

A dark blue background featuring a network graph with numerous glowing blue nodes and connecting lines, suggesting a complex data structure or cloud environment.

Advanced Copilot Analytics: From Zero to Hero with the Unified Audit Log, Entra ID and Power BI

Tatu Seppälä



★ Data security
★ Insider risk
Power Platform
Governance
IAM / Entra ID
Generative AI



The Digital
Neighborhood



Agenda

- ⚠️ Pain points
- 🤖 Pull Copilot events from the UAL
- 👉 Grab identity metadata from Entra ID
- ⌚ Bring 'em together!
- 🔍 Analyze & take action
- ⚡ Automate & expand



Pain points



Enabled users

145

Active users

132

Active users rate

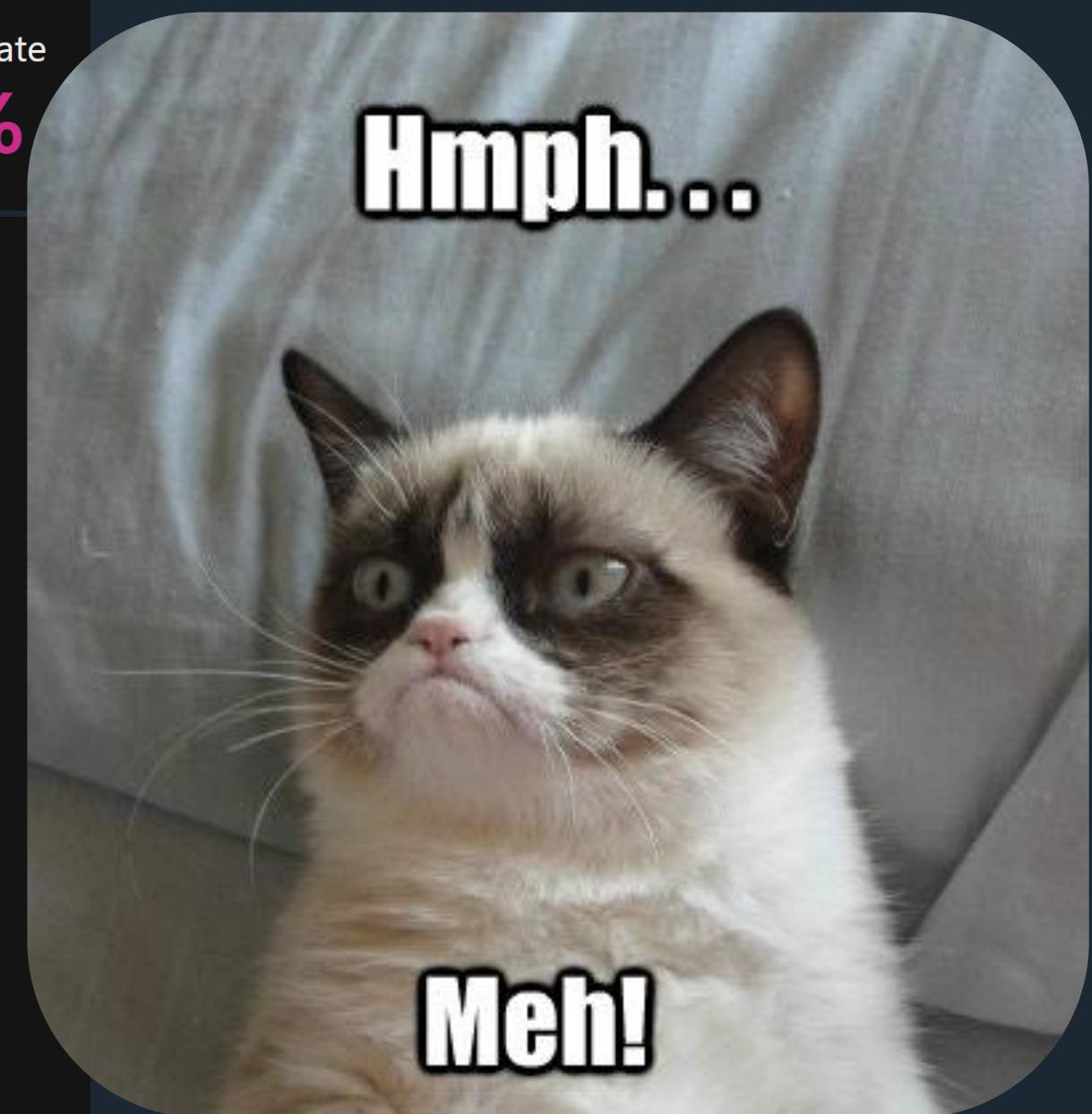
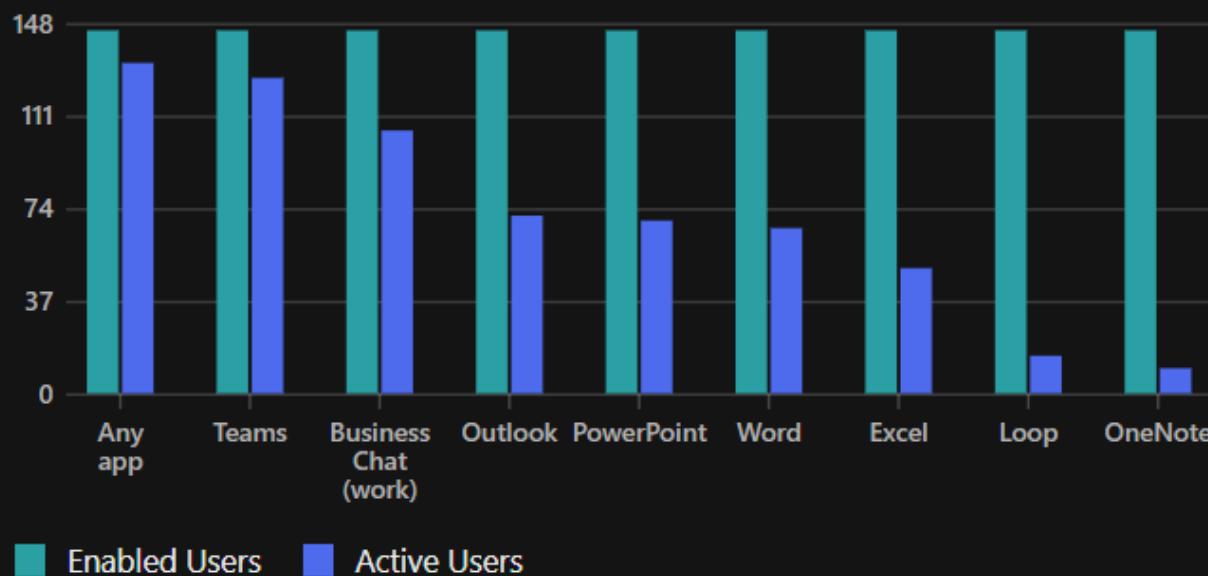
91.0%

Adoption by app

Summary

Trend

The number of enabled and active users of Microsoft 365 Copilot apps for the selected period [See metric definitions](#)



Native Copilot Analytics?

The dashboard displays the following data:

Category	Value
Active Copilot users	127,370
Copilot actions taken	1,786,203
Copilot assisted hours	183,290 hours

Scope: Your group, Organizations (All), Job function (All). Time period: Mar 31. Metric: Total number of active Copilot users. View by: Scope.

Today we're announcing Viva Insights will be included in Microsoft 365 Copilot at no additional charge as part of the new **Copilot Analytics**. Copilot Analytics is designed to empower every IT

The dashboard displays the following data:

App	Count
Outlook	6,062
Word	5,625
PowerPoint	4,924
Excel	4,115
Copilot Chat	8,108

Meeting hours summarized by Copilot: 18,967. Emails drafts using Copilot: 18,687. Chat conversation summaries created by Copilot: 91,490. More Insights coming soon!

Microsoft on November 19th,
2024





Highlights

Meetings

94,452

Meetings summarized by Copilot

77,607

Meeting hours summarized by Copilot

43,354

Meeting hours summarized by Copilot

[Explore more](#)

Teams Chat

7,265

Chat conversations summarized by Copilot

84,683

Chat messages composed using Copilot

57,352

Chat conversation summaries created by Copilot

Native analytics are slowly getting better..

Email

40,890

Emails sent using Copilot

119,984

Email thread summaries created by Copilot

86,435

Emails drafts using Copilot

[Explore more](#)

Documents

175,361

Document creation actions using Copilot

82,193

Document summaries created by Copilot

160,338

Document edit or format actions using Copilot



Things we need to know

-  Roles utilizing specific Copilots the most? Overall?
-  Underutilized Copilots per role?
-  Who are the **pioneers**?
-  Effectiveness of trainings?
-  Licenses ripe for reassignment?

CopilotInteraction events



Copilot audit logging

A bit of history

- › Before May 2024, M365 Copilot audit logs were very inconsistent 😔
- › On May 1st, 2024, the **CopilotInteraction** audit log schema finally got corrected and was made consistent 🎉



CopilotInteraction events

- › One event saved in the UAL for each **interaction thread**
- › Each thread can contain multiple messages – both user prompts *and* Copilot responses
- › Most of what you need is in the **AuditData** attribute

RecordID: 99b0a960-13a0-461f-8c5c-cb2
CreationDate: 12/13/2023 17:12
RecordType: 261
Operation: CopilotInteraction
UserID: admin@MODERNCOMMS97518-
AuditData: {"CreationTime": "2023-12-13T17:12:00Z", "Operation": "CopilotInteraction", "RecordID": "99b0a960-13a0-461f-8c5c-cb2316ea273d", "RecordType": 261, "UserID": "admin@MODERNCOMMS97518-84335f0ce512", "Version": 1, "WorkflowID": "f8884f3f373e", "UserType": 0, "AISystemPlugin": []}, "AccessedResources": [{"url": "https://my.sharepoint.com/personal/admin_moderncomms97518/_api/v2.0/me/drive/items/01B87F4ACA19F7%7D", "sourcedoc": "%7B9FDE1491-B079-4180-9B87F4ACA19F7%7D&file=AboutElephant"}, {"url": "https://my.sharepoint.com/personal/admin_moderncomms97518/_api/v2.0/me/messages", "sourcedoc": "%7B9FDE1491-B079-4180-9B87F4ACA19F7%7D&file=AboutElephant"}, {"url": "https://my.sharepoint.com/personal/admin_moderncomms97518/_api/v2.0/me/messages/1715187560311", "sourcedoc": "%7B9FDE1491-B079-4180-9B87F4ACA19F7%7D&file=AboutElephant"}, {"url": "https://my.sharepoint.com/personal/admin_moderncomms97518/_api/v2.0/me/messages/1715187561014", "sourcedoc": "%7B9FDE1491-B079-4180-9B87F4ACA19F7%7D&file=AboutElephant"}], "Messages": [{"Id": "1715187560311", "isPrompt": false}, {"Id": "1715187561014", "isPrompt": false}], "ThreadID": "nSX2U7tjccqSrtYAoG341@thread.v2"}

AppHost

- > AppHost identifies the Copilot scenario / type
- > New apps added regularly
- > Usually clear. Can be cryptic too.
- > One of the key improvements available from May 1st '24 onwards

AppHost values:

-  Bing
-  Teams
-  Outlook
-  Office
-  DevUI
-  BashTool
-  Word
-  Excel
-  PowerPoint
-  OneNote
-  SharePoint
-  Loop
-  Whiteboard
-  M365App
-  M365AdminCenter
-  Planner
- VivaEngage

AppHost values on Jan 30th, 2025

 appchat

 **Bing**

 **Copilot Studio**

 Designer

 Excel

 Forms

 Loop

 **Office (also Bing!)**

 **M365AdminCenter**

 Microsoft Teams

 OneNote

 Outlook

 Planner

 **Power BI**

 PowerPoint

 SharePoint

 Stream

 Teams

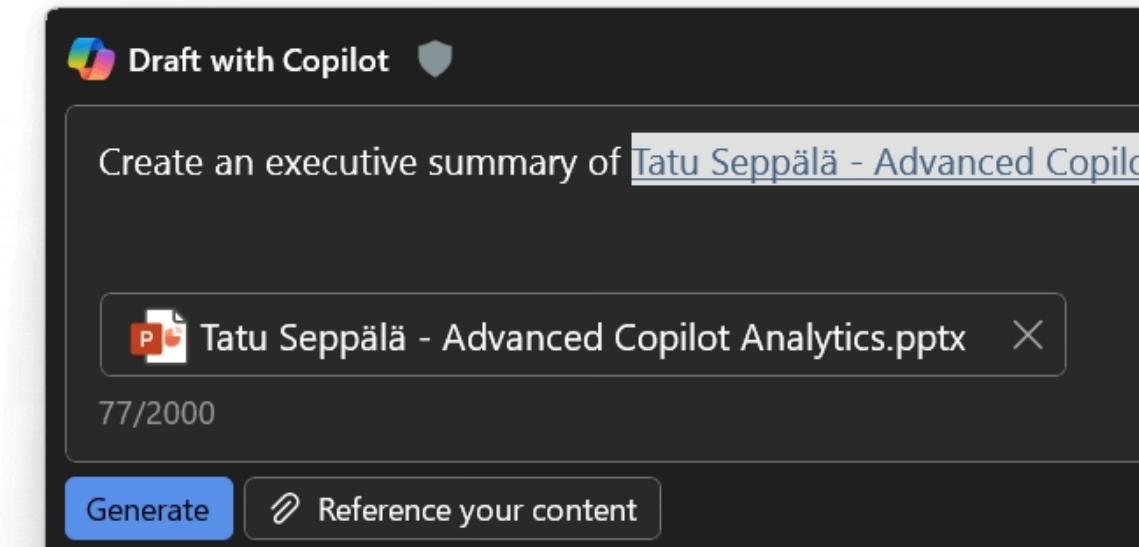
 Whiteboard

 Word



AccessedResources

- › Tells us which emails, files and website URLs were referenced during the Copilot interaction
- › There's also information of the sensitivity label of referenced content



Messages

- › Each **CopilotInteraction** event captures a single **interaction thread**
- › Metadata (not the text itself!) on each user prompt and Copilot reply in the thread is saved separately under the **Messages** attribute

 **Copilot interaction thread**
AuditData.Id = 13491c61-0149-400-9363-147cd48f55ab

 **isPrompt = TRUE**
MessageId = 1720074774700
Hey Copilot! Why is  so awesome?

 **isPrompt = FALSE**
MessageId = 1720074774701
The  is awesome because it brings together tech professionals from around the world for inclusive, innovative learning and networking opportunities.





