Mastering KQL

A Guide for Endpoint Admins

Sorry Who Are You?

David Brook
Microsoft MVP · Endpoint & Security

Role
Director, CEO, CFO, Tea Maker, Chaos Monkey, Dogs Body… The lot really.

Focus
Intune · Security · Automation · Identity

Blog, Hobbies and more
euc365.com
davidbrookcxp
DBBrook24

Sorry Who Are You?

Maurice Daly
Microsoft MVP · Endpoint & Security

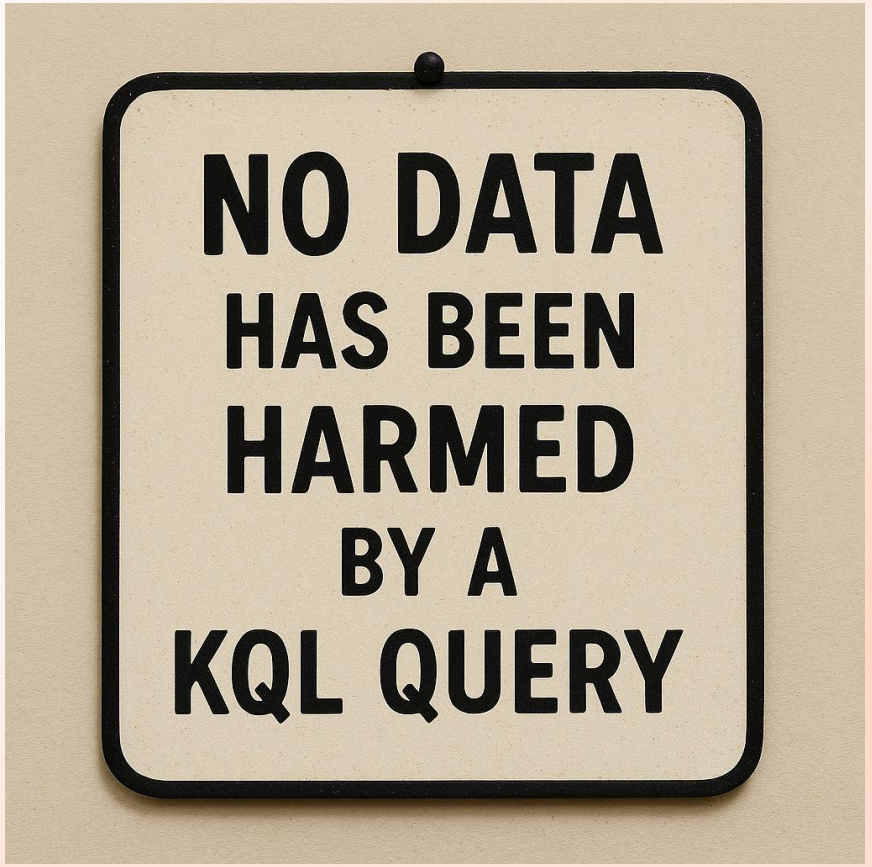
Role
Microsoft MVP, Senior Security Architect

Focus
Vibe Coding....

Blog, Hobbies and more
msendpointmgr.com
mauricedaly
modaly_it

What is Kusto Query Language (KQL)?

- Simple & powerful language to query structured, semi-structured, and unstructured data
  - Read-only
- Used in many places
  - Log Analytics
  - Microsoft Defender for Endpoint (MDE)
  - ConfigMgr CMPivot
  - Intune Single Device Query/Multi device query
  - Sentinel
- Different implementations
  - Minor differences
- “KQL is the new PowerShell” - Rod Trent



KQL IS EASY!!

But hold the line caller!...

Do you have any of these?

