-
11/22/2021, 8:04:05.000 AM	OfficeActivity	ExchangeItem	Send	f70d46d0-7fd7-48a5-8586-e6a8199d...	f70d46d0-7fd7-48a5-
11/22/2021, 8:04:10.000 AM	OfficeActivity	50	MailItemsAccessed	f70d46d0-7fd7-48a5-8586-e6a8199d...	f70d46d0-7fd7-48a5-
11/22/2021, 8:07:10.000 AM	OfficeActivity	50	MailItemsAccessed	f70d46d0-7fd7-48a5-8586-e6a8199d...	f70d46d0-7fd7-48a5-

KQL at the core of Sentinel

Analytics rule wizard - Edit existing rule

PowerShell Execution with Download

General **Set rule logic** Incident settings (Preview) Automated response Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
union DeviceProcessEvents, DeviceNetworkEvents, DeviceEvents
| where Timestamp > ago(7d)
| where FileName in~ ("powershell.exe", "powershell_ise.exe")
| where ProcessCommandLine has_any("WebClient", "DownloadFile", "DownloadData", "DownloadString", "WebRequest", "Shellcode", "http", "I")
| project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine, FileName, ProcessCommandLine, RemoteIP, RemoteIPCustomEntity - RemoteIP
View query results >
```

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string or Datetime.

Entity Type	Column
Account	Choose column <input type="button" value="Add"/>