Copilot interaction thread

AuditData.Id = 13491c61-0149-400-9363-



MESSAGES

isPrompt = TRUE
MessageId = 1720074774700

Hey Copilot! Why is  so awesome?



isPrompt = FALSE
MessageId = 1720074774701

The  is awesome because it brings together tech professionals from around the world for inclusive, innovative learning and networking opportunities.

What other metadata is available?

- 🧠 AI model name (ModelTransparencyDetails)
- 🔌 Plugins used in BizChat interactions
- 🏷️ The sensitivity label a BizChat interaction inherited from referenced docs
- 🌐 Public IP address & region of the client
- 📁 The context the Copilot interaction took place in (open document, Teams Chat or Meeting etc.)



How to get CopilotInteraction events

⚡ Immediate

- > Advanced Hunting & Log Analytics
 - Table: CloudAppEvents
 - ActionType: CopilotInteraction
 - ⚠️ Requires Defender for Cloud Apps
- > Search-UnifiedAuditLog
(Security & Compliance PowerShell)



⌚ Asynchronous

- > Audit Search ([Purview Portal](#))
- > Audit Search ([Graph API](#))
- > O365 Management Activity API



Getting the audit logs



Purview Audit Search

Solutions

Audit

Search

Policies

Related solutions

eDiscovery

Information Protection

Data Loss Prevention

AI Hub (preview)

Insider Risk Management...

Search

Searches completed: 1 | Active searches: 0 | Active unfiltered searches: 0

Date and time range (UTC) *

Start: May 00:00 | End: Oct 00:00

Activities - friendly names

Interacted with Copilot

Activities - operation names

Enter operation values, separate...

Keyword Search

Enter the keyword to search for

Admin Units

Choose which Admin Units...

Record Types

Select the record types to search for

Search name

Give the search a name

ⓘ Search results might be impacted by audit log retention policies. Activities that happened over 180 days ago will only show up in results for users who have licensing for long-term audit log retention.

Users

Add the users whose audit logs you want to search for

File, folder, or site

Enter all or a part of the name of a file, folder, or site

Workloads

Enter the workloads to search for

Search



Audit Search CSV export has it's limits, too..

E3 and below:

Up to ~50 000 rows with Audit Standard



E5 & E5/F5 Compliance:

Up to ~500 000 rows with Audit Premium



Entra ID metadata



Entra ID
metadata



Entra ID is the source of HR metadata

Home > Users >

Odin Allfather

User

Search

Edit properties Delete Refresh Reset password Revoke sessions

Overview Audit logs Sign-in logs Diagnose and solve problems Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments

Overview Monitoring Properties

Basic info



Odin Allfather
odin@Seppala365Dev.onmicrosoft.com
Member

User principal name	odin@Seppala365Dev.onmicrosoft.com
Object ID	b59e860b-7c1d-43f3-a7a6-a9b1d931a2c6
Created date time	Jul 11, 2024, 11:45 AM
User type	Member
Identities	Seppala365Dev.onmicrosoft.com



Entra ID is the source of HR metadata

Home > Users > Odin Allfather >

Odin Allfather

...

X

Properties

Refresh

Got feedback?

Showing 9 results under "Job Information"

Job title

Chief Executive Officer

Company name

Asgard Enterprises

Department

Leadership

Employee ID

ODIN1337

Employee type

Full-time

Employee hire date

Thu Feb 02 1961



Office location

Valhalla, Asgard



Grab a report of Entra ID member users

Home >

 **Users** ...
Seppala365

« + New user Delete Download users Bulk operations Refresh ...

 All users (i) Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

 Audit logs

 Sign-in logs

 Diagnose and solve problems

 Deleted users

 Password reset

 User settings

 Bulk operation results

 New support request

User type == Member X Add filter

4 users found

<input type="checkbox"/>	Display name ↑	User principal name ↑	User type
<input type="checkbox"/>	 ADM Tatu Seppälä	adm-tatu@Seppala365De...	 Member
<input type="checkbox"/>	 HR	HR@Seppala365Dev.onm...	 Member
<input type="checkbox"/>	 Odin Allfather	odin@Seppala365Dev.on...	 Member
<input type="checkbox"/>	 Tatu Seppälä	tatu@Seppala365Dev.on...	 Member



Grab a report of Entra ID member users

Home >

Users

Seppala365

Search

[+ New user](#) [Delete](#) [Download users](#) [Bulk operations](#)

[Azure Active Directory is now Microsoft Entra ID](#)

Search User type == Member

4 users found

<input type="checkbox"/>	Display name ↑	User principal
<input type="checkbox"/>	ADM Tatu Seppälä	adm-tatu@Seppala365.onmicrosoft.com
<input type="checkbox"/>	HR	HR@Seppala365.onmicrosoft.com
<input type="checkbox"/>	Odin Allfather	odin@Seppala365.onmicrosoft.com
<input type="checkbox"/>	Tatu Seppälä	tatu@Seppala365.onmicrosoft.com

Download users

⚠ Please be aware of the bulk operations service limitations before using this feature. Operations can only run for up to 1 hour and has known issues in large tenants. [Click here to learn more.](#)

File name * .CSV

Start download

[Learn more about download users](#)



Grab a report of Entra ID member users

Home >

Users

Seppala365

Search

[New user](#) [Delete](#) [Download users](#) [Bulk operations](#)

[All users](#) (i) Azure Active Directory is now Microsoft Entra ID)

Search User type == Member

4 users found

<input type="checkbox"/>	Display name ↑	User principal
<input type="checkbox"/>	ADM Tatu Seppälä	adm-tatu@Seppala365
<input type="checkbox"/>	HR	HR@Seppala365
<input type="checkbox"/>	Odin Allfather	odin@Seppala365
<input type="checkbox"/>	Tatu Seppälä	tatu@Seppala365

Download users

⚠ Please be aware of the bulk operations service limitations before using this feature. Operations can only run for up to 1 hour and has known issues in large tenants. [Click here to learn more.](#)

File name: exportUsers_2024-10-16 .csv

[Start download](#)

Succeeded

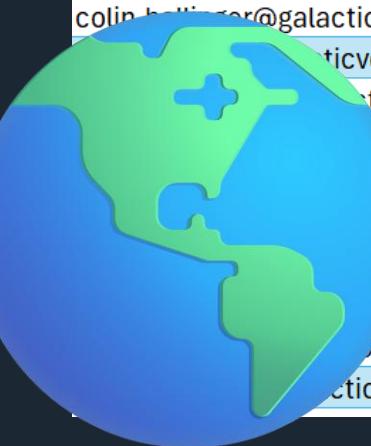
File is ready! [Click here to download](#)

ℹ Click here to view the status of each operation



Grab a report of Entra ID member users

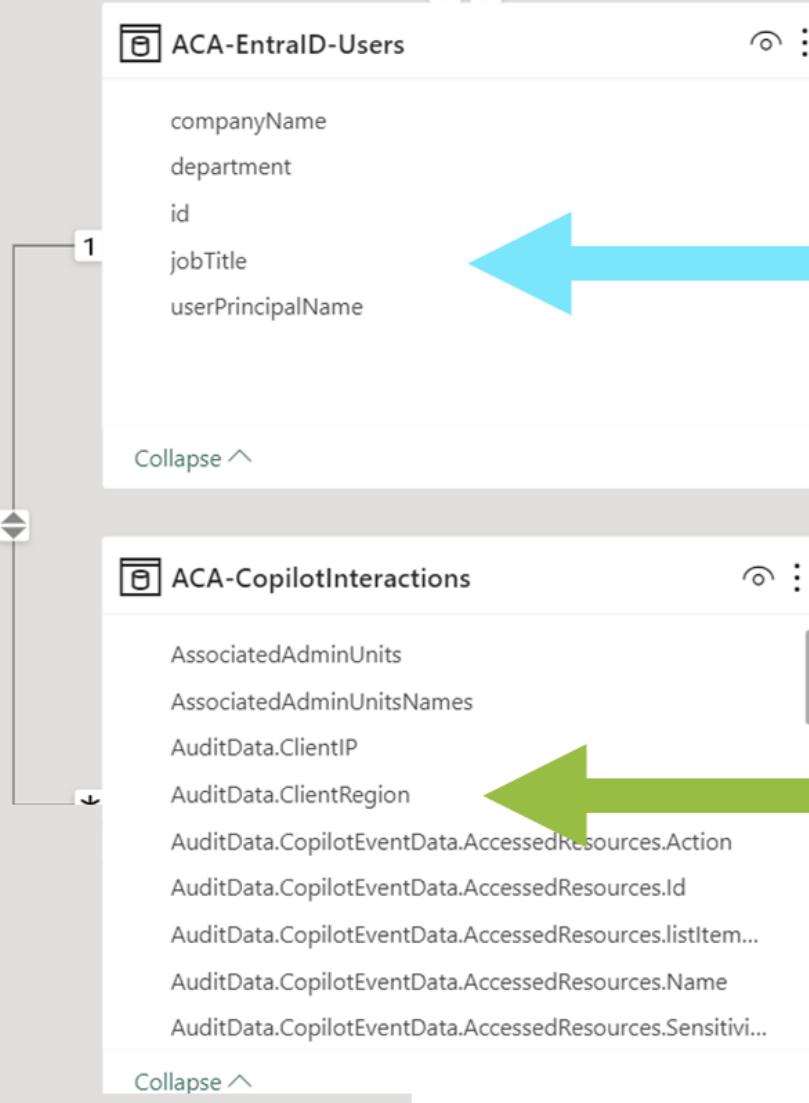
userPrincipalName	id	jobTitle	department	Galaxy
adele.vance@galacticvoyages.com	0215a438-1da2-4b88-9d65-95a108b65d25	Cargo Handler	Cargo Management	Galactic Voyages Freight
alex.wilber@galacticvoyages.com	026cf76-e8c0-4a41-b3ce-3596c7986a50	Cargo Handler	Cargo Management	Galactic Voyages Freight
allan.deyoung@galacticvoyages.com	04a18dad-5fc4-45d7-b67a-2ca2c57eeb6c	Cargo Handler	Cargo Management	Galactic Voyages Freight
amanda.brady@galacticvoyages.com	04fa3cdc-5122-42af-942e-bc0c81a46e51	Cargo Handler	Cargo Management	Galactic Voyages Freight
amir.rahimi@galacticvoyages.com	055ce9db-9738-403d-b13a-535946736f4c	Space Freight Coordinator	Cargo Management	Galactic Voyages Freight
ana.trujillo@galacticvoyages.com	057be55a-1e9b-4016-9e56-6cafc3819a49	Space Freight Coordinator	Cargo Management	Galactic Voyages Freight
andy.fitzgerald@galacticvoyages.com	0630b2dd-86b7-4ef6-8af4-d19402a99deb	Space Freight Coordinator	Cargo Management	Galactic Voyages Freight
arvind.kumar@galacticvoyages.com	068baa65-0d1b-4953-a0f3-3397c2c8cb20	Space Freight Coordinator	Cargo Management	Galactic Voyages Freight
ashley.martin@galacticvoyages.com	06f8050c-9c19-4224-8132-4946cdd54bc1	Cargo Operations Assistant	Cargo Management	Galactic Voyages Freight
ben.walters@galacticvoyages.com	0714a63e-d7b1-4805-af81-ecdd8390897b	Cargo Operations Assistant	Cargo Management	Galactic Voyages Freight
beth.melton@galacticvoyages.com	0aaa3ea9-579b-44e8-8060-f25368be16dc	Cargo Handler	Cargo Management	Galactic Voyages Freight
carlos.slattery@galacticvoyages.com	0b3ba966-080e-4052-8ec6-ea535695ed2b	Cargo Handler	Cargo Management	Galactic Voyages Freight
cecil.folk@galacticvoyages.com	0d1d39bd-7e64-49de-a597-d84435eb25e7	Interstellar Load Specialist	Cargo Management	Galactic Voyages Freight
christie.kline@galacticvoyages.com	0d964c8e-6870-4d12-b5f6-c876133937d9	Interstellar Load Specialist	Cargo Management	Galactic Voyages Freight
claudia.lu@galacticvoyages.com	0d9b51f5-03ec-4509-809d-c421f6310dce	Space Route Planner	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	0dafa86b-abff-4eb7-b0fe-762353268f65	Space Route Planner	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	0f8e3eb0-73fb-4ae9-a8db-c4eaadf445aa	Space Route Planner	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	0fe9d756-b119-4301-871c-654353a1a172	Space Route Planner	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	10672165-5bb8-4c76-9a26-4fc48d4d143b	Galactic Navigation Assistant	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	11c00080-b15e-427e-b0be-188ae5a7498b	Orbital Path Coordinator	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	129d3836-fc41-4dbf-82ff-825479dc6048	Spaceway Scheduler	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	12a05ed1-bc83-445a-a296-8a6b3cbc60b7	Spaceway Scheduler	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	14b170a0-b14b-4672-92e2-1f9430d54925	Spaceway Scheduler	Route Planning	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	16456818-405c-4f9d-84d1-db5d9bec1113	Spacecraft Technician	Fleet Maintenance	Galactic Voyages Freight
colin.hallinan@galacticvoyages.com	16b261c7-a6d0-4a5c-9686-8638562fb3b3	Spacecraft Technician	Fleet Maintenance	Galactic Voyages Freight



Bring the ingredients
together!