ConfigMgr

Intune

Microsoft
Defender for Endpoint

Log analytics

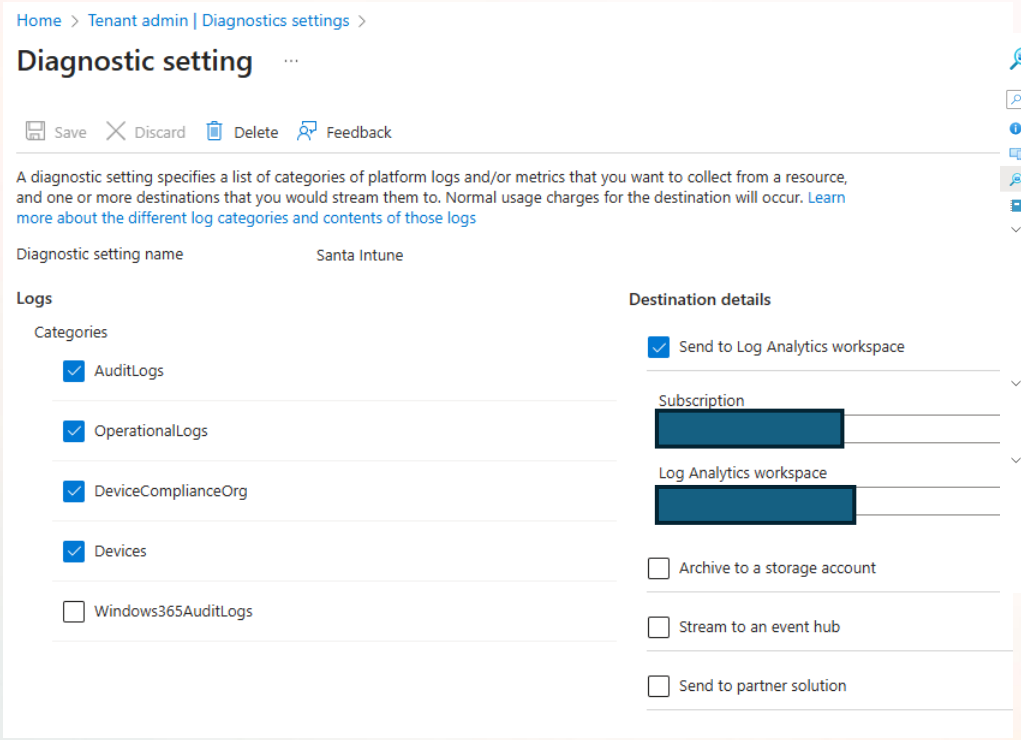
Intune Device Query

Windows Update
for Business Reports

Implementing KQL datasets for device management

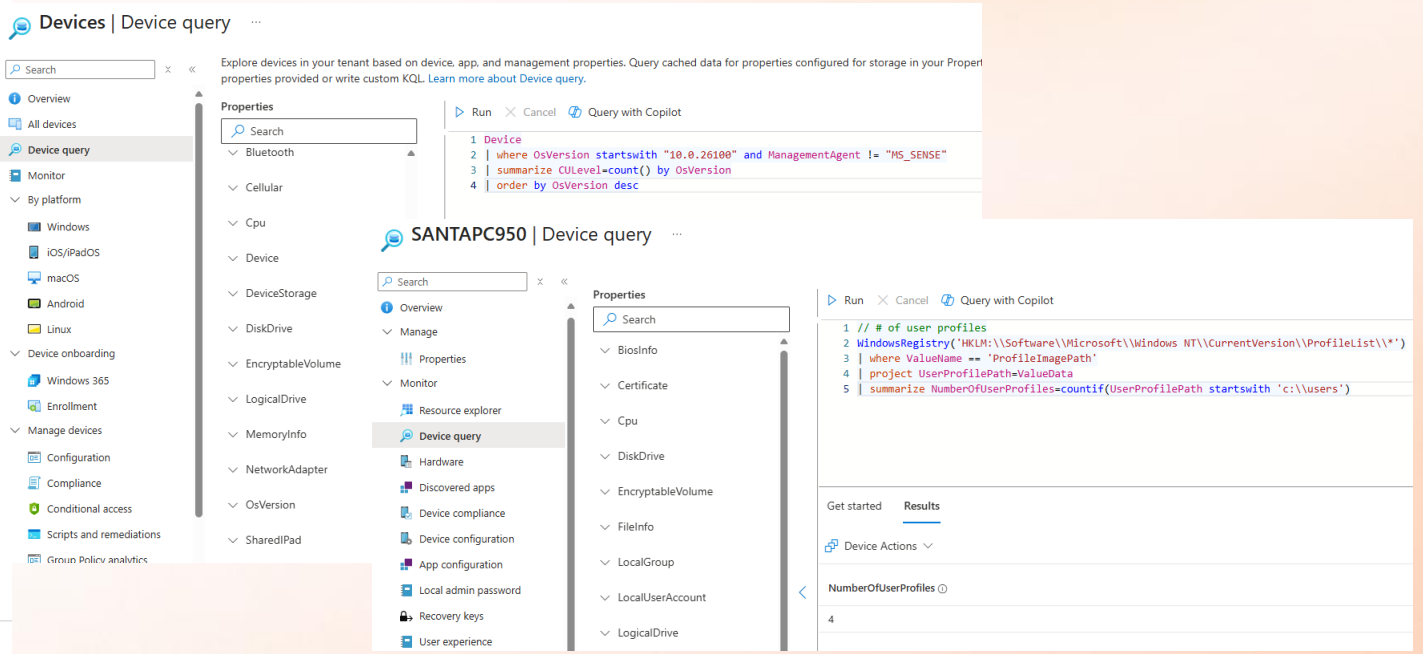
Intune: multiple places where you can utilize KQL

1. Import data to Log analytics



*Requires a Log analytics workspace

2. Intune Suite's Advanced analytics



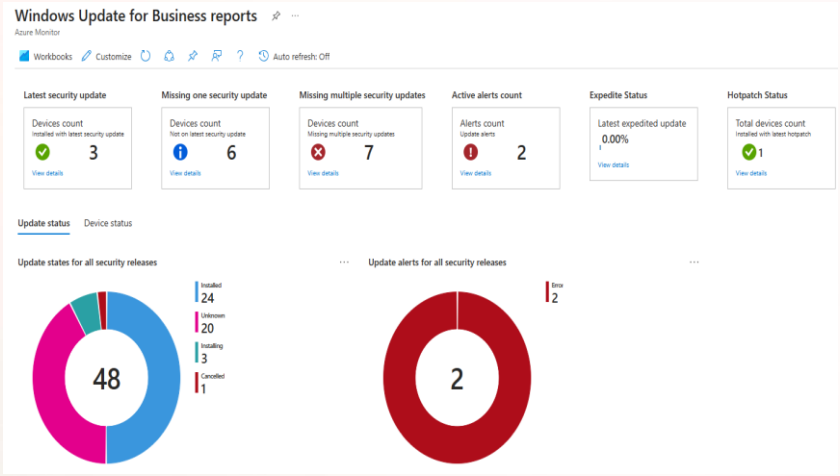
Multi-device query
- Based on enhanced inventory info

Single-device query

NOTE: Not all KQL commands supported!

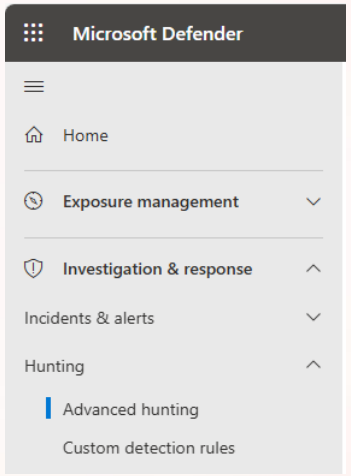
Implementing KQL datasets for device management

Windows Update for Business reports



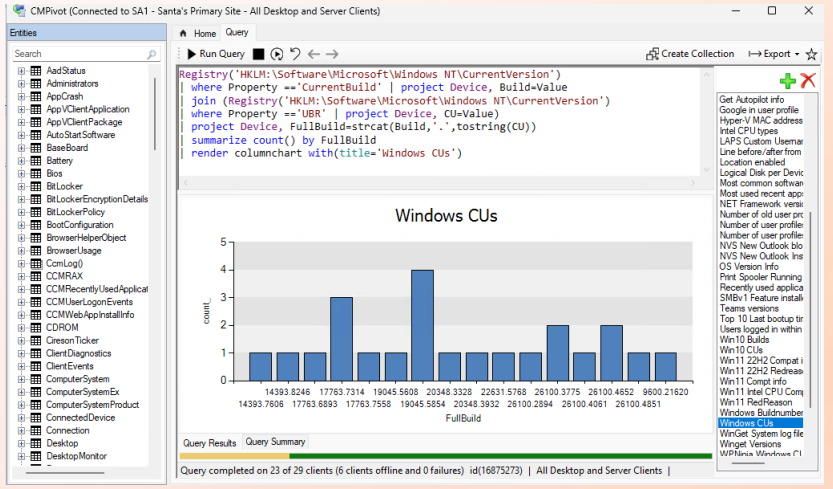
1. Requires a Log analytics workspace
2. Enable WUfB Reports: https://aka.ms/wufbreports

Microsoft Defender for Endpoint



Built-in

ConfigMgr: CMPivot



Built-in

Where do you start?

You need to know your datasets/schemas!

1. Where do you find the information you are looking for?

2. What information different entities/tables contain?

3. What is the datatype (string/integer/datetime/dynamic)?

KQL Result Set

Picture a CSV in the cloud!

