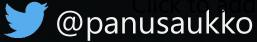# Unearth your Intune data

Panu Saukko

ProTrainIT

🐦 @panusaukko

MVP – Enterprise Mobility

Merlijn Van Waeyenberghe

OB-V-US

🐦 @MerlinFromBE

MVW – T&T

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC – VIRTUAL SUMMIT –

Purpose of the session

- Show different *easy* ways to get relevant data from Intune
  - Not a deep dive!

- Different methods:
  - Microsoft Endpoint Manager Admin Center portal
  - Graph/PowerShell
  - Log Analytics/KQL
  - PowerBI

- One example task:
  - Report OS versions of Windows devices to find out which CU is installed to the devices

MEM Admin Center portal

MEM Admin Center portal

- MEM Admin Center is the main tool to manage Intune devices
- Issues with the portal
  - UI is not consistent
  - Different parts are coming from different product groups
  - "Older" parts have different UI than "newer" parts!
  - Limited searching/filtering
- Many built-in reports

Example1: Devices

Search: Contains
Search based on multiple attributes

Can select additional columns

Filter

Managed by

7 selected

Device action

4 selected

Category

2 selected

Ownership

3 selected

Compliance

5 selected

Jailbroken

3 selected

OS

13 selected

Columns ✕

☑ Managed by
☑ Ownership
☑ Compliance
☐ Compliance grace period expiration
☑ OS
☑ OS version
☐ Device action
☐ Device state
☐ Primary user email address
☑ Last check-in
☐ Enrollment date
☐ IMEI
☐ EAS activated
☐ EAS activation ID
☐ Intune Registered

↻ Refresh   ▽ Filter   ≡≡ Columns   ⬇ Export | ⊞ Bulk Device Actions

🔍 top

Showing 1 to 4 of 4 records

Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance ↑↓	OS
AINON-LAPTOP	Co-managed	Corporate	✓ Compliant	Windows

Filtering option   Export

Sorting by "all" columns

Export data for all managed devices

This will export data to a comma-separated values (.csv) file. Do you want to continue?

◉ Only include selected columns in the exported file

○ Include all inventory data in the exported file
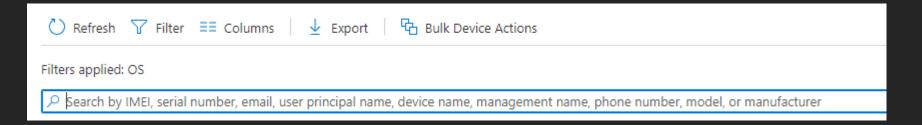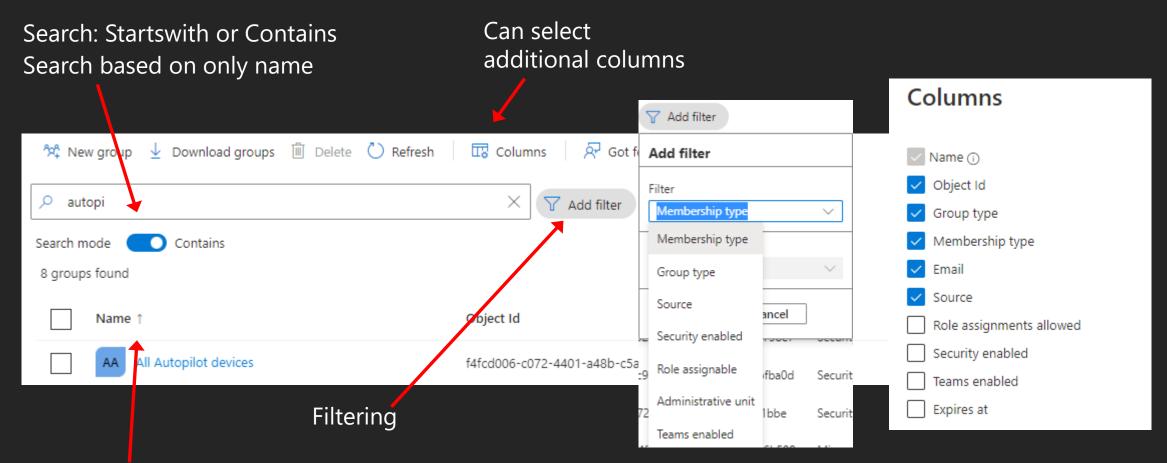
[Yes]   [No]