Add the ingredients to the stew in Power BI Desktop



Entra ID
users



M365 Copilot
events



Create 1:* relationship between tables

Imagine you have a  school with **one teacher** and **many students**.

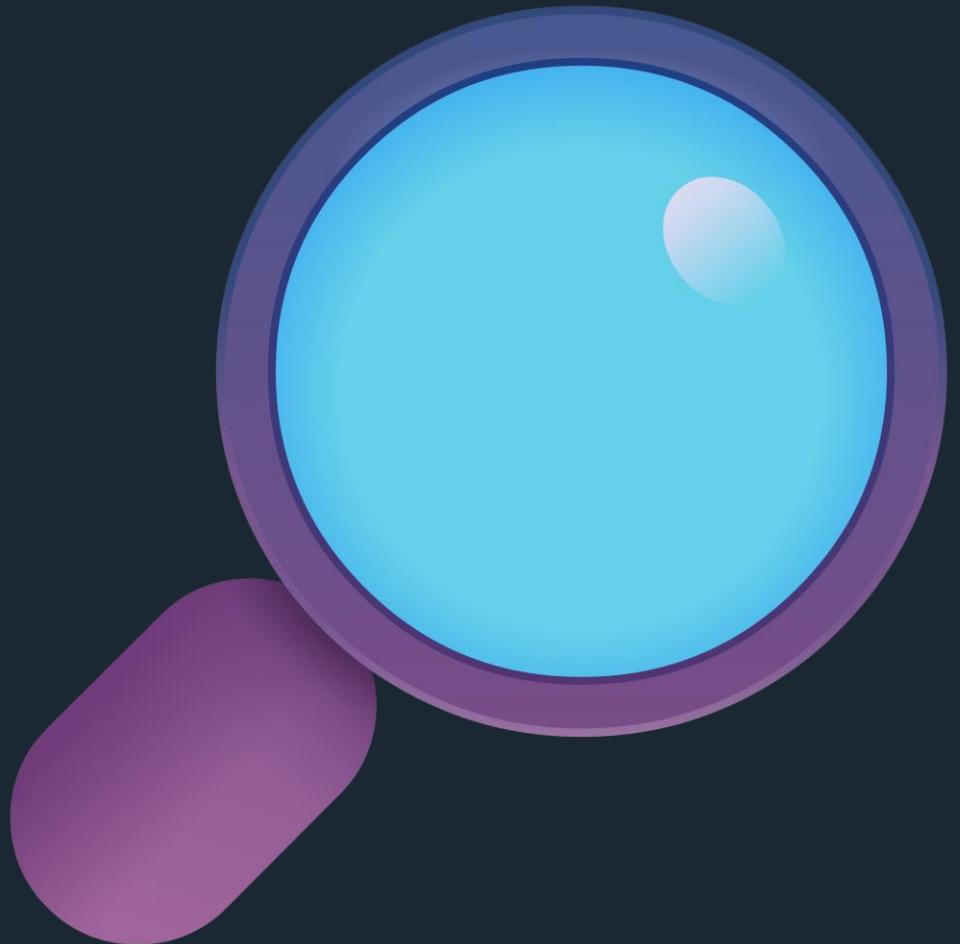
The teacher is like the "1"

The students are like the "*".

Each student has only one teacher, but the teacher has many students.

<p>Cardinality</p> <p>One to many (1:*)</p> <p><input checked="" type="checkbox"/> Make this relationship active</p> <p><input type="checkbox"/> Assume referential integrity</p>	<p>Cross filter direction</p> <p>Single</p> <p><input type="checkbox"/> Apply security filter in both directions</p>
---	--

Analyze & take action



Copilot adopter: Galactic Voyages



Copilot adopter: Galactic Voyages

~360 employees



100% M365 Copilot licensed
since **January 2024**

Handles interstellar shipping,
logistics and luxury travel



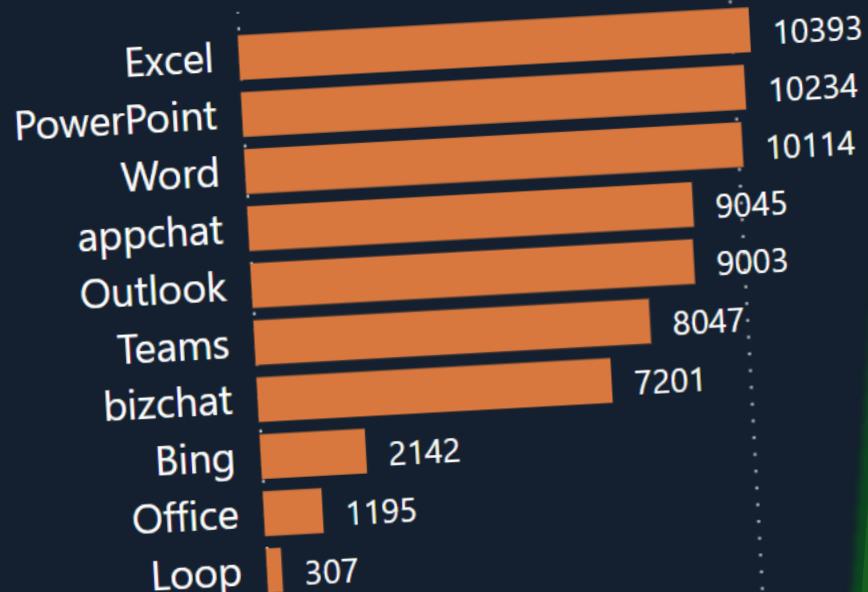
Power BI!



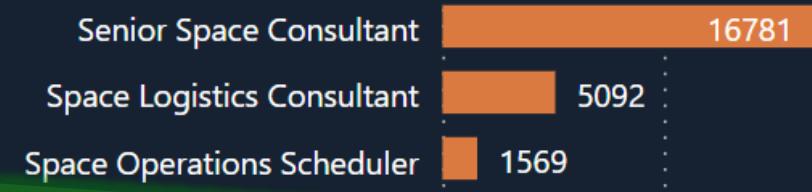
Build some tasty visuals..



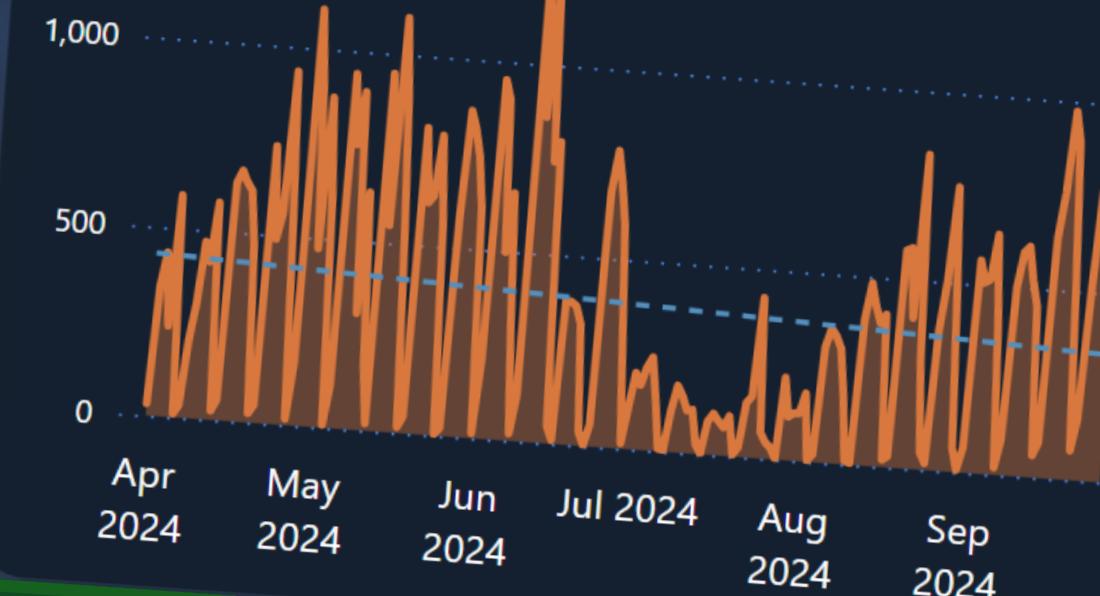
Copilot threads by type



User prompts by job title

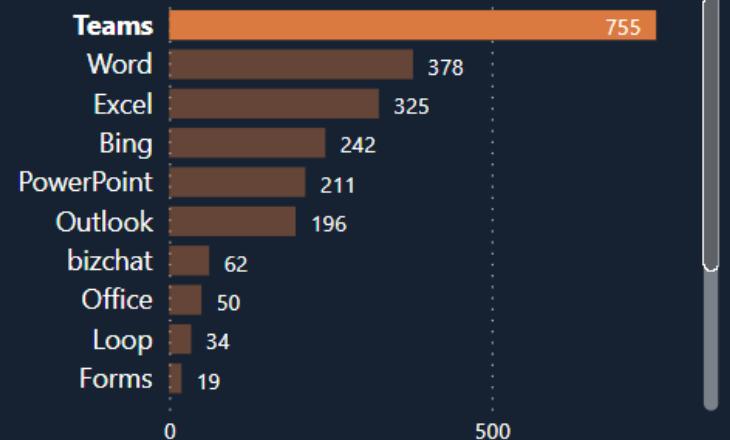


Copilot threads over time



..and cross-filter!

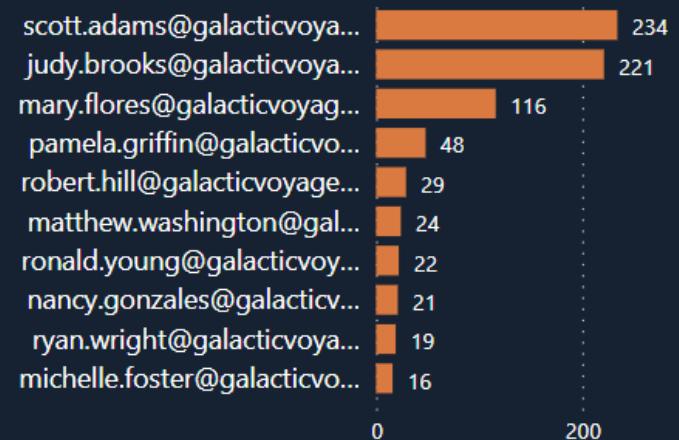
User prompts by copilot type



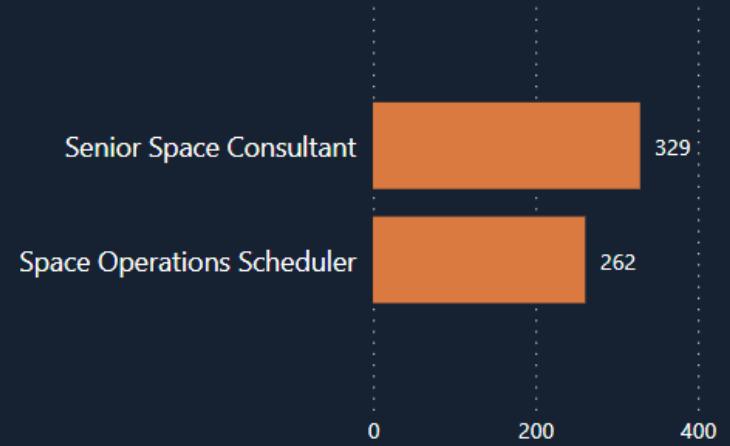
User prompts by department



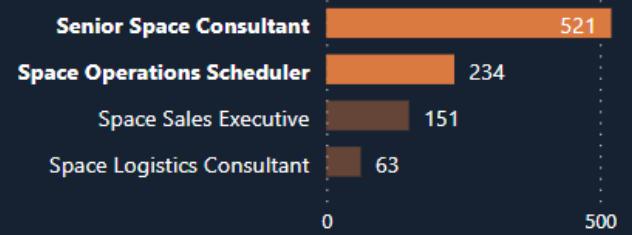
User prompts by UPN



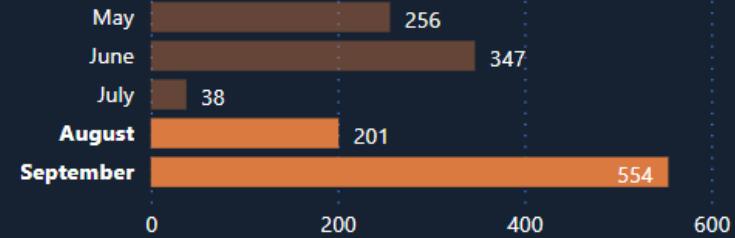
Average prompts per user in role



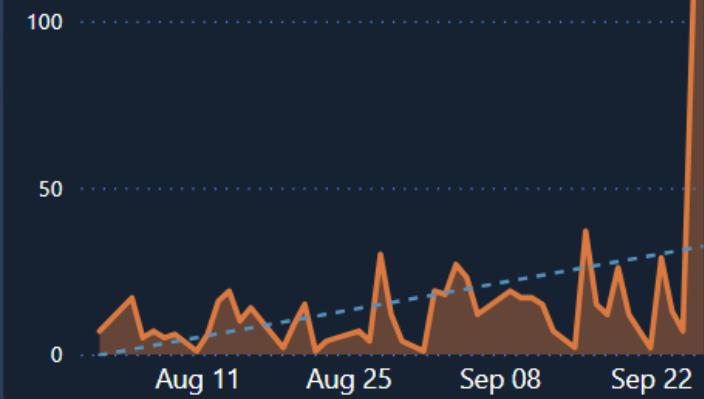
User prompts by job title



User prompts per month



User prompts over time



Add some custom tables for unique insights

```
1 AveragePromptsPerUser =  
2 VAR CurrentJobTitle = 'ACA-UserPromptsPerJobTitle'[jobTitle]  
3 RETURN  
4     MEDIANX(  
5         FILTER(  
6             'ACA-UserPromptsPerJobTitle',  
7             'ACA-UserPromptsPerJobTitle'[jobTitle] = CurrentJobTitle  
8         ),  
9         'ACA-UserPromptsPerJobTitle'[TotalUserPrompts] /  
'ACA-UserPromptsPerJobTitle'[UniqueUsers]
```