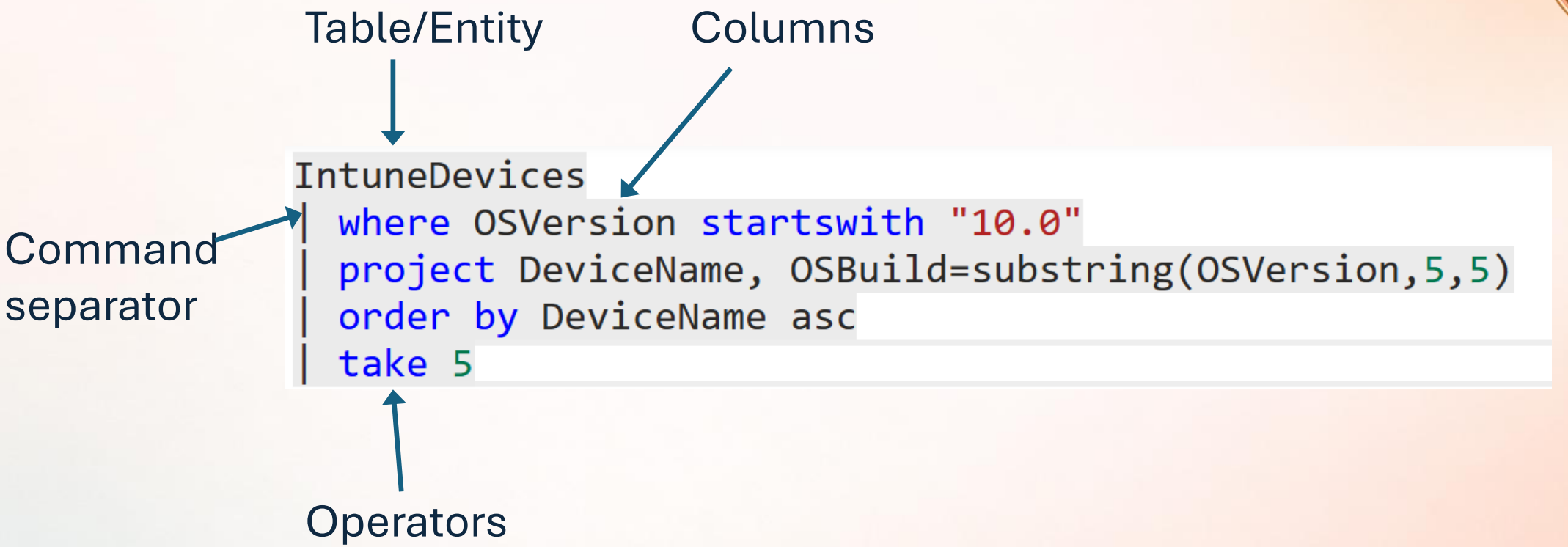
TimeDate	Name	UPN	UBR	DeviceID	Enabled	Info
3/4/2025, 4:04:17.871 AM	PC123	tpsreports@foobar.com	3014	d1408951-d99b-48f4-8c51-f01be2	True	{"Date":"3/4/2025 6:52:28AM","Result":1,"Type":3,"Actor":{"AppId":"5926-34e-4f-8bed-58a4","AppName":"Intune portal","Name":null,"UPN":“tpsreports@foobar.com"},"TargetIds":["6a7e38e5b-f1ce46b8d"],"Targets":[{"ModifiedProperties":[{"Name":"GroupTarget","Old":null,"New":"14f0733a-8b62-8"}],"Name":"Enable hotpatch"}]}

Different data types

Add new columns

Multiple rows…

KQL Basics

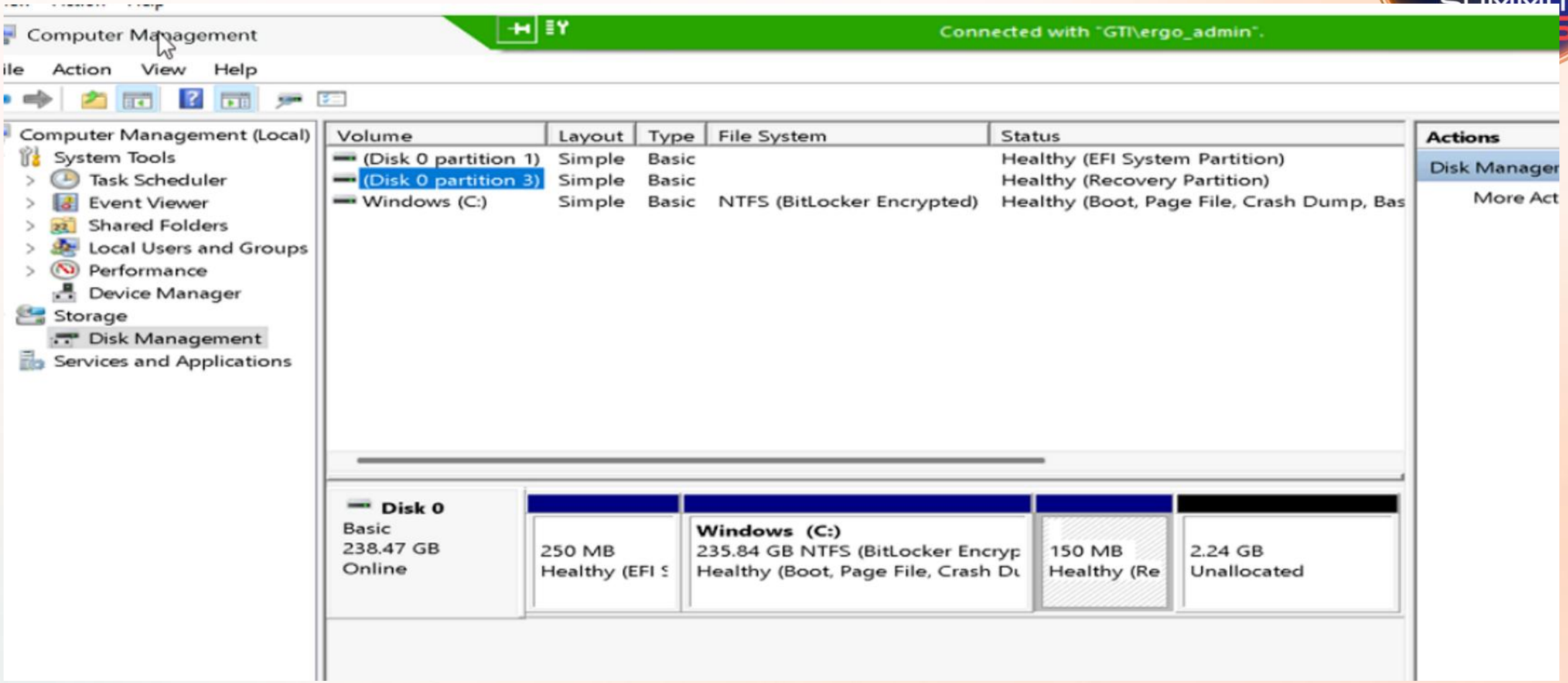

Table/Entity
Columns
IntuneDevices
| where OSVersion startswith "10.0"
| project DeviceName, OSBuild=substring(OSVersion,5,5)
| order by DeviceName asc
| take 5
Command separator
Operators