Example1: Devices

The query is looking from the following attributes:
- Device name
- Serial number
- IMEI
- User's email
- Management name
- Phone number
- Manufacturer/Model
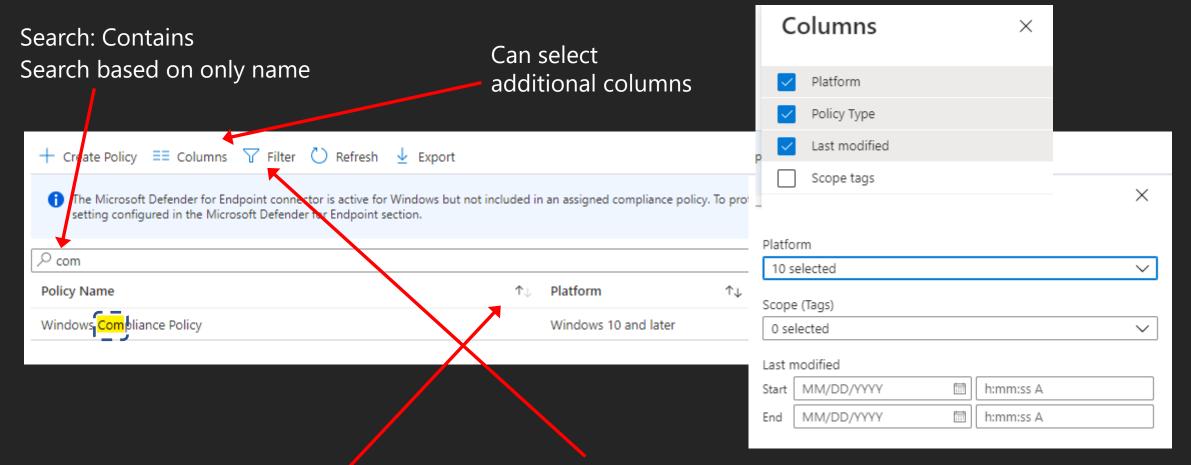- Azure AD/Intune Device ID

Example2: Groups

Search: Startswith or Contains
Search based on only name

Can select
additional columns

Filtering

Sorting by only name

Example3: Autopilot devices

Search: only Startswith
Search based on only serial number

No additional columns

⟳ Sync	▽ Filter	⤒ Import	⤓ Export	⚲₊ Assign user	⟳ Refresh	🗑 Delete

Filter ✕

∧ Essentials

Last sync request : 02/15/22 6:48 AM

State

| 2 selected ⌄ |

22, 6:48 AM

Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.

Profile status

| 2 selected ⌄ |

🔍 11

Serial number	Manufacturer	Model	Profile status
☐ 1165-8867-8180-7796-0826-3723-57	Microsoft Corporation	Virtual Machine	Assigned
☐ 1187-1669-7182-7164-0441-1792-96	Microsoft Corporation	Virtual Machine	Assigned

Model

| |

Purchase order

| |

Manufacturer

| |

Filtering available

Group Tag

| |

No sorting

Example4: Compliance policies

Search: Contains
Search based on only name

Can select
additional columns

Columns ✕

☑ Platform
☑ Policy Type
☑ Last modified
☐ Scope tags

✕

+ Create Policy   ≡≡ Columns   ▽ Filter   ↻ Refresh   ⬇ Export

ⓘ The Microsoft Defender for Endpoint connector is active for Windows but not included in an assigned compliance policy. To pro
setting configured in the Microsoft Defender for Endpoint section.

🔍 com

Policy Name ↑↓	Platform ↑↓
Windows Compliance Policy	Windows 10 and later

Platform
10 selected   ⌄

Scope (Tags)
0 selected   ⌄

Last modified
Start   MM/DD/YYYY 🗓   h:mm:ss A
End   MM/DD/YYYY 🗓   h:mm:ss A

Filtering available

Sorting by all columns

Builtin reports

Monitor
Home > Devices >

Configuration
- Assignment status
- Assignment failures (preview)
- Devices with restricted apps
- Encryption report
- Certificates

Compliance
- Noncompliant devices
- Devices without compliance policy
- Setting compliance
- Policy compliance
- Noncompliant policies (preview)
- Windows health attestation report

Enrollment
- Autopilot deployments (preview)
- Enrollment failures
- Incomplete user enrollments

Software updates
- Per update ring deployment state
- Installation failures for iOS devices
- Feature update failures (Preview)
- Windows Expedited update failures (Preview)

Other
- Device actions

Reports
Home >

Device management
- Device compliance
- Device configuration (preview)
- Group policy analytics (preview)
- Windows updates (preview)
- Cloud attached devices (preview)

Endpoint security
- Microsoft Defender Antivirus
- Firewall

Analytics
- Endpoint analytics

Intune data warehouse
- Data warehouse

Azure monitor
- Diagnostic settings
- Log analytics
- Workbooks

These reports are often missed!