Collapse ^

ACA-UserPromptsPerJobTitle

⋮

AveragePromptsPerUser

jobTitle

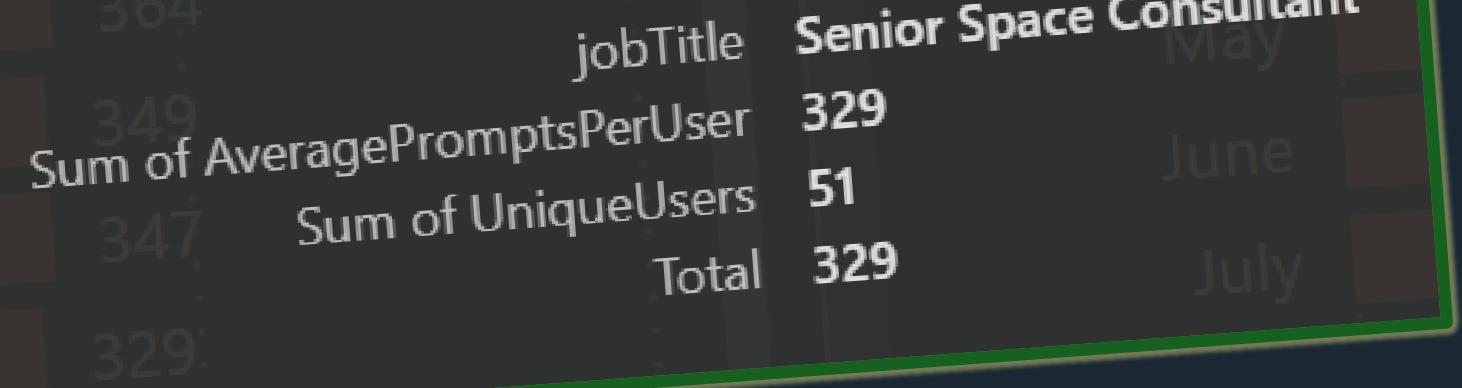
Σ TotalUserPrompts

Σ UniqueUsers

Collapse ^

✍ Average prompts per user in role

Galactic Account Navigator	929
Chief Space Technology Of...	904
President of Space AI and ...	874
Lead Space Systems Archit...	767
Galactic Operations Coord...	609
Space Guest Relations Assi...	491
Space Flight Attendant	465
Principal Space Consultant	

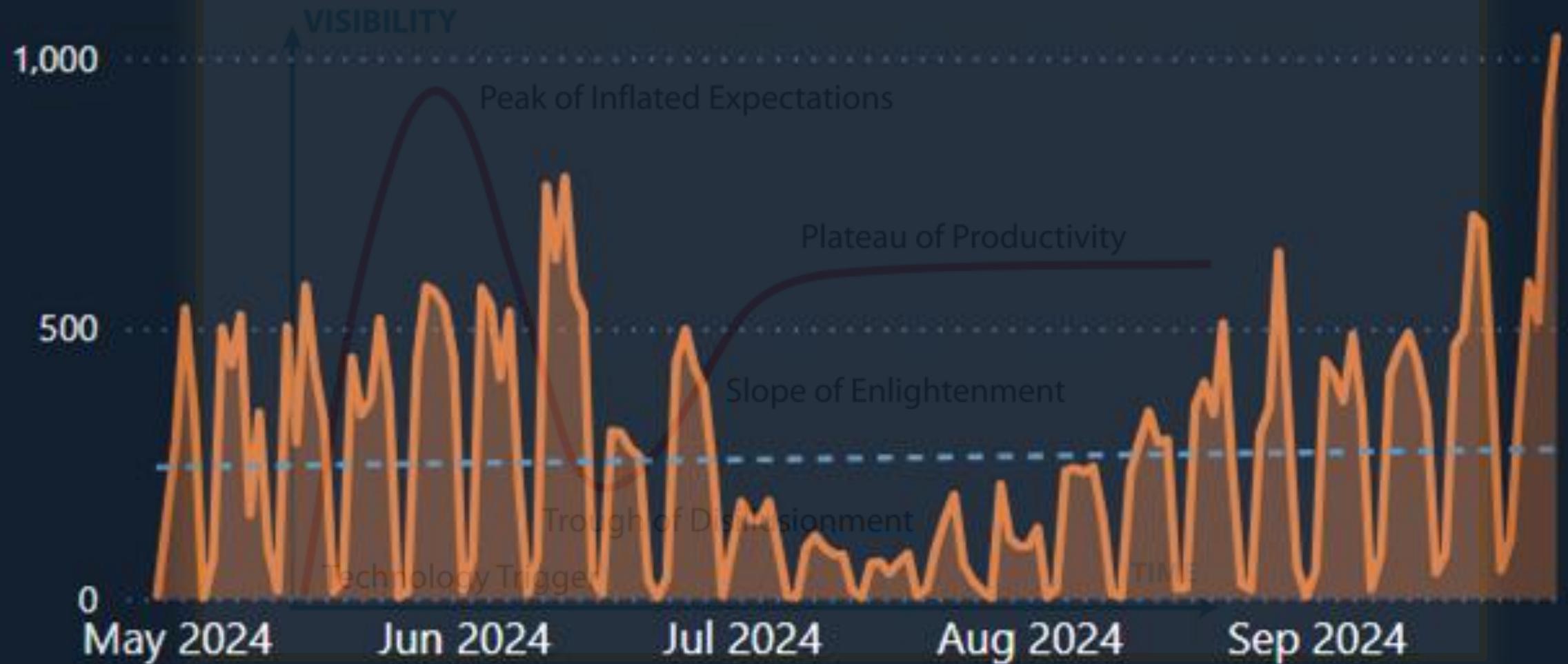


Disclaimer: I'm a Power BI newbie - you can optimize the DAX queries far better for scale!



⌚ User prompts over time

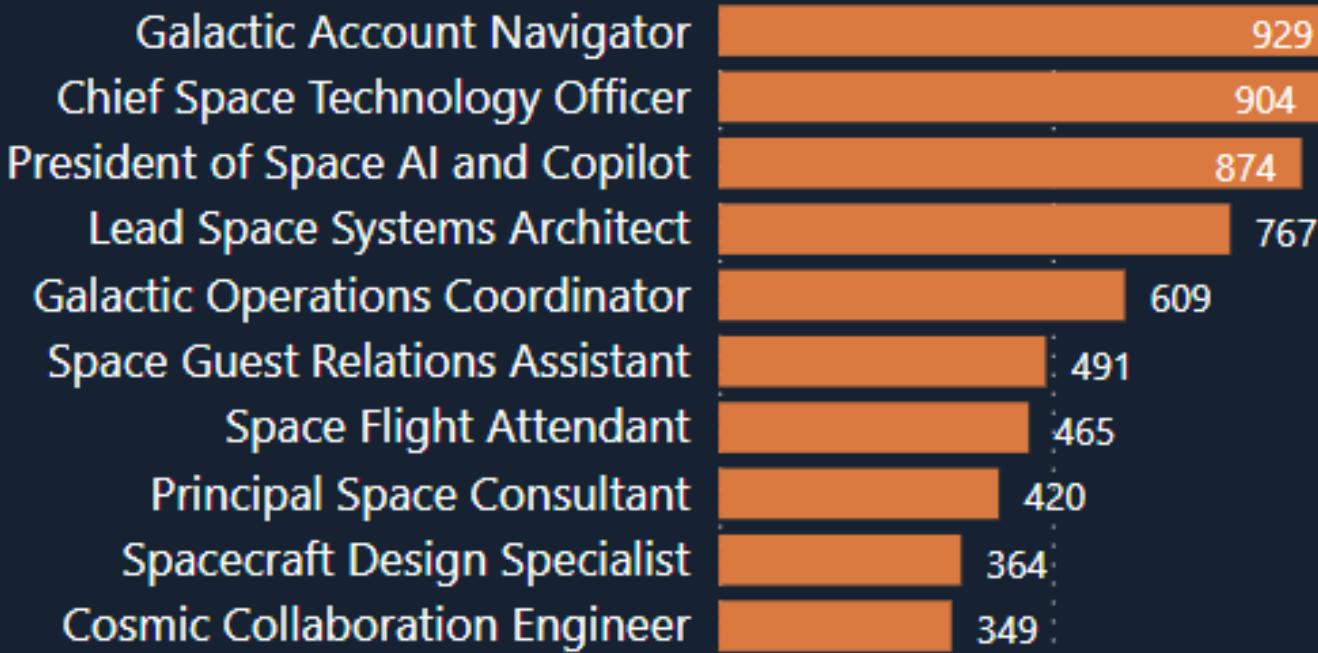
Gartner Hype Cycle



Identify roles with high *average* usage..



Average prompts per user in role

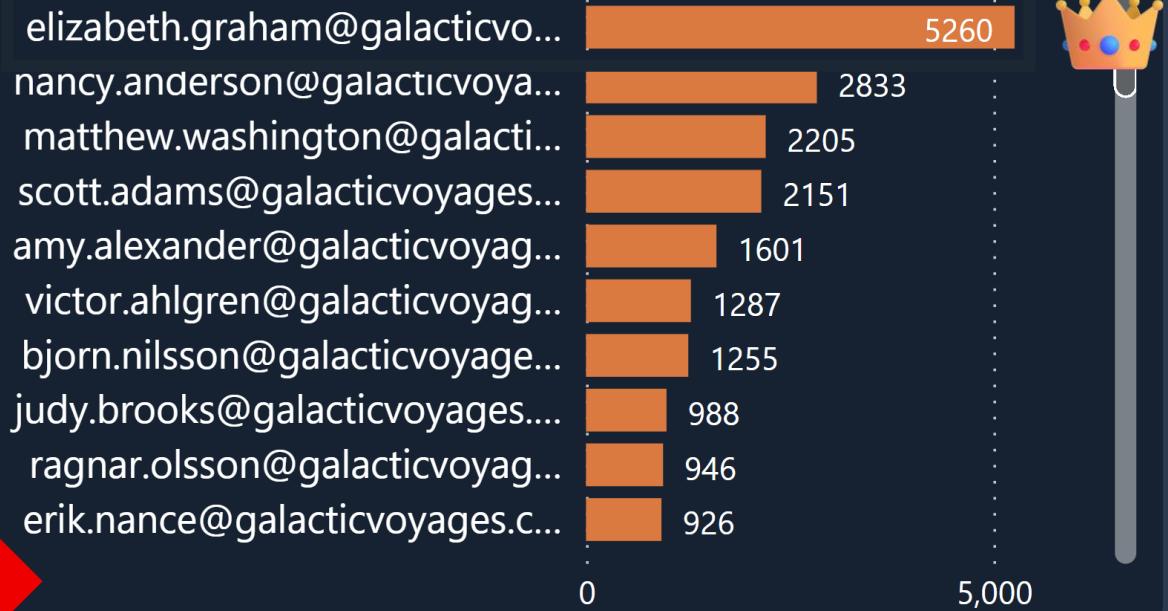


..and then discover the **pioneers!**

💬 Average Copilot threads per user in role



👤 Copilot threads by UPN



Discover the pioneers!

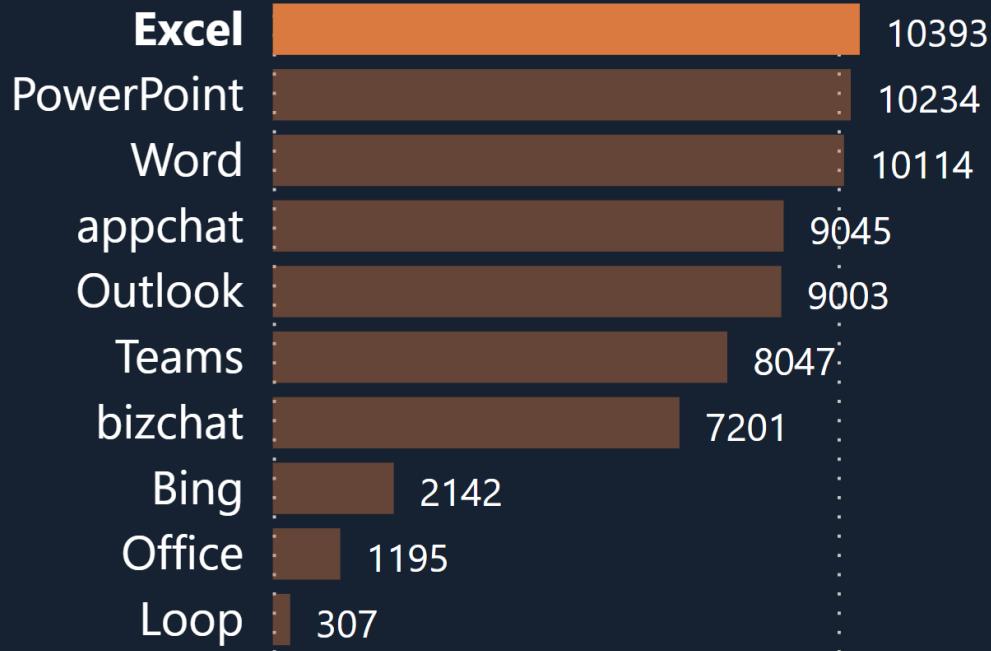
- › There is usually a significant gap in Copilot use between..
 - The **top 3-5** individuals
 - The bottom **~30-40%** of users within any given job / role
- › Recruit top users within roles for your adoption efforts
- › Have pioneers share their use cases and methods with others



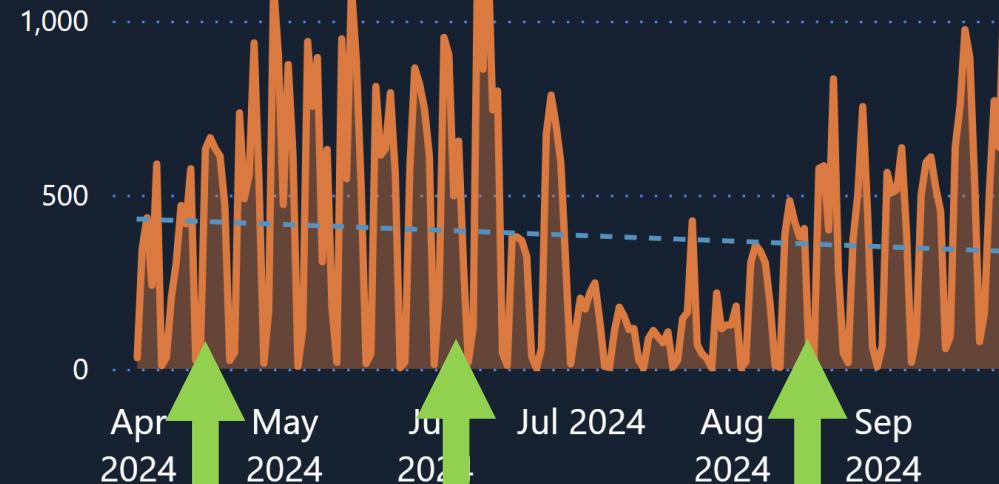
Monitor the impact of trainings



Copilot threads by type



Copilot threads over time



For E5: Configure audit retention policy

Record Type

CopilotInteraction



Activities

Interacted with Copilot



If no activities are selected, then this policy will apply to all activities for the selected record types.