My first KQL queries

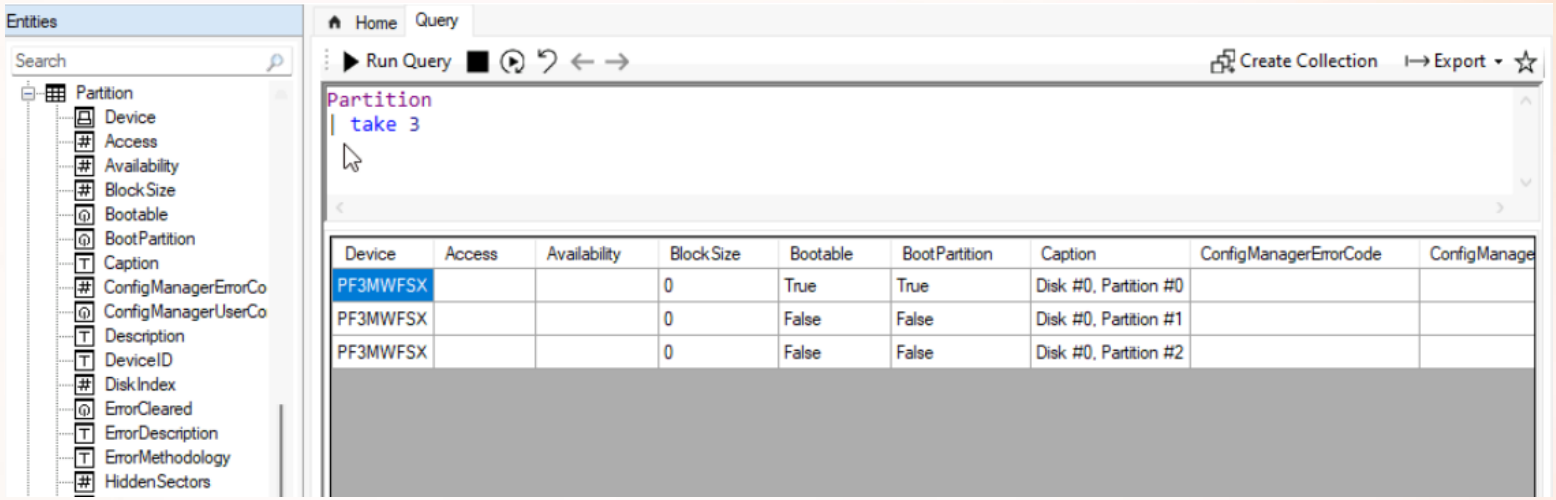
Most Common KQL Operators

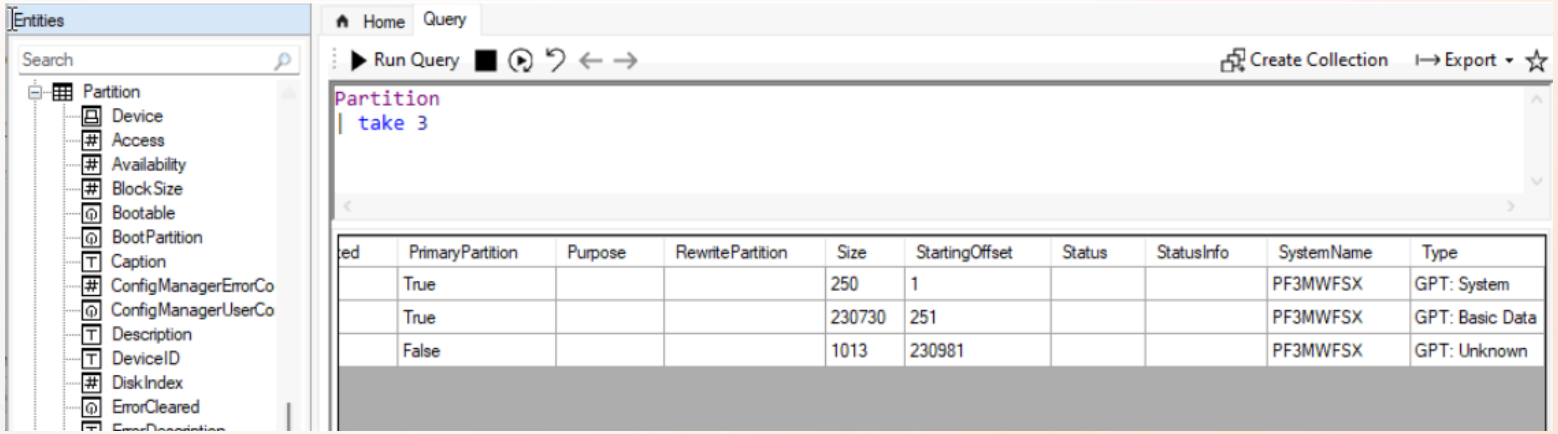
Operator	Description
where	Filters rows of data based on certain criteria
project	Simplify the view and select a specific subset of columns
distinct	Only show unique values
order by/ sort by column	Arrange the rows in descending order (can use asc)
count	Gives you the number of records returned
take	Allows you to specify an arbitrary number of records to return
top n by column	Returns the first n rows sorted by the specified column