Demo: OS versions from MEM Admin Center portal
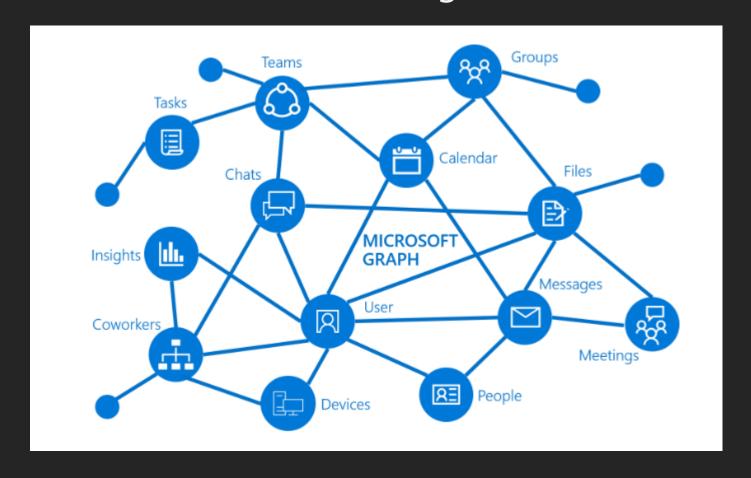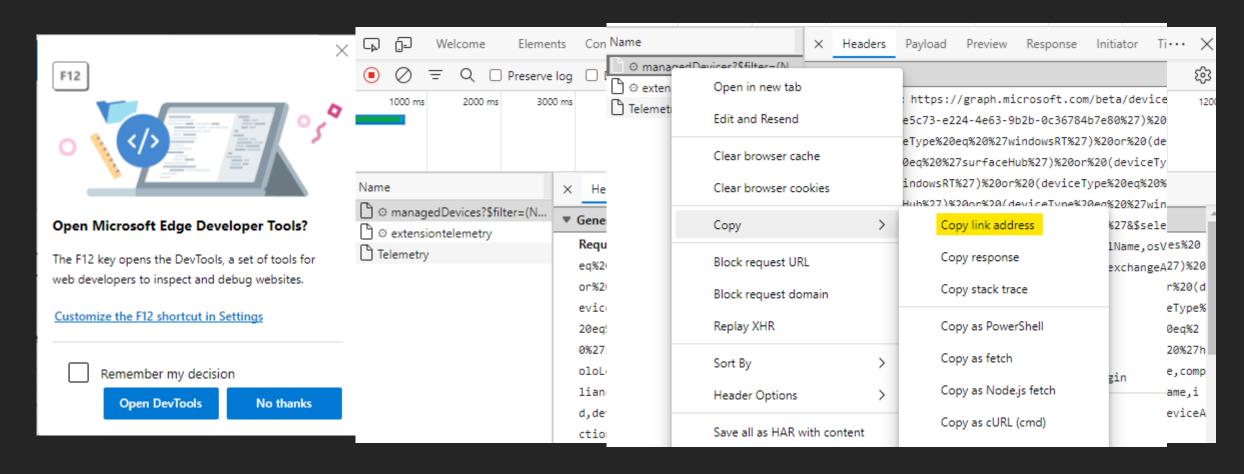
Graph and PowerShell

What is Graph?

- Exposes REST APIs and client libraries to access data on Microsoft cloud services (including Intune)

Browser developer mode

- F12 is your friend!

Graph Query

https://graph.microsoft.com/beta/deviceManagement/managedDevices?$fil
ter=(Notes%20eq%20%27bc3e5c73-e224-4e63-9b2b-
0c36784b7e80%27)%20and%20(((deviceType%20eq%20%27desktop%27)%
20or%20(deviceType%20eq%20%27windowsRT%27)%20or%20(deviceType
%20eq%20%27winEmbedded%27)%20or%20(deviceType%20eq%20%27surf
aceHub%27)%20or%20(deviceType%20eq%20%27desktop%27)%20or%20(d
eviceType%20eq%20%27windowsRT%27)%20or%20(deviceType%20eq%20
%27winEmbedded%27)%20or%20(deviceType%20eq%20%27surfaceHub%2
7)%20or%20(deviceType%20eq%20%27windowsPhone%27)%20or%20(devi
ceType%20eq%20%27holoLens%27)))&$top=25&$skipToken=Skip=%270%
27&$select=deviceName,osVersion,id,deviceType,ownerType,deviceRegistrat
ionState,managementState,exchangeAccessState,exchangeAccessStateReaso
n,deviceActionResults,deviceEnrollmentType

%20 = space
%27 = '