Duration *

Choose how long to retain logs that match this policy's conditions before they're automatically deleted. [Learn more about licensing](#)

1 Year



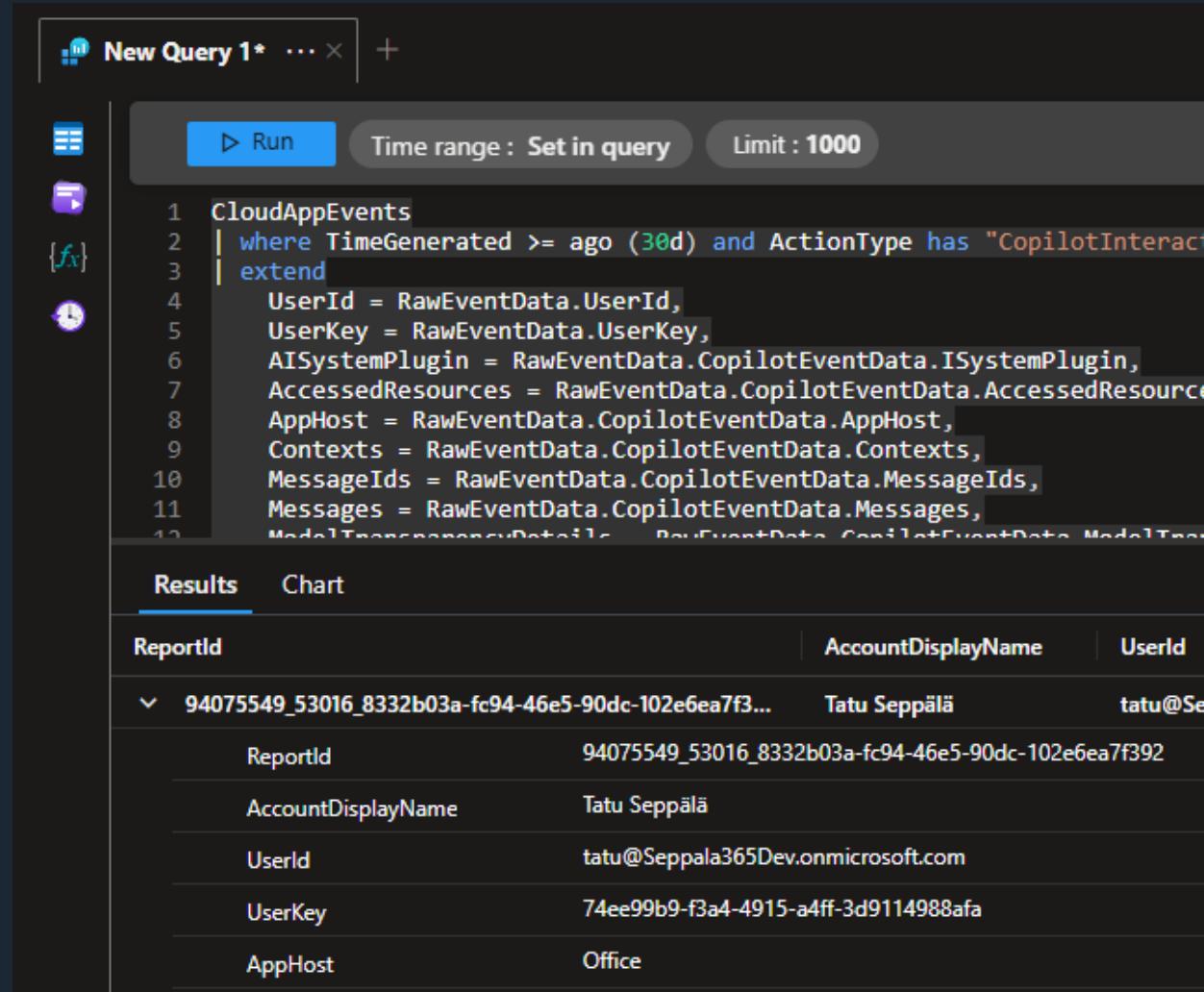
Automate fetching
CopilotInteraction events



Directly from Sentinel's Log Analytics workspace

Prerequisites:

- E5/E5 Security or similar licensing
- Defender for Cloud Apps (MDA) deployed & connected to M365 Unified Audit Log
- Defender XDR connector ingesting events from MDA to CloudAppEvents



The screenshot shows the Microsoft Sentinel Log Analytics workspace. A query is being run in a new query window. The query is as follows:

```
1 CloudAppEvents
2 | where TimeGenerated >= ago (30d) and ActionType has "CopilotInteraction"
3 | extend
4     UserId = RawEventData.UserId,
5     UserKey = RawEventData.UserKey,
6     AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
7     AccessedResources = RawEventData.CopilotEventData.AccessedResources,
8     AppHost = RawEventData.CopilotEventData.AppHost,
9     Contexts = RawEventData.CopilotEventData.Contexts,
10    MessageIds = RawEventData.CopilotEventData.MessageIds,
11    Messages = RawEventData.CopilotEventData.Messages,
12    ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails
```

The results table shows the following data:

ReportId	AccountDisplayName	UserId
94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com
ReportId	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392	
AccountDisplayName	Tatu Seppälä	
UserId	tatu@Seppala365Dev.onmicrosoft.com	
UserKey	74ee99b9-f3a4-4915-a4ff-3d9114988afa	
AppHost	Office	

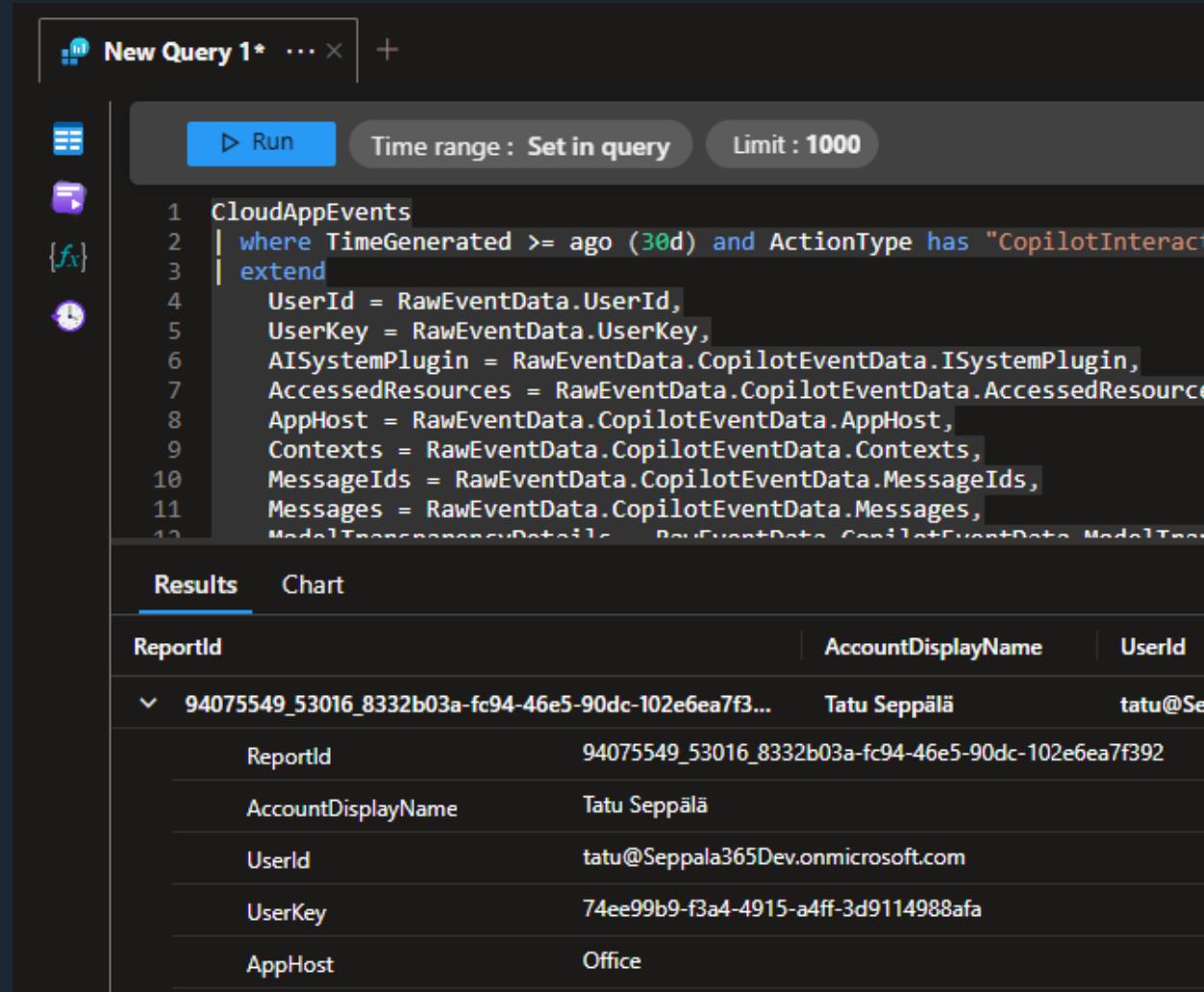
✨ Recommended method ✨



Directly from Sentinel's Log Analytics workspace

Benefits:

- ✓ Fetch up to 500,000 **CopilotInteraction** events programmatically to Power BI
- ✓ Only fetch the attributes you need
- ✓ Granular summarization also supported
- ✓ Setting up the prerequisites is a win for your security team too!



The screenshot shows a Log Analytics workspace with a query editor and a results table.

Query Editor:

```
1 CloudAppEvents
2 | where TimeGenerated >= ago (30d) and ActionType has "CopilotInteraction"
3 | extend
4     UserId = RawEventData.UserId,
5     UserKey = RawEventData.UserKey,
6     AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
7     AccessedResources = RawEventData.CopilotEventData.AccessedResources,
8     AppHost = RawEventData.CopilotEventData.AppHost,
9     Contexts = RawEventData.CopilotEventData.Contexts,
10    MessageIds = RawEventData.CopilotEventData.MessageIds,
11    Messages = RawEventData.CopilotEventData.Messages,
12    ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails
```

Results Table:

ReportId	AccountDisplayName	UserId
94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com
ReportId	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392	
AccountDisplayName	Tatu Seppälä	
UserId	tatu@Seppala365Dev.onmicrosoft.com	
UserKey	74ee99b9-f3a4-4915-a4ff-3d9114988afa	
AppHost	Office	

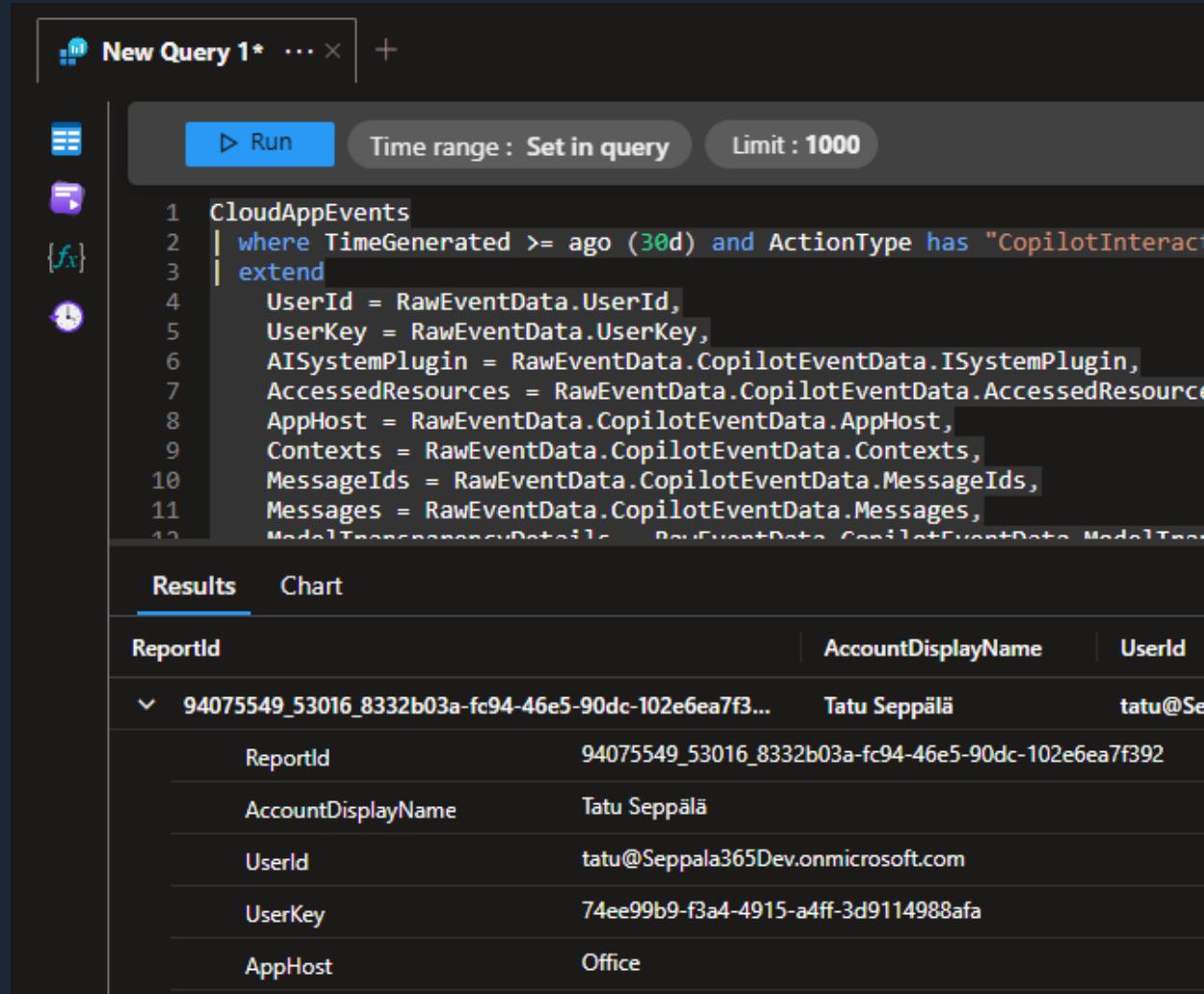
⭐ Recommended method ⭐



Directly from Sentinel's Log Analytics workspace

Limitations:

- More than 500,000 record queries not supported by API
- Queries running for >10 minutes not supported by API



The screenshot shows the Log Analytics workspace interface. At the top, there is a query bar with the text "New Query 1* ... x +". Below the bar are icons for file, copy, and refresh. The main area contains a query editor with the following code:

```
1 CloudAppEvents
2 | where TimeGenerated >= ago (30d) and ActionType has "CopilotInteraction"
3 | extend
4     UserId = RawEventData.UserId,
5     UserKey = RawEventData.UserKey,
6     AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
7     AccessedResources = RawEventData.CopilotEventData.AccessedResources,
8     AppHost = RawEventData.CopilotEventData.AppHost,
9     Contexts = RawEventData.CopilotEventData.Contexts,
10    MessageIds = RawEventData.CopilotEventData.MessageIds,
11    Messages = RawEventData.CopilotEventData.Messages,
12    ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails
```

Below the query editor, there are tabs for "Results" and "Chart". The "Results" tab is selected, showing a table with the following data:

ReportId	AccountDisplayName	UserId
94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com
ReportId	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392	
AccountDisplayName	Tatu Seppälä	
UserId	tatu@Seppala365Dev.onmicrosoft.com	
UserKey	74ee99b9-f3a4-4915-a4ff-3d9114988afa	
AppHost	Office	

✨ Recommended method ✨





Delete data

Connected apps**App Connectors**

Conditional Access App Control apps

Information Protection

Admin quarantine

Microsoft Information Protection

Files

Conditional Access App Control

General Settings

User monitoring

Device identification

App onboarding/maintenance

App Connectors

App connectors provide you with greater visibility and control over your cloud apps.



Filters:

 Advanced filtersApp: **Select apps**App category: **Select category**Connected by: **Select users**[+ Connect an app](#)

Hide filters



Table settings

App

Status

Was co...

Last ac...

Acc... ▾



Microsoft 365

Collaboration



...

Nov 4, 2024...

Dec 2, 2024...

342



Microsoft Azure

Cloud computing platform



...

Jun 14, 202...

Dec 2, 2024...

8



 **Select Microsoft 365 components** Great, Microsoft 365 is connected

Select Microsoft 365 components

Connect as Microsoft 365 administrator to gain full visibility and control.

 To connect this app, provide your access credentials. We secure your data as described in the [privacy statement](#) | [Terms](#)

- Microsoft Entra Users and groups 
- Microsoft Entra ID Management events 
- Microsoft Entra ID Sign-in events 
- Microsoft Entra ID Apps 
- Microsoft 365 activities 

Microsoft 365 files 

Enable file monitoring before enabling Office 365 files.

Connect Microsoft 365

Cancel



Microsoft Sentinel | Content hub



Selected workspace: 'la-seppala365dev'



Search



Install/Update



Delete



SIEM Migration



Guides & Feedback

> General

> Threat management

Content management

Content hub

Repositories (Preview)

Community

> Configuration

368

Solutions

307

Standalone contents

14

Installed

7

Updates

Defender XDR



Status : All

Content type : All

Support : All

Provider : All

Category : All

Content source



Content title

Status

Content source



Log4j Vulnerability Det...

FEATURED

 Not installed

Solution



Microsoft Defender XDR

FEATURED

 Installed

Updates

Solution



Business Email Compromise - Financ...

 Not installed

Solution



Endpoint Threat Protection Essentials

 Not installed

Solution



Legacy IOC based Threat Protection

 Not installed

Solution



Microsoft Defender XDR

Microsoft Provider

Microsoft Support

3.0.8

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Microsoft Defender XDR solution for Microsoft Sentinel enables you to ingest Security Alerts/Incidents and raw logs from the products within Microsoft Defender XDR suite into Microsoft Sentinel.

Additional Hunting Queries to support proactive and reactive hunting for the Microsoft Defender XDR solution can be found



Microsoft Defender XDR

...

X



Microsoft Defender XDR

Connected Status

Microsoft Provider

49 minutes ago
Last Log Received

Description

Microsoft Defender XDR is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft Defender XDR suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alerts
- Microsoft Defender Vulnerability Management
- Microsoft Purview Data Loss Prevention
- Microsoft Entra ID Protection

When turning on Incidents synchronization **Microsoft Defender for Cloud** Incidents are automatically synced to Sentinel at a tenant level. To match all alerts that may appear in incidents, turn

i Note: Office 365 data does not necessarily reside in the region where your Microsoft Sentinel workspace is located. Office 365 data may therefore cross regional boundaries when being ingested to Sentinel.

Instructions

Microsoft Defender for Cloud Apps (1/1 connected)

<input checked="" type="checkbox"/> Name	Description
--	-------------

<input checked="" type="checkbox"/> CloudAppEvents	Events involving accounts and objects in Office...
--	--

Microsoft Defender for Identity (0/3 connected)



la-seppala365dev | Logs

Log Analytics workspace

New Query 1* ⋮ +

Save ⋮ Share ⋮ ⋮ | Queries hub

Run

Time range: Set in query

Limit: 1000

KQL mode

```
1 CloudAppEvents
2 | where TimeGenerated >= ago(30d) and ActionType has "CopilotInteraction"
3 | extend
4     UserId = RawEventData.UserId,
5     UserKey = RawEventData.UserKey,
6     AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
7     AccessedResources = RawEventData.CopilotEventData.AccessedResources,
8     AppHost = RawEventData.CopilotEventData.AppHost,
9     Contexts = RawEventData.CopilotEventData.Contexts,
10    MessageIds = RawEventData.CopilotEventData.MessageIds,
11    Messages = RawEventData.CopilotEventData.Messages,
12    ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails,
13    ThreadId = RawEventData.CopilotEventData.ThreadId,
14    CopilotLogVersion = RawEventData.CopilotLogVersion
15 | project
16     ReportId,
17     AccountDisplayName,
18     UserId,
19     UserKey,
20     AppHost,
21     AccessedResources,
22
23     Contexts,
24     ThreadId,
25     MessageIds,
26     Messages,
27     AISystemPlugin,
28     ModelTransparencyDetails,
29     Application,
30     ApplicationId,
31     CopilotLogVersion
32
```

Results

Chart

ReportId	AccountDisplayName	UserId	UserKey	AppHost	AccessedResources	Contexts	ThreadId	MessageIds
94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f3...	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.co...	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:3XC_Cnpk05e-hhjfgEHO/bgZN8JULAsWi44ub6RA5M1...	[]
ReportId	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392							
AccountDisplayName	Tatu Seppälä							
UserId	tatu@Seppala365Dev.onmicrosoft.com							
UserKey	74ee99b9-f3a4-4915-a4ff-3d9114988afa							
AppHost	Office							
AccessedResources	[]							



New Query 1* ... +Run Time range: Set in query Limit: 1000

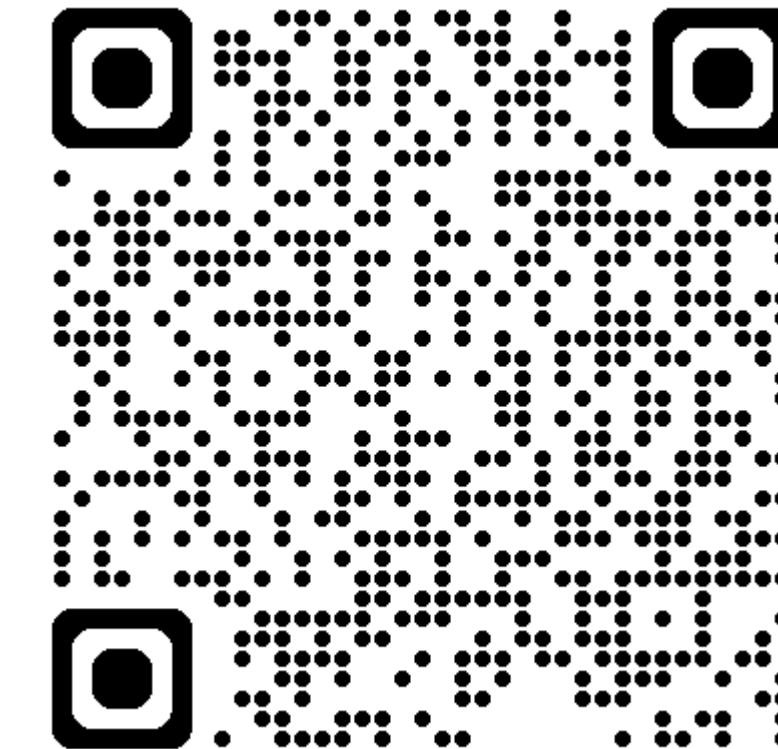
```
1 CloudAppEvents
2 | where TimeGenerated >= ago(30d) and ActionType has "CopilotInteraction"
3 | extend
4     UserId = RawEventData.UserId,
5     UserKey = RawEventData.UserKey,
6     AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin
7     AccessedResources = RawEventData.CopilotEventData.AccessedResources
8     AppHost = RawEventData.CopilotEventData.AppHost,
9     Contexts = RawEventData.CopilotEventData.Contexts,
10    MessageIds = RawEventData.CopilotEventData.MessageIds,
11    Messages = RawEventData.CopilotEventData.Messages,
12    ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails
13    ThreadId = RawEventData.CopilotEventData.ThreadId,
14    CopilotLogVersion = RawEventData.CopilotLogVersion
15 | project
16     ReportId,
17     AccountDisplayName,
18     UserId,
19     UserKey,
20     AppHost,
21     AccessedResources,
22
23     Contexts,
24     ThreadId,
25     MessageIds,
26     Messages,
27     AISystemPlugin,
28     ModelTransparencyDetails,
29     Application,
30     ApplicationId,
31     CopilotLogVersion
32
```

Results Chart

ReportId	AccountDisplayName
94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f3...	Tatu Seppälä
ReportId	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f3...
AccountDisplayName	Tatu Seppälä
UserId	tatu@Seppala365Dev.onmicrosoft.com
UserKey	74ee99b9-f3a4-4915-a4ff-3d9114988afa
AppHost	Office
AccessedResources	[]



Grab the query from GitHub!