Real World Example 1

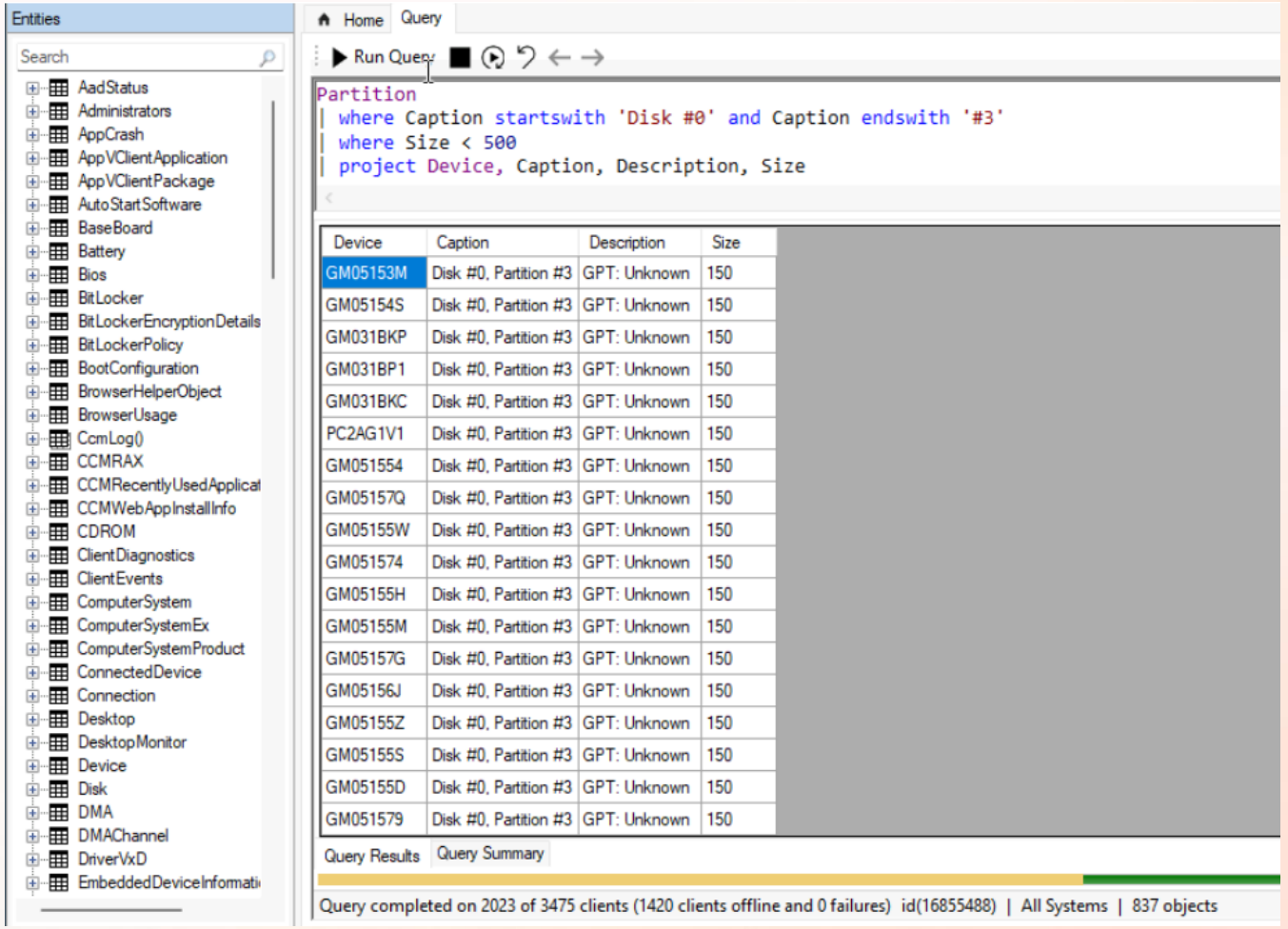


Real World Example 1





Real World Example 1



Summarize and Render

Summarize

- Very useful command!
  - Can be simple or complex!
- | summarize <aggregation> [by column(s)]
- The “by column(s)” in summarize p
  “GROUP BY”
- Common Aggregations
  - count
  - max/min
  - arg_max/ arg_min
  - sum
  - bin

```
1  IntuneAuditLogs
2  | where OperationName == "UpdateDeviceProperties WindowsAutopilotDeviceIdentity"
3  | summarize Count = count() by ResultType
4  | order by Count
```

Results | Chart

ResultType	Count
Success	96

Simple

More Complex

```
1  let Start = ago(7d);
2  let End = now();
3  IntuneAuditLogs
4  | where TimeGenerated between (Start .. End)
5  | where OperationName == "UpdateDeviceProperties WindowsAutopilotDeviceIdentity"
6  | extend ParsedProps = parse_json(Properties)
7  | where ParsedProps.Actor.ApplicationName endswith "umi"
8  //| summarize Count = count() by bin(TimeGenerated, 1d)
9  | union (
10     range x from 1 to 1 step 1
11     | mv-expand TimeGenerated=range(Start, End, 1d) to typeof(datetime)
12     | extend EventCount=0
13     )
14 | summarize EventCount=count(ResultType == "Success") by bin(TimeGenerated, 1d)
15
```

Aggregation Functions

Operator	Description
count	number of times the value appears in the dataset
max / min	highest/lowest value that appears in the dataset for that column (returns max/min value only)
arg_max / arg_min	highest/lowest value that appears in the dataset for that column (allows additional columns)
sum	adds values from different column together, you specify the columns
bin	rounds down values based on based on a specific criteria

Render

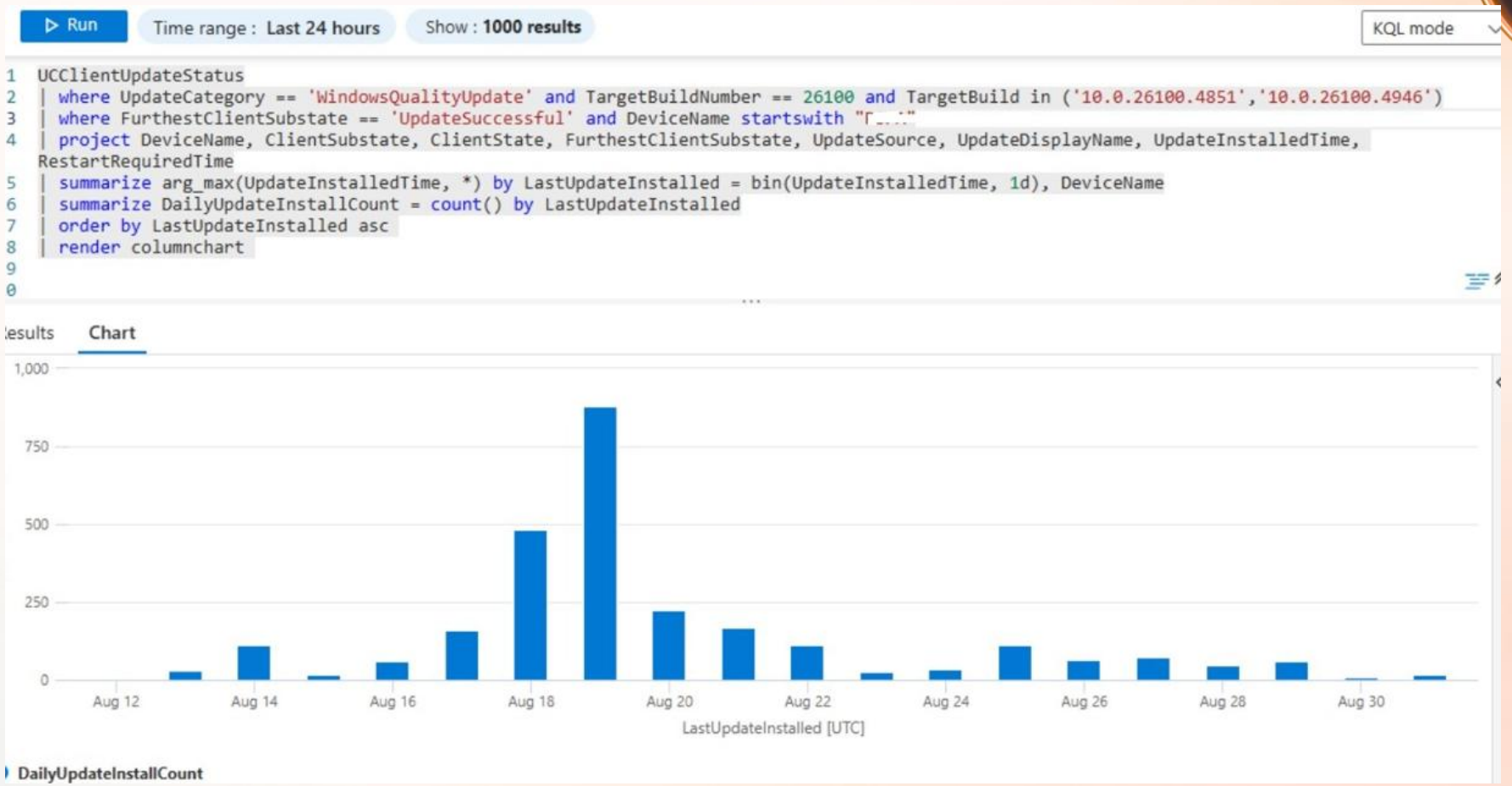
- Easy to visualize with Render
- Multiple chart types
- Change chart options: with (propertyName = propertyValue [, ...])

```
IntuneDevices
| where OS == "Windows"
| summarize count() by OSVersion
| order by count_
| render
```