Graph Query

https://graph.microsoft.com/beta/deviceManagement/managedDevices?
$filter=(Notes eq 'bc3e5c73-e224-4e63-9b2b-0c36784b7e80') and
(((deviceType eq 'desktop') or (deviceType eq 'windowsRT') or (deviceType
eq 'winEmbedded') or (deviceType eq 'surfaceHub') or (deviceType eq
'desktop') or (deviceType eq 'windowsRT') or (deviceType eq 'winEmbedded')
or (deviceType eq 'surfaceHub') or (deviceType eq 'windowsPhone') or
(deviceType eq
'holoLens')))&$top=25&$skipToken=Skip='0'&$select=deviceName,osVersi
on,id,deviceType,ownerType,deviceRegistrationState,managementState,exch
angeAccessState,exchangeAccessStateReason,deviceActionResults,deviceEnr
ollmentType

Graph Query

1. Which object?

https://graph.microsoft.com/beta/deviceManagement/managedDevices?
$filter=((deviceType eq 'desktop') or (deviceType eq
'windowsRT'))&$top=25&$skipToken=Skip='0'&$select=deviceName,osVers
ion,id

Graph Query

1. Which object?   2. Filter

https://graph.microsoft.com/beta/deviceManagement/managedDevices?
$filter=((deviceType eq 'desktop') or (deviceType eq
'windowsRT'))&$top=25&$skipToken=Skip='0'&$select=deviceName,osVers
ion,id

Graph Query

1. Which object? 2. Filter 3. Which attributes to show

https://graph.microsoft.com/beta/deviceManagement/managedDevices?
$filter=((deviceType eq 'desktop') or (deviceType eq
'windowsRT'))&$top=25&$skipToken=Skip='0'&$select=deviceName,osVersion,id
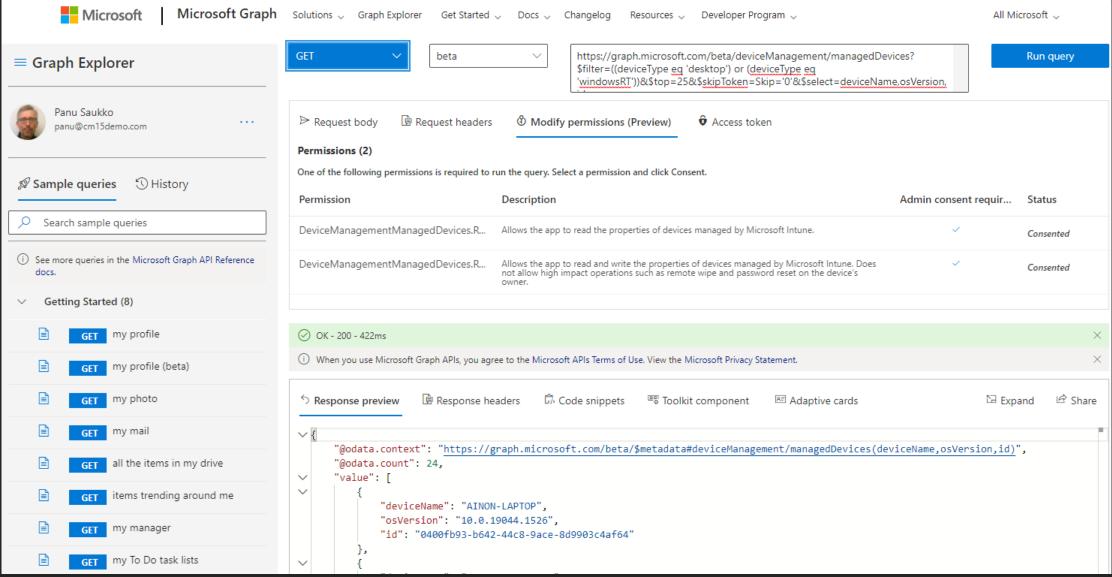
Common Graph queries

- $select   = properties to show
- $filter   = filter objects
- $orderby = sort by a property
- $search   = find specific objects
- $top   = first x objects