Host	Defined in query
IP	Defined in query
URL	
FileHash	

Incident

Incident ID: 372

Cloud Shell Execution

Incident ID: 372

Description: Keep track of when Cloud Shell is run and who did it.

Provider: Azure Sentinel

Evidence: 1 Events, 1 Alerts, 0 Bookmarks

Last update time: 11/05/20, 05:08 PM

Creation time: 11/05/20, 05:08 PM

Entities (2): rodtrent@simillondollama..., 52.191.193.105

Incident workbook: Incident Auditing and Metrics

Analytic rule: Cloud Shell Execution

Tags: +

Incident link: https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Inc...

Cloud Shell Execution

Low severity

Timeline

- Cloud Shell Execution: 11/05/20, 05:08 PM
- When an Analytics Rule is Modified: 11/05/20, 05:08 PM
- When an Analytics Rule is Modified: 11/05/20, 05:08 PM
- Cloud Shell Execution: 11/05/20, 05:08 PM

Entity details

NAME: 1

Provider: rodtrent@simillondollama.onmicrosoft.com

Account: rodtrent@simillondollama.onmicrosoft.com

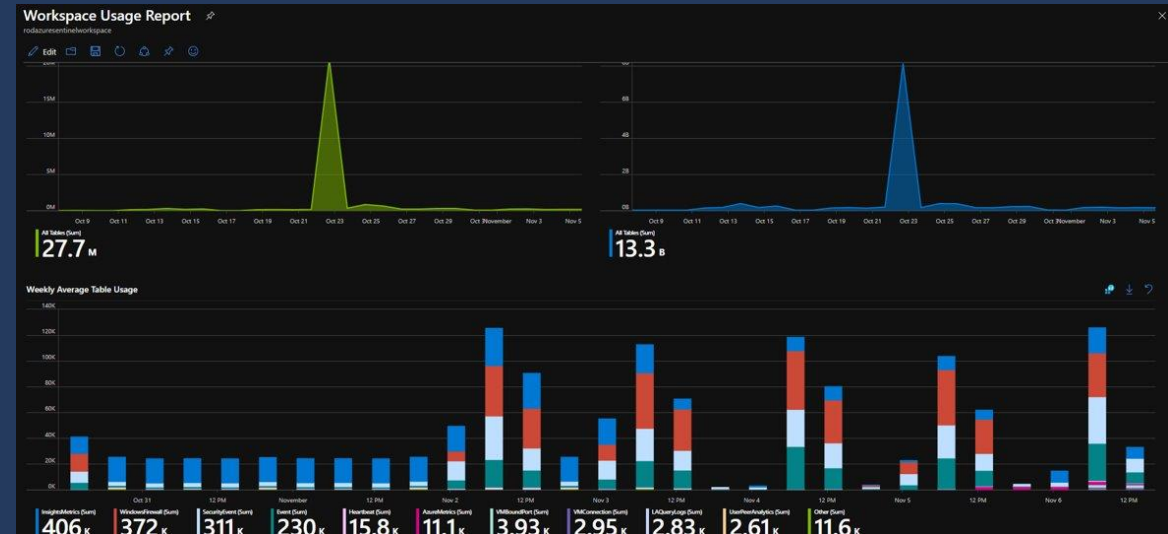
IP: 52.191.193.105

Cloud Shell Execution

Low severity

Timeline

- Cloud Shell Execution: 11/05/20, 05:08 PM
- When an Analytics Rule is Modified: 11/05/20, 05:08 PM
- When an Analytics Rule is Modified: 11/05/20, 05:08 PM