Contexts	ThreadId	MessageId	Column
[]	19:3XC_Cnpk05e-hhjfgEHO/bgZN8JULAsWi44ub6RA5M1...	[]	

la-seppala365dev | Logs



Log Analytics workspace

New Query 1* ... +

Save Share ... | Queries hub

Run

Time range : Set in query

Limit : 1000

KQL mode

```
1 CloudAppEvents
2 | where TimeGenerated >= ago (30d) and ActionType has "CopilotInteraction"
3 | extend
4     UserId = RawEventData.UserId,
5     UserKey = RawEventData.UserKey,
6     AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
7     AccessedResources = RawEventData.CopilotEventData.AccessedResources,
8     AppHost = RawEventData.CopilotEventData.AppHost,
9     Contexts = RawEventData.CopilotEventData.Contexts,
10    MessageIds = RawEventData.CopilotEventData.MessageIds,
11    Messages = RawEventData.CopilotEventData.Messages,
12    ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails
```

Results

Chart



ReportId	AccountDisplayName	UserId	UserKey	AppHost	AccessedResources	Contexts	ThreadId	MessageId
94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f3...	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.co...	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:3XC_Cnpk05e-hhjfgEHOJbgZN8JULAAswi44ub6RA5M1...	[]
ReportId	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392							
AccountDisplayName	Tatu Seppälä							
UserId	tatu@Seppala365Dev.onmicrosoft.com							
UserKey	74ee99b9-f3a4-4915-a4ff-3d9114988afa							
AppHost	Office							
AccessedResources	[]							
Contexts	[]							
ThreadId	19:3XC_Cnpk05e-hhjfgEHOJbgZN8JULAAswi44ub6RA5M1@thread.v2							
MessageIds	[]							
Messages	[{"Id": "1731951250164", "isPrompt": true}, {"Id": "1731951250361", "isPrompt": false}]							
ModelTransparencyDetails	[{"ModelName": "DEEP_LEO"}]							
Application	Microsoft Copilot for Microsoft 365							
ApplicationId	53016							
CopilotLogVersion	1.0.0.0							
94075549_53016_16febb1-84d9-4363-95c4-290d50a13e1	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tKSMu1aZwM1...	[]
94075549_53016_16febb1-84d9-4363-95c4-290d50a13e1	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tKSMu1aZwM1...	[]
94075549_53016_8ah0dde-5b2f-4ed8-a953-0145a4b4cdf8	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tKSMu1aZwM1...	[]



la-seppala365dev | Logs



New Query 1* ... +

Save

Run

Time range : Set in query

Limit : 1000

```
1 CloudAppEvents
2 | where TimeGenerated >= ago (30d) and ActionType has "CopilotInteraction"
3 | extend
4     UserId = RawEventData.UserId,
5     UserKey = RawEventData.UserKey,
6     AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
7     AccessedResources = RawEventData.CopilotEventData.AccessedResources,
8     AppHost = RawEventData.CopilotEventData.AppHost,
9     Contexts = RawEventData.CopilotEventData.Contexts,
10    MessageIds = RawEventData.CopilotEventData.MessageIds,
11    Messages = RawEventData.CopilotEventData.Messages,
12    ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails
```

- Share
- Copy link to query
- Copy query text
- Copy results
- Export to CSV (all columns)
- Export to CSV (displayed columns)
- Export to Power BI (as an M query)
- Export to Power BI (new Dataset)
- Open in Excel

Results

Chart

ReportId	AccountDisplayName	UserId	UserKey	AppHost	AccessedResources	Contexts	ThreadId	MessageId
94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f3...	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.co...	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:3XC_Cnpk05e-hhjfgEHOJbgZN8JULAAswi44ub6RA5M1...	[]
ReportId	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392							
AccountDisplayName	Tatu Seppälä							
UserId	tatu@Seppala365Dev.onmicrosoft.com							
UserKey	74ee99b9-f3a4-4915-a4ff-3d9114988afa							
AppHost	Office							
AccessedResources	[]							
Contexts	[]							
ThreadId	19:3XC_Cnpk05e-hhjfgEHOJbgZN8JULAAswi44ub6RA5M1@thread.v2							
MessageId	[]							
Messages	[{"Id": "1731951250164", "isPrompt": true}, {"Id": "1731951250361", "isPrompt": false}]							
ModelTransparencyDetails	[{"ModelName": "DEEP_LEO"}]							
Application	Microsoft Copilot for Microsoft 365							
ApplicationId	53016							
CopilotLogVersion	1.0.0.0							
94075549_53016_16fefbb1-84d9-4363-95c4-290d50a13e1e	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSH	Greenshot
94075549_53016_16fefbb1-84d9-4363-95c4-290d50a13e1e	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSH	Greenshot
94075549_53016_8ab0ddea-5b2f-4ed8-a953-0145a4b4cdf8	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSH	Exported to: Save as (displaying dialog)



Greenshot
Exported to: Save as (displaying dialog)



la-seppala365dev | Logs

Log Analytics workspace

New Query 1* ... +

```
1 CloudAppEvents
2 | where TimeGenerated >
3 | extend
4   UserId = RawEventData.UserId
5   UserKey = RawEventData.UserKey
6   AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin
7   AccessedResources = RawEventData.CopilotEventData.AccessedResources
8   AppHost = RawEventData.CopilotEventData.AppHost
9   Contexts = RawEventData.CopilotEventData.Contexts
10  MessageIds = RawEventData.CopilotEventData.MessageIds
11  Messages = RawEventData.CopilotEventData.Messages
12  ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails
13  ThreadId = RawEventData.CopilotEventData.ThreadId
14  CopilotLogVersion = RawEventData.CopilotLogVersion
```

Results

ReportId

94075549_53016_8332b03a-fc94-4c4a-8...

ReportId

AccountDisplayName

UserId

UserKey

AppHost

AccessedResources

Contexts

ThreadId

MessageIds

Messages

ModelTransparencyDetails

Application

ApplicationId

CopilotLogVersion

```
1 /*
2  The exported Power Query Formula Language (M Language ) can be used with Power Query in Excel
3  and Power BI Desktop.
4  For Power BI Desktop follow the instructions below:
5  1) Download Power BI Desktop from https://powerbi.microsoft.com/desktop/
6  2) In Power BI Desktop select: 'Get Data' -> 'Blank Query'->'Advanced Query Editor'
7  3) Paste the M Language script into the Advanced Query Editor and select 'Done'
8 */
9
10 let AnalyticsQuery =
11 let Source =
12 Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/2e4366f9-b7d7-460d-bc18-37e2819f3f6c/query",
13 [Query=[#"query"="CloudAppEvents
14 | where TimeGenerated >=ago (30d) and ActionType has ""CopilotInteraction""
15 | extend UserId = RawEventData.UserId,
16   UserKey = RawEventData.UserKey,
17   AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
18   AccessedResources = RawEventData.CopilotEventData.AccessedResources,
19   AppHost = RawEventData.CopilotEventData.AppHost,
20   Contexts = RawEventData.CopilotEventData.Contexts,
21   MessageIds = RawEventData.CopilotEventData.MessageIds,
22   Messages = RawEventData.CopilotEventData.Messages,
23   ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails,
24   ThreadId = RawEventData.CopilotEventData.ThreadId,
25   CopilotLogVersion = RawEventData.CopilotLogVersion
26 | project ReportId, AccountDisplayName, UserId, UserKey, AppHost, AccessedResources, Contexts, ThreadId, MessageIds, ModelTransparencyDetails, ThreadId, CopilotLogVersion"])))
```

Normal text file length: 2 359 lines: 49 Ln: 1 Col: 1 Pos: 1 Windows (CR LF) UTF-8 INS

> 94075549_53016_16fefbb1-84d9-4363-95c4-290d50a13e1e	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	0	0	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tKSMu1aZwM1...	0
> 94075549_53016_16fefbb1-84d9-4363-95c4-290d50a13e1e	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	0	0	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tKSMu1aZwM1...	0
> 94075549_53016_8ab0ddea-5b2f-4ed8-a953-0145a4b4cdf8	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	0	0	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tKSMu1aZwM1...	0



File Home Help



Get data



Refresh



Manage relationships



New measure



New column



New

Common data sources

Excel workbook

Power BI datasets

Dataflows

Dataverse

SQL Server

Analysis Services

Text/CSV

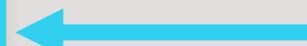
Web

OData feed

Blank query

Power BI Template Apps

More...



Untitled - Power Query Editor

The screenshot shows the ribbon of the Power Query Editor. The 'Advanced Editor' button, located in the 'Query' section of the ribbon, is highlighted with a yellow box and a blue arrow pointing to it. The ribbon tabs include File, Home, Transform, Add Column, View, Tools, and Help. The 'Query' tab is selected. The 'Advanced Editor' button is part of a group that also includes 'Properties' and 'Refresh Preview'. Other buttons in the 'Query' group include 'Choose Columns', 'Remove Columns', 'Keep Rows', 'Remove Rows', 'Reduce Rows', and 'Sort'. The 'Data Type' dropdown is set to 'Any'. The 'Advanced Editor' button is described as 'Manage' with a dropdown arrow.

File Home Transform Add Column View Tools Help

Close & Apply New Source Recent Sources Enter Data Data source settings Manage Parameters Refresh Preview Advanced Editor Properties Manage Choose Columns Remove Columns Keep Rows Remove Rows Reduce Rows Sort Data Type: Any Use First Row as Headers 1 2 Replace Values Close New Query Data Sources Parameters Query Transform

Queries [1]

A^B C Query1

Untitled - Power Query Editor

File Home Transform Add Column View Tools Help

Close & Apply New Source Recent Sources Enter Data Data source settings Manage Parameters Refresh Preview Advanced Editor Choose Columns Remove Columns Keep Rows Remove Rows Data Type: Any Split Column Group By Use First Row as Headers Merge Queries Text Analytics Append Queries Combine Files Azure Machine Learning

Close New Query Data Sources Parameters Queries [1] Advanced Editor

Query1

Advanced Editor

Query1

```
let
    Source = ""
in
    Source
```

No syntax errors have been detected.

Display Options ? Done Cancel

Query Settings

PROPERTIES

Name: Query1

All Properties

APPLIED STEPS

Source

8365

Untitled - Power Query Editor

File Home Transform Add Column View Tools Help

Close & Apply New Source Recent Sources Enter Data Data source settings Manage Parameters Refresh Preview Advanced Editor Choose Columns Remove Columns Keep Rows Remove Rows Data Type: Any Split Column Group By Use First Row as Headers Merge Queries Text Analytics Append Queries Combine Files Azure Machine Learning

Close New Query Data Sources Parameters Queries [1] Advanced Editor

Query1

Advanced Editor

Query1

Display Options ?

```
/*
The exported Power Query Formula Language (M Language ) can be used with Power Query in Excel
and Power BI Desktop.
For Power BI Desktop follow the instructions below:
1) Download Power BI Desktop from https://powerbi.microsoft.com/desktop/
2) In Power BI Desktop select: 'Get Data' -> 'Blank Query'->'Advanced Query Editor'
3) Paste the M Language script into the Advanced Query Editor and select 'Done'
*/
```

```
let AnalyticsQuery =
let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/2e4366f9-b7d7-460d-bc18-37e2819f3f6c/query",
[Query=[#"query"="CloudAppEvents
| where TimeGenerated >=ago (30d) and ActionType has ""CopilotInteraction""
| extend UserId = RawEventData.UserId,
UserKey = RawEventData.UserKey,
AISystemPlugin = RawEventData.CopilotEventData.ISystemPlugin,
AccessedResources = RawEventData.CopilotEventData.AccessedResources,
AppHost = RawEventData.CopilotEventData.AppHost,
Contexts = RawEventData.CopilotEventData.Contexts,
MessageIds = RawEventData.CopilotEventData.MessageIds,
Messages = RawEventData.CopilotEventData.Messages,
ModelTransparencyDetails = RawEventData.CopilotEventData.ModelTransparencyDetails,
ThreadId = RawEventData.CopilotEventData.ThreadId,
CopilotLogVersion = RawEventData.CopilotLogVersion
| project ReportId, AccountDisplayName, UserId, UserKey, AppHost, AccessedResources, Contexts, ThreadId, MessageIds, Messages, AISystemPlugin
",#"x-ms-app"="OmsAnalyticsPBI",#"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 }.
```

✓ No syntax errors have been detected.

Done Cancel

Query Settings

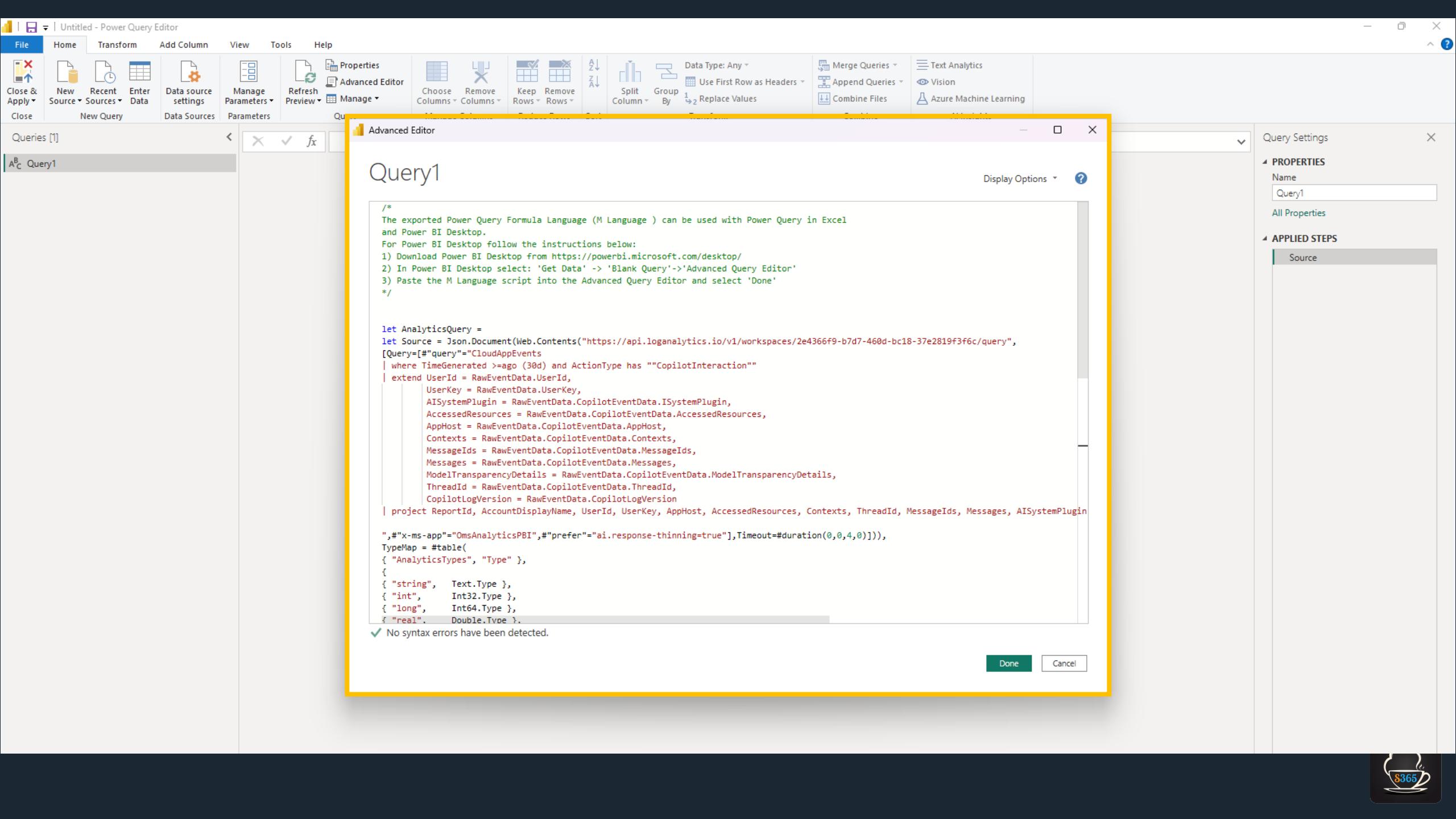
PROPERTIES

Name: Query1

All Properties

APPLIED STEPS

Source



Untitled - Power Query Editor

File Home Transform Add Column View Tools Help

Close & Apply Close New Source Recent Enter Data Data source settings Manage Parameters Refresh Preview Advanced Editor Choose Columns Remove Columns Keep Rows Remove Rows Split Column Group By Use First Row as Headers Sort Replace Values Merge Queries Append Queries Combine Files Text Analytics Vision Azure Machine Learning AI Insights

Queries

fx = let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/2e4366f9-b7d7-460d-bc18-37e2819f3f6c/query",

	ReportId	AccountDisplayName	UserId	UserKey	AppHost	AccessedResources	Contexts	ThreadId
1	94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f...	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:3XC_Cnpk05e-hhjfgEHOJbgZN8JULAA5Wi4
2	94075549_53016_16fefbb1-84d9-4363-95c4-290d50a1...	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tk
3	94075549_53016_16fefbb1-84d9-4363-95c4-290d50a1...	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tk
4	94075549_53016_8ab0dde-a5b2f-4ed8-a953-0145a4b4...	Tatu Seppälä	tatu@Seppala365Dev.onmicrosoft.com	74ee99b9-f3a4-4915-a4ff-3d9114988afa	Office	[]	[]	19:F4DZqSHMfpWZ6iY-tuOTqntxeUPFtFIG3tk

Query Settings

PROPERTIES

Name: Query1

All Properties

APPLIED STEPS

AnalyticsQuery

94075549_53016_8332b03a-fc94-46e5-90dc-102e6ea7f392

8365

Alternate method: Graph API audit log search

Audit log query (preview)

Microsoft Purview Audit provides an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.