Graph Explorer

https://developer.microsoft.com/en-us/graph/graph-explorer

Microsoft.Graph PowerShell module

- Main module to use
  - Install-module –name Microsoft.Graph
  - Multiple sub modules
- Key commands:
  - Connect-MgGraph –Scopes *permission-scope*
  - Disconnect-MgGraph
  - Get-MgContext
  - Select-MgProfile –Name "beta"
  - Find the right command! ☺
  - Invoke-MgGraphRequest

```
PS C:\> get-command -module Microsoft.graph* *MgDevice* | Measure-Object

Count             : 1452
```
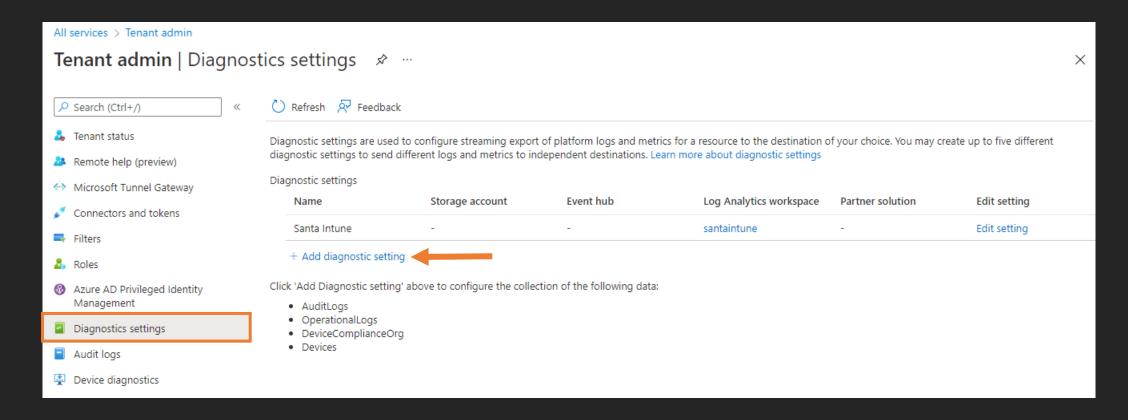
Demo: A simple PowerShell script to get OS versions

Getting started
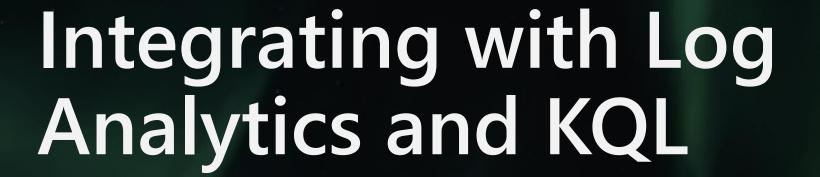
- In-depth how-to guides:
    - [Get started with the Microsoft Graph PowerShell SDK - Microsoft Graph | Microsoft Docs](#)
    - [Azure Automation Runbook scripts to grab Intune data and output CSV to Storage Account containers.](#)
    - [Migrate from Azure AD PowerShell to the Microsoft Graph PowerShell SDK. | Microsoft Docs](#)
- Some nice Youtube videos
    - [Getting started with Microsoft Graph](#)
    - [Managing with Microsoft Graph (and PowerShell) by John Savill](#)

Getting started

- Permissions to Graph Explorer
- In-depth how-to guides:
  - [Get started with the Microsoft Graph PowerShell SDK - Microsoft Graph | Microsoft Docs](#)
  - [Azure Automation Runbook scripts to grab Intune data and output CSV to Storage Account containers.](#)
  - [Microsoft Graph Archives - Sandy's blog (sandyzeng.com)](#)
  - [Posts on graph - MSEndpointMgr](#)
    - [Export Microsoft Intune audit data to Log Analytics using Graph API and Azure Automation - Jan Ketil Skanke](#)
    - [Using Azure AD authentication with Intune Graph API and PowerShell - Nickolaj Andersen](#)
  - [Using the Microsoft Graph API with PowerShell (adamtheautomator.com)](#)
  - [Migrate from Azure AD PowerShell to the Microsoft Graph PowerShell SDK. | Microsoft Docs](#)

Integrating with Log Analytics and KQL

Connecting Intune to Log Analytics (Azure Monitor)

[Route logs to Azure Monitor using Microsoft Intune | Microsoft Docs](#)
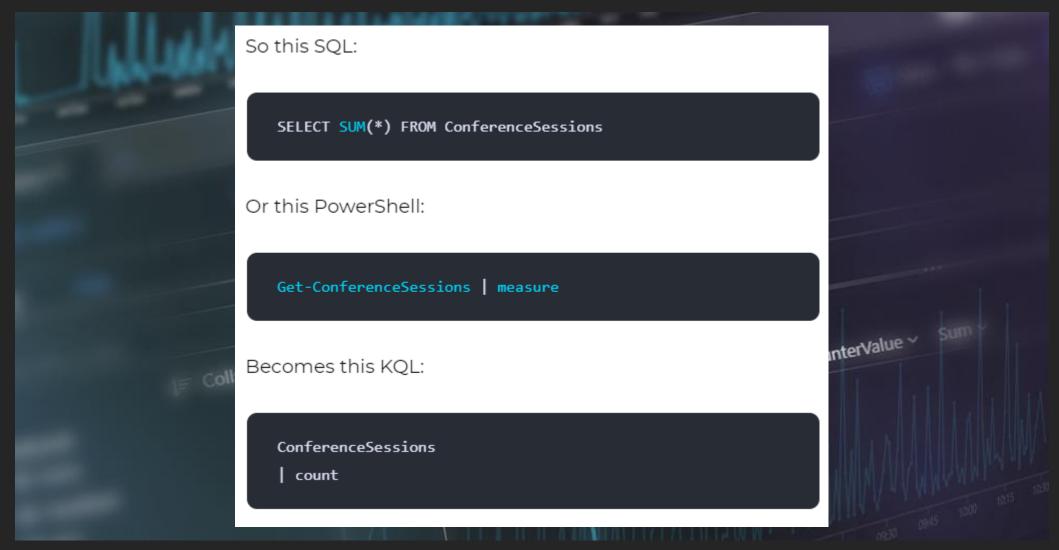
Requirements