- Cloud Shell Execution: 11/05/20, 05:08 PM



Azure Sentinel | Hunting

Selected workspace: 'rodazuresentinelworkspace'

Search (Ctrl+/) Refresh Last 24 hours New Query Run all queries Columns

General

- Overview
- Logs
- News & guides
- Threat management
- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior (Preview)

92 Total queries

0 My bookmarks

0 Livestream Results

MITRE ATT&CK™

Queries Livestream Bookmarks

Search queries Favorites: All Provider: All Data sources: All Tactics: All

Query	Provider	Data Source	Results	Tactics
Rare Audit activity initiated by User	Microsoft	AuditLogs +1	3	Persistence
Changes made to AWS IAM policy	Microsoft	AWSCloudTrail	0	Persistence
Consent to Application discovery	Microsoft	AuditLogs +1	0	Persistence

Story time:

Must Learn KQL

<http://aka.ms/MustLearnKQL>





Rod Trent

Cloud Security Advocate @ Microsoft



@rodtrent



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

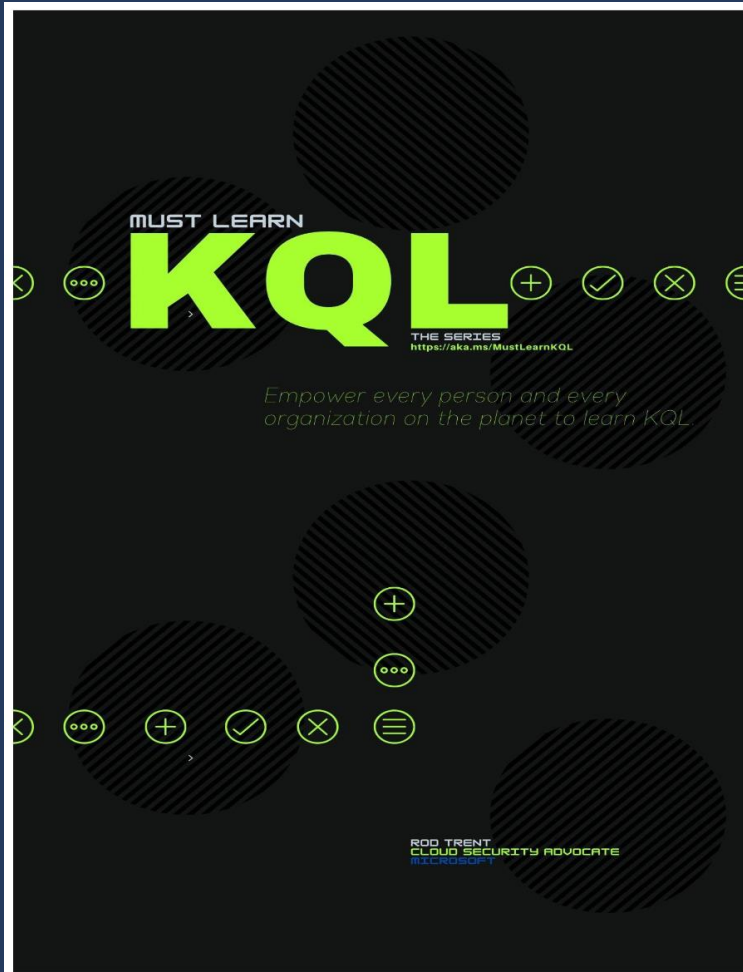


aka.ms/RodsBlog

MustLearnKQL



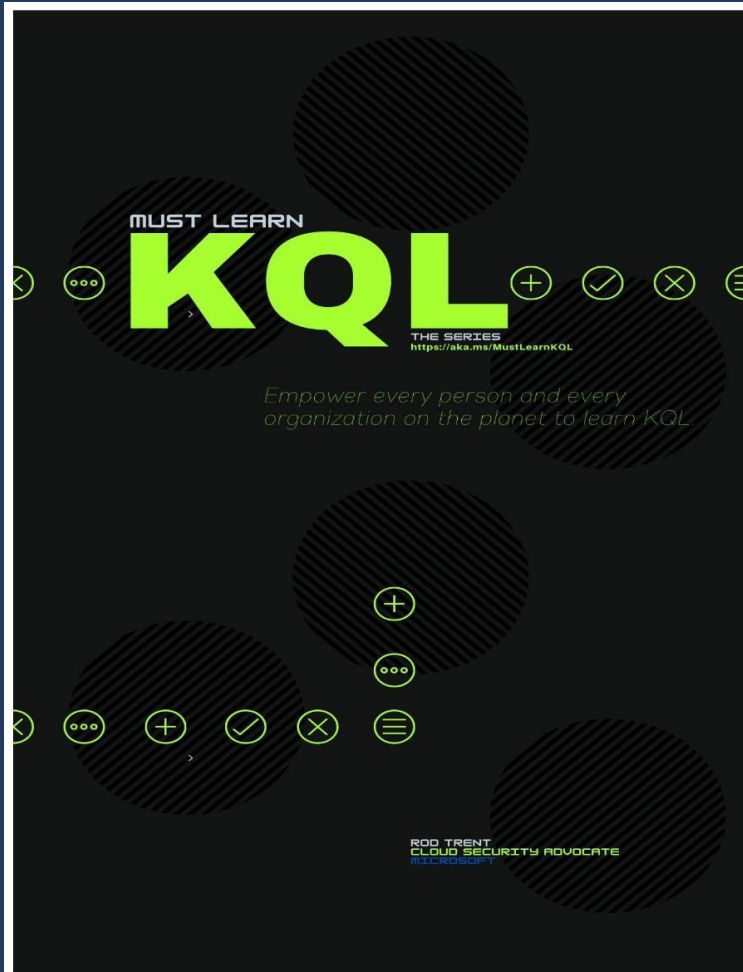
e-book



Free e-book

<https://cda.ms/4rg>

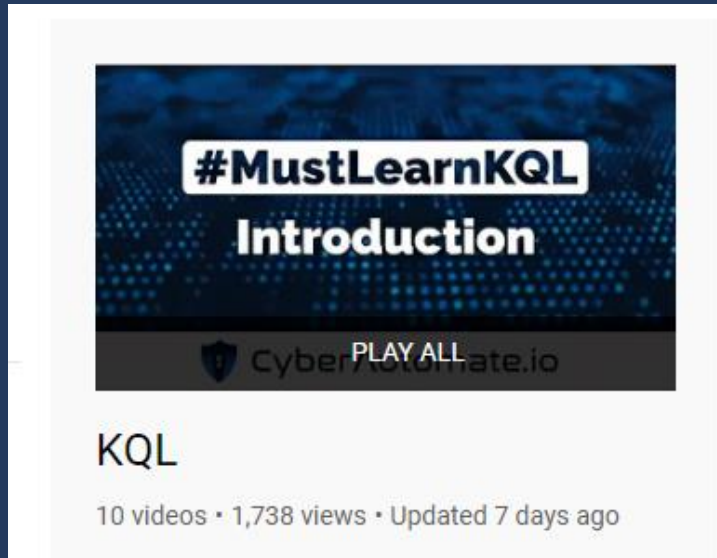
Book



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