areachart
barchart
columnchart
piechart
scatterchart
table
timechart
treemap

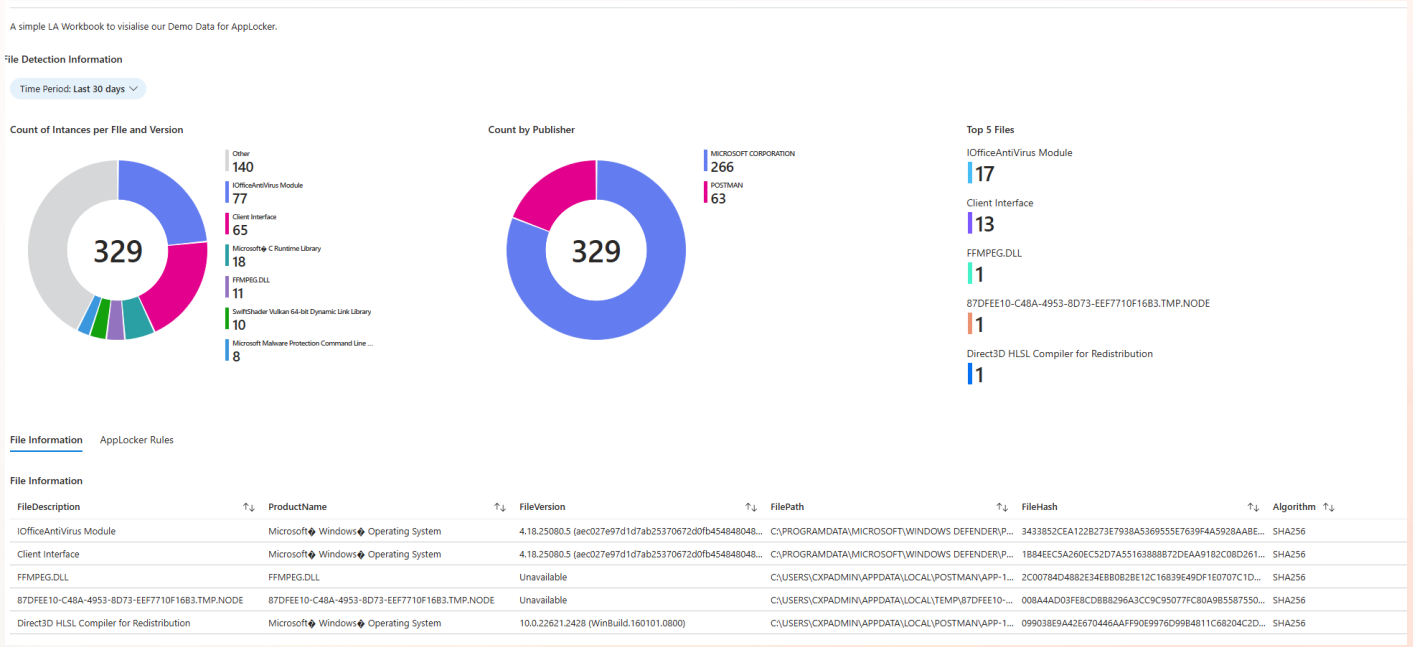
Results Ch

Real World Example 2



Summarise & Render

- Super useful for when you want to build workbooks
- What are workbooks…



Using Summarise & Render

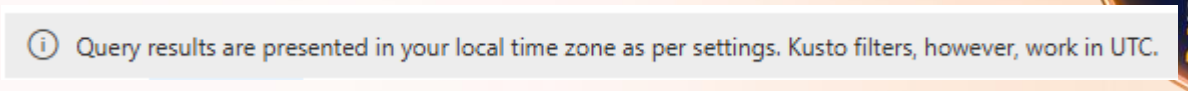
Working with data types

Handling Strings

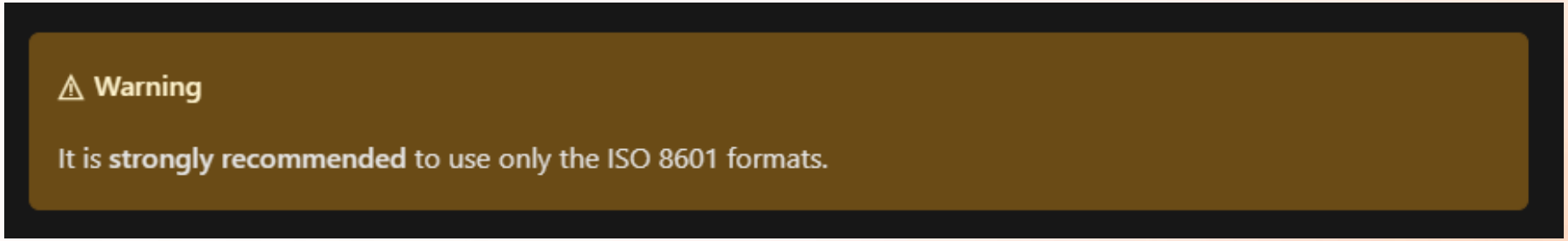
- String manipulation
  - substring()
  - tostring()
  - strlen()
  - strcat()
  - indexOf()
- Case sensitivity
  - By default, KQL is cAsE-sEnSiTiVe
  - Big performance benefits!
  - contains vs contains_cs
- Contains and Search, the performance devil's tools!
  - has vs contains
  - where vs search
- Matches regex() with strings?
  - Not in CMPivot/Intune Device query/Intune multi-device query

Date/Time values

- Might be in UTC! Check!



- Use ISO 8601 format
  - %Y-%m-%dT%H:%M:%s 2024-05-21T08:20:03.123456
  - %Y-%m-%d %H:%M 2024-05-21 15:55
- now()
  - now(-2d)
- ago()
  - ago(2d)



- between(..)
  - Timestamp between (datetime(2024-03-19T08:00:00) .. datetime(2024-03-21T08:00:00)
- todatetime()

Datetime example


```
IntuneAuditLogs
| where TimeGenerated between (datetime(2024-04-22) .. datetime(2024-05-05T04:00:00) )
| project TimeGenerated, Identity, Properties, ResultType

IntuneAuditLogs
| where TimeGenerated > ago(5d) and TimeGenerated < now(-2d)
| project TimeGenerated, Identity, Properties, ResultType
```