- Azure Subscription
- Log Analytics workspace
- An Azure storage account
- Global Administrator or Intune Service Administrator
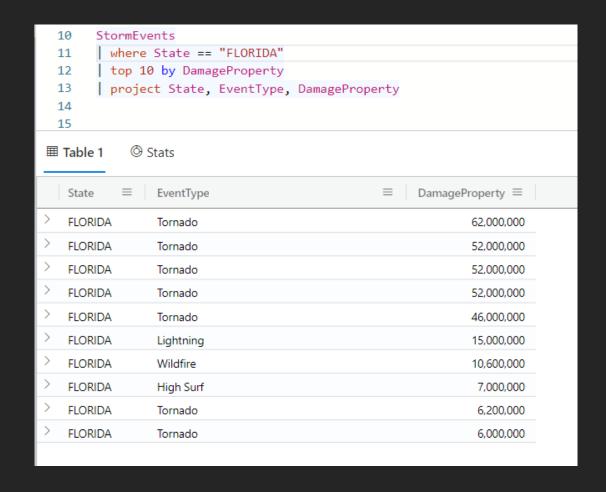
Cost considerations

Introducing Kusto

So this SQL:

```
SELECT SUM(*) FROM ConferenceSessions
```
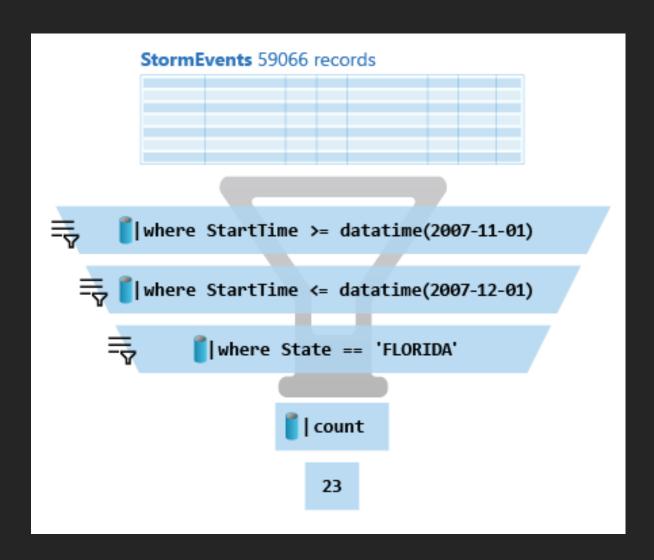
Or this PowerShell:

```
Get-ConferenceSessions | measure
```

Becomes this KQL:

```
ConferenceSessions
| count
```

Credit: Kusto 101 - A Jumpstart Guide to KQL - SquaredUp

KQL Query – example 1


```
Kusto

StormEvents
| where State == "FLORIDA"
| top 10 by DamageProperty
| project State, EventType, DamageProperty
```

```
10    StormEvents
11    | where State == "FLORIDA"
12    | top 10 by DamageProperty
13    | project State, EventType, DamageProperty
14
15
```

⊞ Table 1   ◎ Stats

State	EventType	DamageProperty
FLORIDA	Tornado	62,000,000
FLORIDA	Tornado	52,000,000
FLORIDA	Tornado	52,000,000
FLORIDA	Tornado	52,000,000
FLORIDA	Tornado	46,000,000
FLORIDA	Lightning	15,000,000
FLORIDA	Wildfire	10,600,000
FLORIDA	High Surf	7,000,000
FLORIDA	Tornado	6,200,000
FLORIDA	Tornado	6,000,000

KQL Query – example 2


```Kusto
Kusto

StormEvents
| where StartTime between (datetime(2007-11-01) .. datetime(2007-12-01))
| where State == "FLORIDA"
| count
```
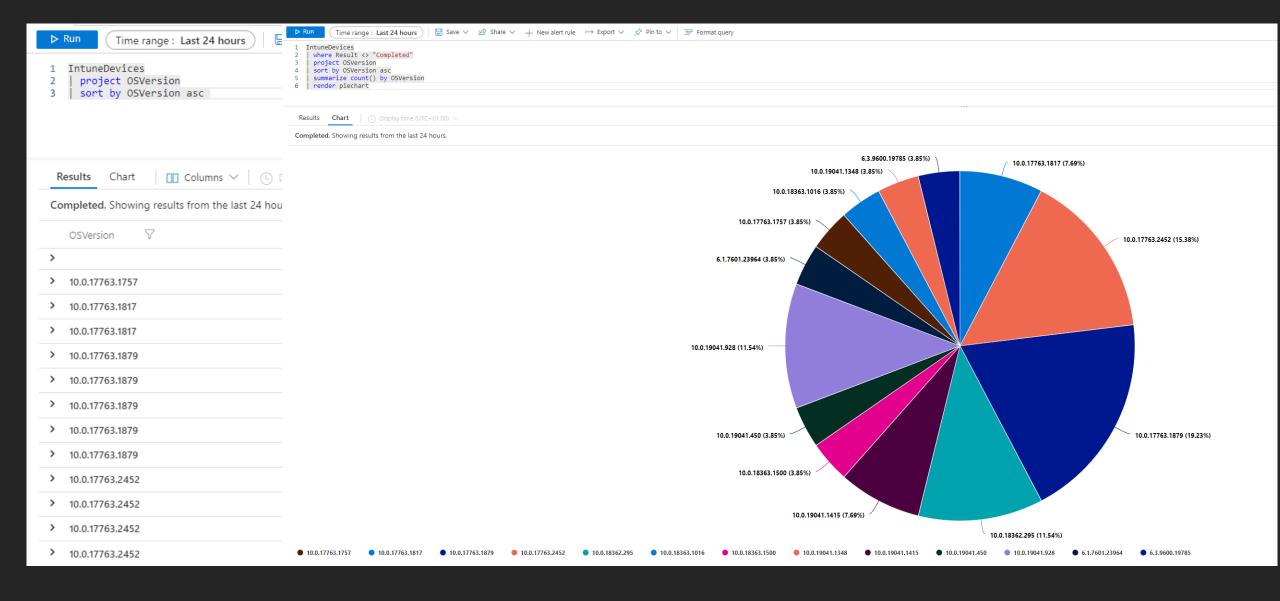
KQL query for OSVersion

KQL query for OSVersion - code

All OS versions
```
IntuneDevices
| project OSVersion
```

Make it prettier
```
| sort by OSVersion asc
```

Exclude "Completed"
```
IntuneDevices
| where Result <> "Completed"
| project OSVersion
| sort by OSVersion asc
```

Add device name
```
IntuneDevices
| where Result <> "Completed"
| project OSVersion, DeviceName
| sort by OSVersion asc
```

Summarize
```
IntuneDevices
| where Result <> "Completed"
| project OSVersion
| sort by OSVersion asc
| summarize by OSVersion
```

Count
```
| summarize count() by OSVersion
```

Render
```
| render piechart
```

Complete query

```
IntuneDevices
| where Result <> "Completed"
| project OSVersion
| sort by OSVersion asc
| summarize count() by OSVersion
| render piechart
```