Working with Data Types

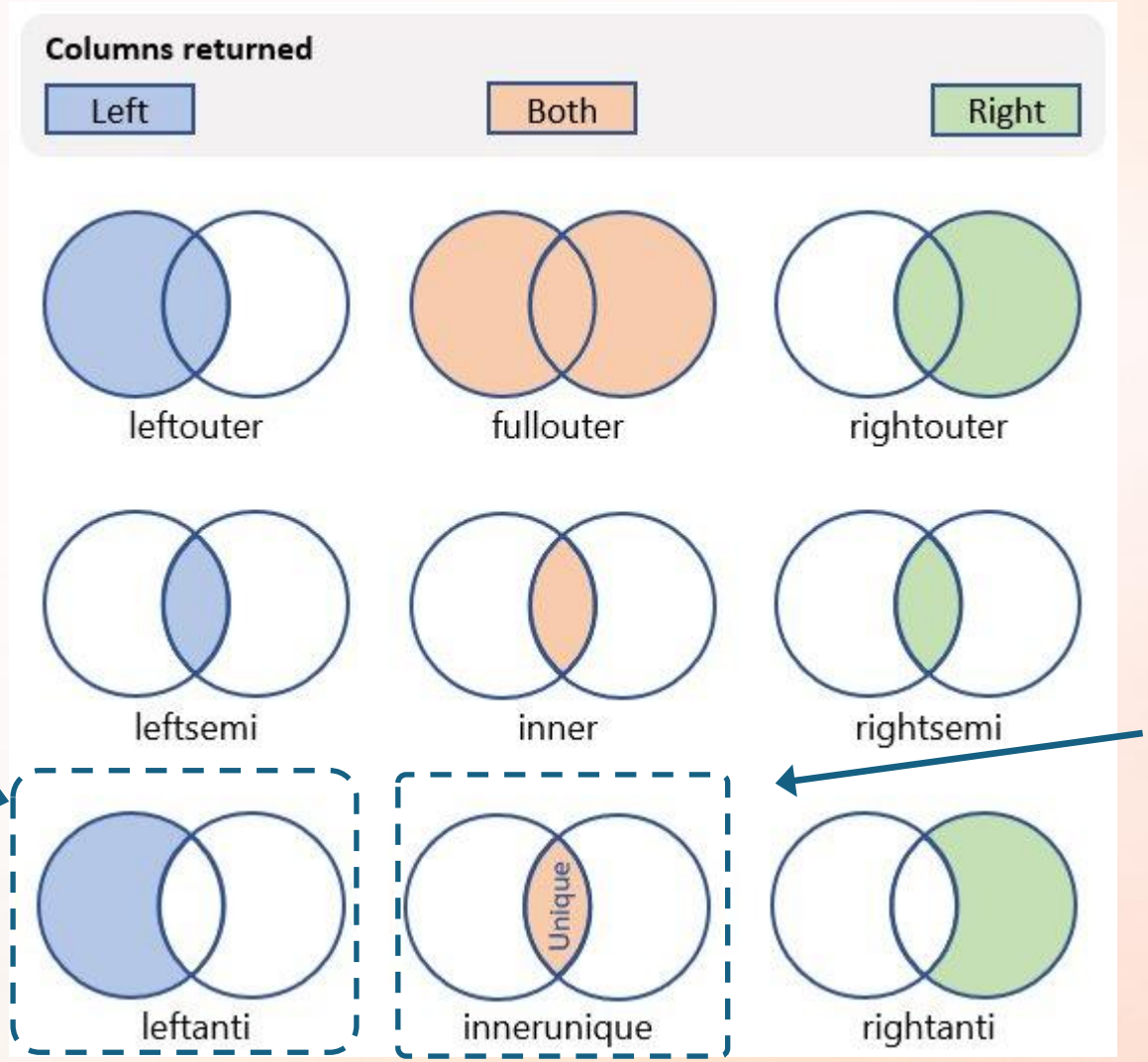
Join Operations

Join

- Combine info from two different entities
- | join kind=<JoinKind> <Table/Query> on ColumnName
- | join kind=<JoinKind> <Table/Query> on $left.ColumnName == $right.ColumnName

```
let ChromeSoftwareQuery = DeviceTvmSoftwareEvidenceBeta
| where SoftwareName == "chrome";
DeviceInfo
| join ChromeSoftwareQuery on DeviceId
| project DeviceName, OSVersion, SoftwareName, SoftwareVersion
| order by DeviceName asc
```

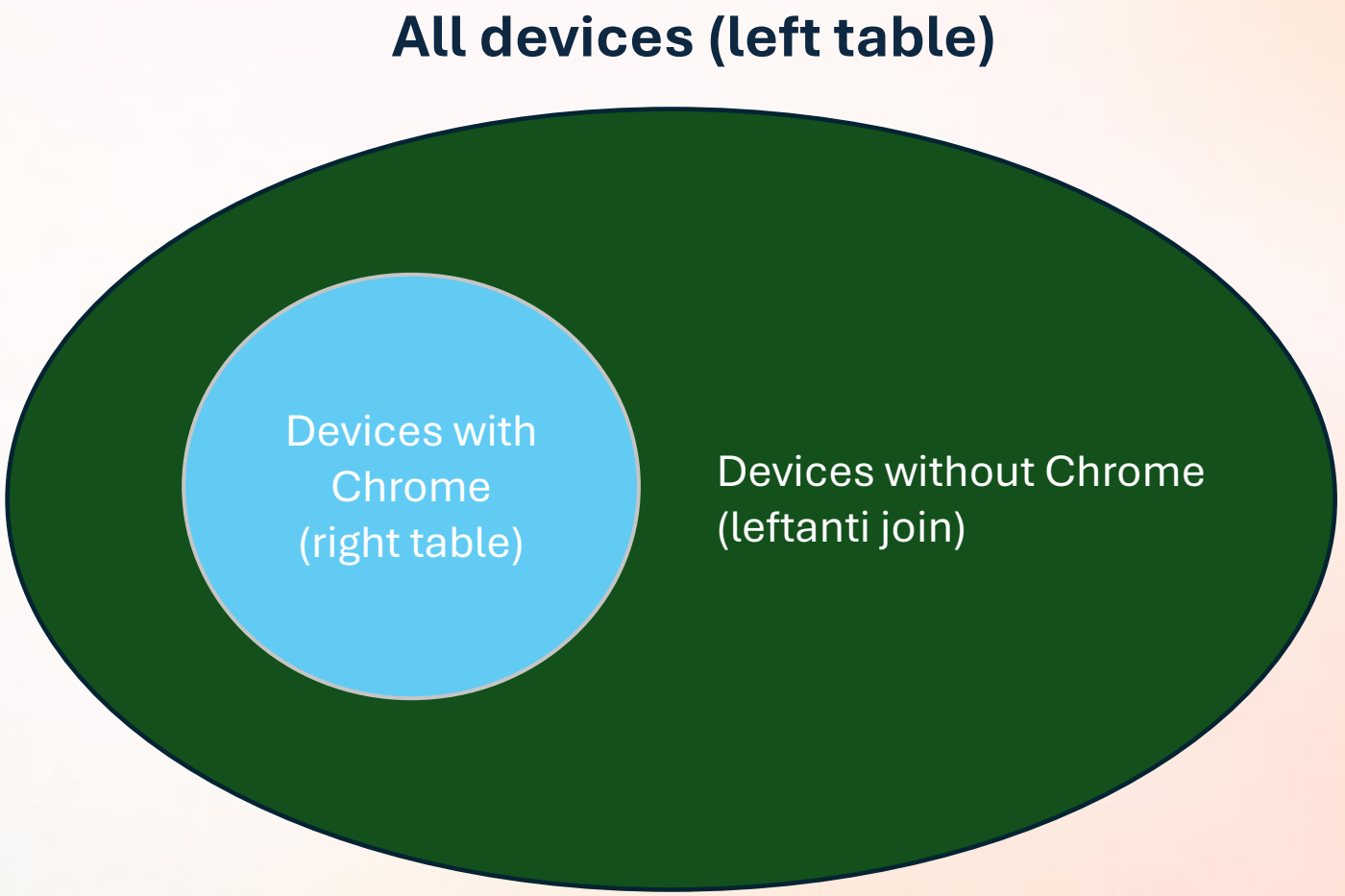
Join types



Sometimes needed (all objects without)

Default

All devices without Chrome

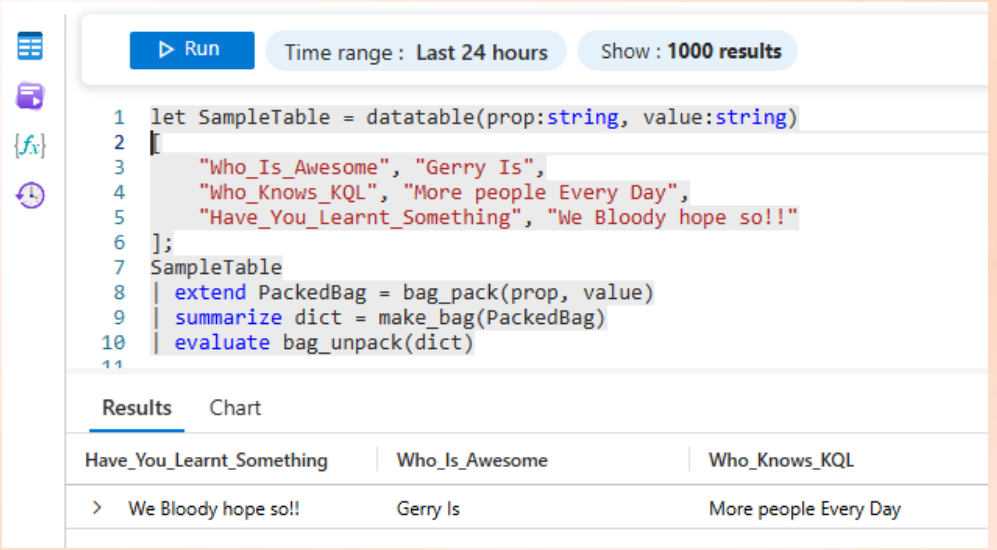


Using join

JSON Data in KQL

JSON with KQL…

- JSON is if a ‘dynamic’ type
- JSON Manipulation
  - parse_json()
  - mv_expand()
  - Combining mv_expand and parse_json()
- Extending/Projecting JSON to Columns
- It’s all about the swag bags!
  - bag_pack()
  - make_bag()
  - bag_unpack()



Parse JSON: Intune Audit Log

TimeGenerated [UTC]	Computer	FileDescription	FileVersion	ProductName	FileHash	Publisher	FullPublisherName	FileUseCount	Type
06/10/2025, 17:25:31.496	5CG34428C2	IOfficeAntiVirus Module	4.18.25080.5 (aec027e97d1d7a...	Microsoft Windows Opera...	{"Algorithm":"SHA256","Hash...	MICROSOFT CORPORATION	{"PublisherName":"O=MICRO...	4	dcrMMSMusic_AppLock

TimeGenerated [UTC]	2025-10-06T17:25:31.4960219Z
Computer	5CG34428C2
FileDescription	IOfficeAntiVirus Module
FileVersion	4.18.25080.5 (aec027e97d1d7ab25370672d0fb4548480483a83)
ProductName	Microsoft Windows Operating System
FileHash	{"Algorithm":"SHA256","Hash":"3433852CEA122B273E7938A5369555E7639F4A5928AABE6AEBB1A63558F9588B","Path":"C:\\PROGRAMDATA\\MICROSOFT\\WINDOWS DEFENDER\\PLATFORM\\4.18.25080.5-0\\MPOAV.DLL"}
Publisher	MICROSOFT CORPORATION
FullPublisherName	{"PublisherName":"O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US","ProductName":"MICROSOFT WINDOWS OPERATING SYSTEM","BinaryName":"MPOAV.DLL","BinaryVersion":"4.18.25080.5","HasPublisherName":true,"HasProductName":true,"HasBinaryName":true}
FileUseCount	4
TenantId	fdcb8ea4-bb1b-402e-bb0b-2c620d0ab139
Type	dcrMMSMusic_AppLocker_CL

{"PublisherName":"O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US","ProductName":"MICROSOFT WINDOWS OPERATING SYSTEM","BinaryName":"MPOAV.DLL","BinaryVersion":"4.18.25080.5","HasPublisherName":true,"HasProductName":true,"HasBinaryName":true}

```
dcrMMSMusic_AppLocker_CL
| extend ParsedJson = parse_json(FullPublisherName)
| project FileDescription, ProductName, FileVersion,
          Binary = ParsedJson.BinaryName,
          Version = ParsedJson.BinaryVersion,
          Product = ParsedJson.ProductName,
          Publisher = ParsedJson.PublisherName,
          FileHash = tostring(parse_json(FileHash).Hash)
```

Results | Chart

FileDescription	ProductName	FileVersion	Binary	Version	Product	Publisher	FileHash
IOfficeAntiVirus Module	Microsoft Windows Opera...	4.18.25080.5 (aec027e97d1d7a...	MPOAV.DLL	4.18.25080.5	MICROSOFT WINDOWS O...	O=MICROSOFT CORPORATIO...	3433852CEA122B273E7938A5369555E7639F4A5928AABE6AEBB1A63558F9588B

FileDescription	IOfficeAntiVirus Module
ProductName	Microsoft Windows Operating System
FileVersion	4.18.25080.5 (aec027e97d1d7ab25370672d0fb4548480483a83)
Binary	MPOAV.DLL
Version	4.18.25080.5
Product	MICROSOFT WINDOWS OPERATING SYSTEM
Publisher	O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US
FileHash	3433852CEA122B273E7938A5369555E7639F4A5928AABE6AEBB1A63558F9588B

Working with JSON

Performance

- Reduce the amount of data being queried (where)
- String operators (use has instead of contains)
- Case-sensitive operators where possible
- Searching text (look in a specific column, don't use *)
- join (Select the table with the fewest rows as the first one (left-most in query))

Tips & Tricks

- Save your Queries
- Extending your Data
- Build yourself a workbook!
- Bring in your Own Data

Summary

- Just use KQL!
- With a few commands you can do a lot
- Filter as soon as possible and as much as possible (where)
- Difficult (impossible?) to do any harm
  - Only queries… No modifications
- Start with a simple query to learn the attributes
- Know your data types

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!