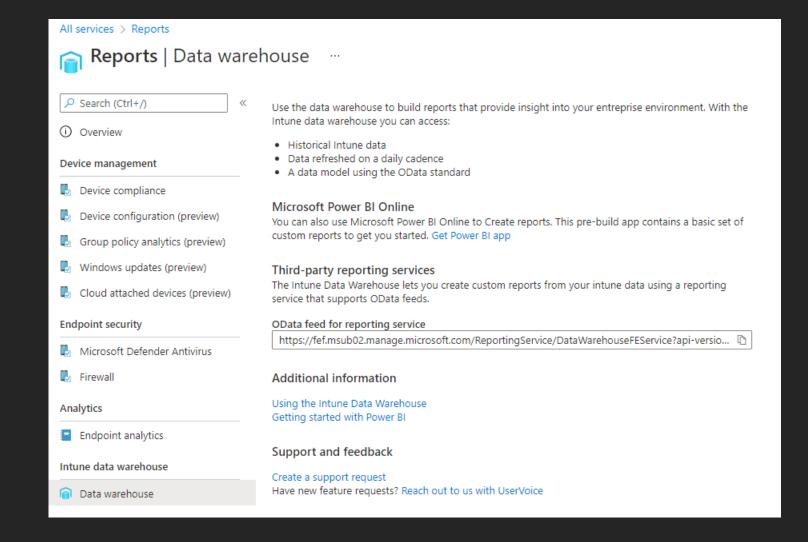# PowerBI reports from Intune data

Requirements

- Power BI licensing
  - Free for OData, M queries...
  - ... no sharing though
  - Pro or Premium for data flow, incremental refresh...
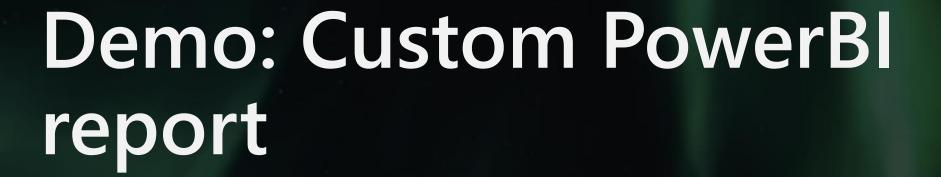- Power BI Desktop
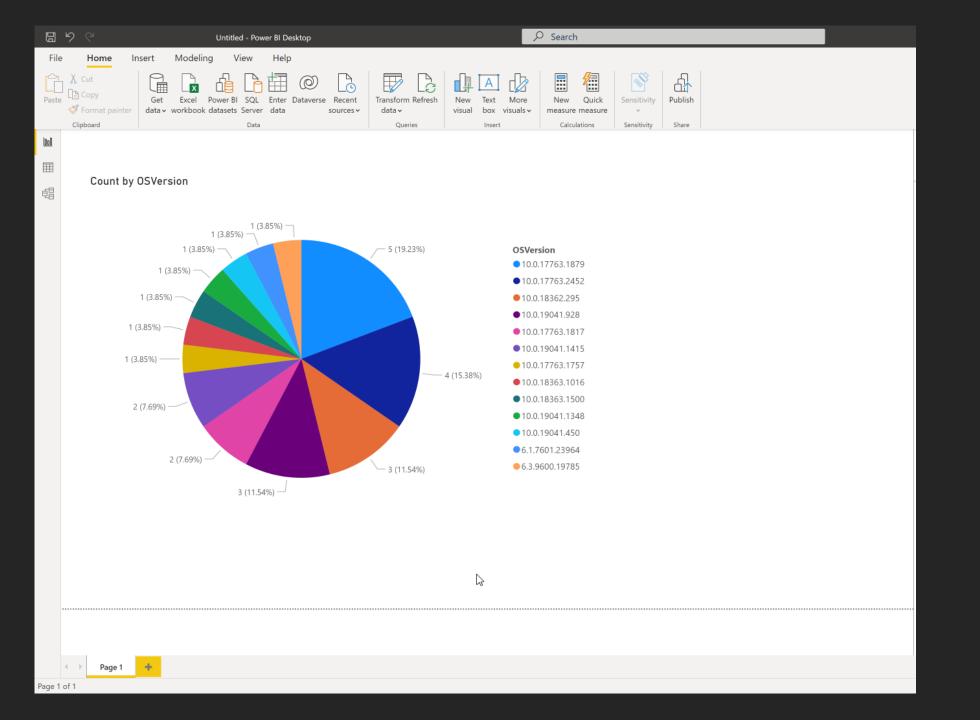
Data warehouse

- Data warehouse?

Reports

- Build query in Log Analytics
- Export as M query
- Power BI Desktop > blank query > advanced editor

Demo: Custom PowerBI report

Power BI M query sample

```
= let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/<your-workspace-guid>/query",

[Query=[#"query"="IntuneDevices

| summarize countif(OSVersion != '') by OSVersion

| where countif_ > 0

",#"x-ms-app"="OmsAnalyticsPBI",#"timespan"="P1D",#"prefer"="ai.response-thinning=true"],Timeout=#duration(0,0,4,0)])),

TypeMap = #table(

{ "AnalyticsTypes", "Type" },

{

{ "string",   Text.Type },

{ "int",      Int32.Type },

{ "long",     Int64.Type },

{ "real",     Double.Type },

{ "timespan", Duration.Type },

{ "datetime", DateTimeZone.Type },

{ "bool",     Logical.Type },

{ "guid",     Text.Type },

{ "dynamic",  Text.Type }

}),

DataTable = Source[tables]{0},

Columns = Table.FromRecords(DataTable[columns]),

ColumnsWithType = Table.Join(Columns, {"type"}, TypeMap , {"AnalyticsTypes"}),

Rows = Table.FromRows(DataTable[rows], Columns[name]),

Table = Table.TransformColumnTypes(Rows, Table.ToList(ColumnsWithType, (c) => { c{0}, c{3}}))

in

Table
```

Options

- Inject more data to Custom Logs
  - Enhance Intune Inventory data with Proactive Remediations and Log Analytics - MSEndpointMgr

- Use Azure Storage Blob and Automation
  - phmehta94/IntuneAutomatedReporting: Azure Automation Runbook scripts to grab Intune data and output CSV to Storage Account containers. (github.com)

Summary

- Many ways to get Intune data
- Portal has limitations
- Graph & PowerShell are your friends for custom queries
- Integrating with Log Analytics gives many benefits
- With Power BI you can easily create nice reports

A big thanks to our sponsors

Thank you!

Please remember to fill out the evals!