Grant Graph API permissions to a Logic Apps managed identity (or register an application)

AuditLogsQuery.Read.All **Required permission**

- ✓ Application permission supported
- ✓ Delegated permission supported

✨ Recommendation ✨

Use a Logic App with a system-assigned managed identity and authorize it to run Audit Log searches directly against Graph API

For guidance on authorizing a managed identity to Graph API, see for example:

<https://laurakokkarinen.com/authenticate-to-entra-id-protected-apis-with-managed-identity-no-key-vault-required/>



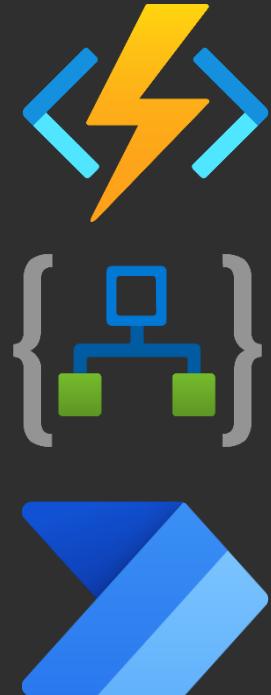
Create auditLogQuery

HTTP

```
POST https://graph.microsoft.com/beta/security/auditLog/queries  
Content-Type: application/json
```

```
{  
  "@odata.type": "#microsoft.graph.security.auditLogQuery",  
  "displayName": "String",  
  "filterStartTime": "String (timestamp)",  
  "filterEndTime": "String (timestamp)",  
  "recordTypeFilters": [  
    "String"  
  ],  
  "keywordFilter": "String",  
  "serviceFilter": "String",  
  "operationFilters": [  
    "String"  
  ],  
  "userPrincipalNameFilters": [  
    "String"  
  ],  
  "ipAddressFilters": [  
    "String"  
  ],  
  "objectIdFilters": [  
    "String"  
  ],  
  "administrativeUnitIdFilters": [  
    "String"  
  ],  
  "status": "String"  
}
```

Copy



HTTP request

HTTP

```
POST /security/auditLog/queries
```

Copy

"operationFilters": [
 "**CopilotInteraction**"
]



Get results of auditLogQuery

HTTP request

HTTP

Copy

```
GET /security/auditLog/queries/{auditLogQueryId}
```



Periodically check
status until
 **complete**

HTTP request

HTTP

Copy

```
GET /security/auditLog/queries/{auditLogQueryId}/records
```



Get results of auditLogQuery



HTTP request

HTTP

```
GET /security/auditLog/queries/{auditLogQueryId}/records
```

Copy

HTTP

HTTP/1.1 200 OK

Content-Type: application/json

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.auditLogRecord",
      "id": "40706737-7eca-f9a1-97a5-dedd3260e24a",
      "createdDateTime": "String (timestamp)",
      "auditLogRecordType": "String",
      "operation": "String",
      "organizationId": "String",
      "userType": "String",
      "userId": "String",
      "service": "String",
      "objectId": "String",
      "userPrincipalName": "String",
      "clientIp": "String",
      "administrativeUnits": [
        "String"
      ],
      "auditData": {
        "@odata.type": "microsoft.graph.security.auditData"
      }
    }
  ]
}
```



Automate fetching CopilotInteraction events



The Graph API method: Query the Users endpoint

List users

Article • 10/21/2024 • 24 contributors

In this article

Permissions

HTTP request

Optional query parameters

Request headers

Show 3 more

Namespace: [microsoft.graph](#)

Retrieve a list of [user](#) objects.

msgraph

 Copy

 Try It

GET <https://graph.microsoft.com/v1.0/users>

HTTP

 Copy

HTTP/1.1 200 OK
`Content-type: application/json`

```
{  
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users",  
  "value": [  
    {  
      "businessPhones": [],  
      "displayName": "Conf Room Adams",  
      "givenName": null,  
      "jobTitle": null,  
      "mail": "Adams@contoso.com",  
      "mobilePhone": null,  
      "officeLocation": null,  
      "preferredLanguage": null,  
      "surname": null,  
      "userPrincipalName": "Adams@contoso.com",  
      "id": "00000000-0000-0000-0000-000000000000"  
    }  
  ]  
}
```



The Graph API method: Query the Users endpoint



Power BI intentionally restricts direct queries to Graph API

Connecting to Microsoft Graph REST APIs  from Power Query isn't recommended or supported. Instead, we recommend users explore alternative solutions for retrieving analytics data based on Graph, such as Microsoft Graph data connect.

[Lack of Support for Microsoft Graph in Power Query -
Power Query | Microsoft Learn](#)



The Graph API method: Query the Users endpoint

⚙️ Steps:

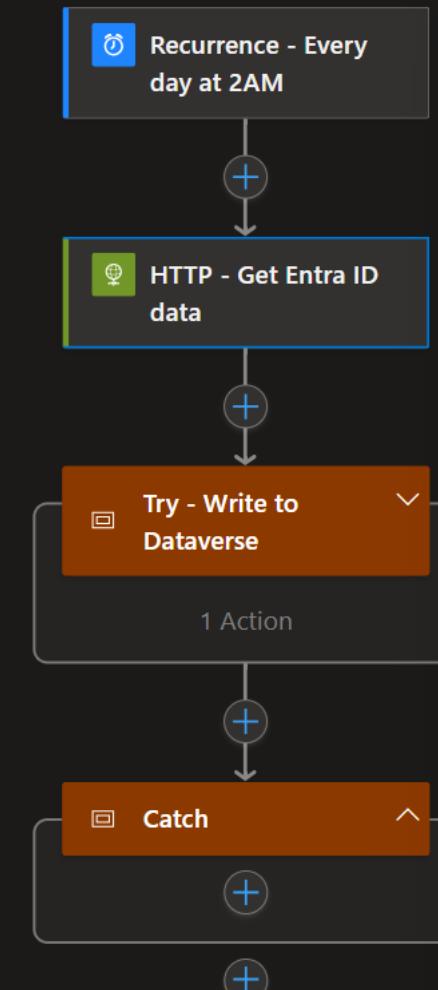
1. Provision a **Logic App** with a system-assigned managed identity
2. Use the method detailed earlier to give it **User.Read.All** rights
3. Have the Logic App use HTTP queries to fetch recurring user reports from Graph API
4. Save only the required information from the user records into a dedicated, access-controlled table in Dataverse / Azure SQL / etc.



la-CopilotAnalytics-GetEntraIDUsers ...



Run Save Discard Parameters Code view Errors Info File a bug



» HTTP - Get Entra ID data

Parameters Settings Code view Testing About

URI *

`https://graph.microsoft.com/v1.0/users`

Method *

GET

Headers

Enter key Enter value

Authentication

Authentication Type *

Managed identity

Managed Identity *

System-assigned managed identity

Audience

`https://graph.microsoft.com`

Runs history

la-CopilotAnalytics-GetEntralIDUsers

Refresh

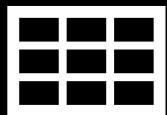
All

Pick a date  Pick a time

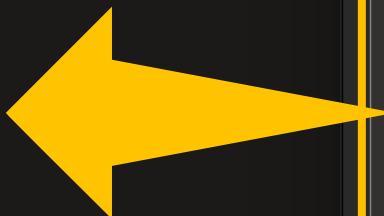
Search to filter items by identifier

Start time Duration

- 12/3/2024, 8:54 AM 407 Milliseconds
- 12/3/2024, 8:45 AM 187 Milliseconds



EntralIDUsers



la-CopilotAnalytics-GetEntralIDUsers

Run details Resubmit Cancel run Refresh Info File a bug

HTTP

Submit from this action

Parameters Settings Code view About

Show more

OUTPUTS

Show raw outputs 

Body

```
{  
  "businessPhones": [],  
  "displayName": "Odin Allfather",  
  "givenName": null,  
  "jobTitle": "Chief Executive Officer",  
  "mail": null,  
  "mobilePhone": null,  
  "officeLocation": "Valhalla, Asgard",  
  "preferredLanguage": null,  
  "surname": null,  
}
```

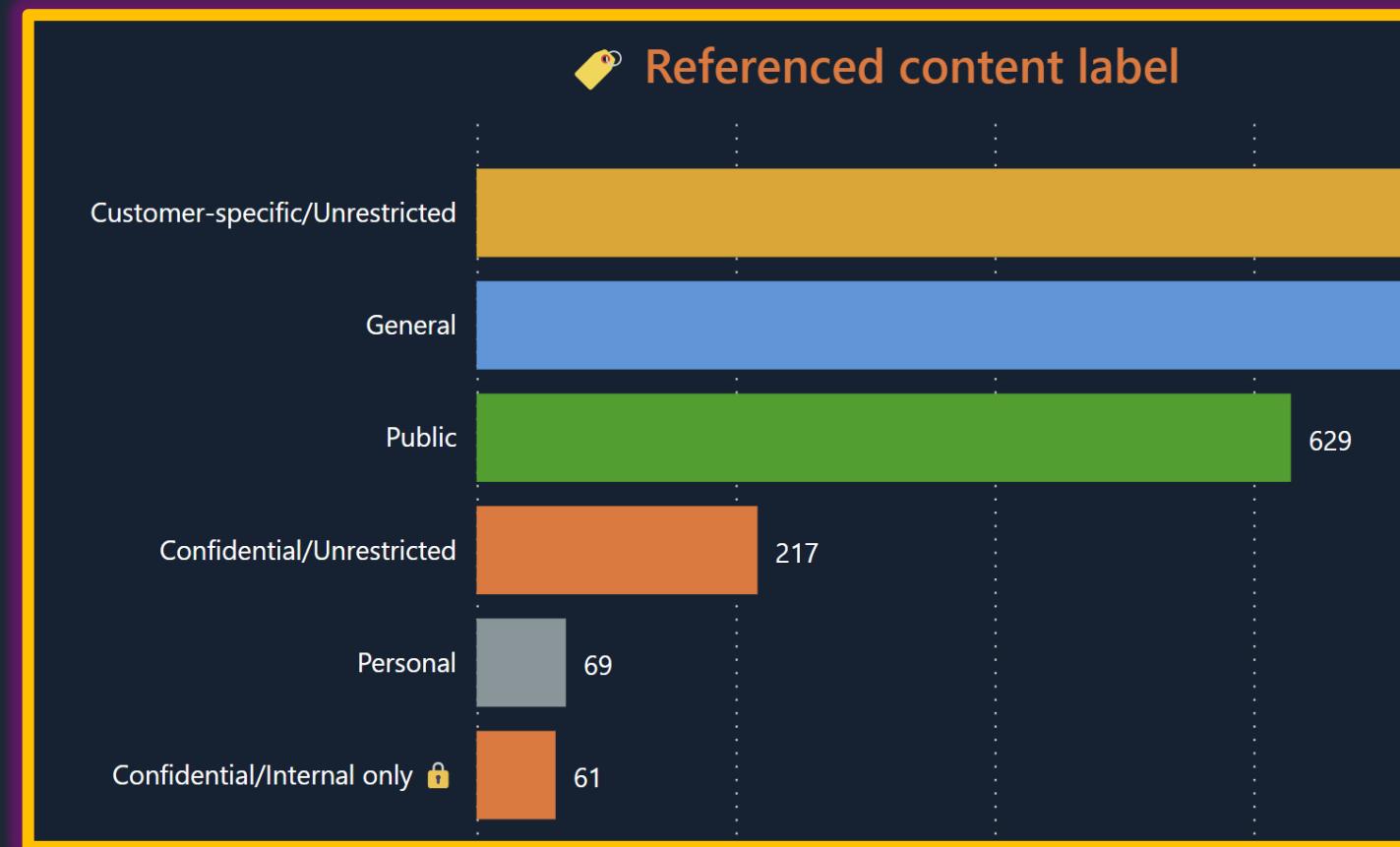
PROPERTIES



Expand



Add sensitivity label insights



Grab **sensitivity label data** with Security & Compliance PowerShell:

- **Label names**
- **Label GUIDs**

Add as a table in Power BI Desktop & create a 1:many relationship w/ CopilotInteraction



Add sensitivity label insights

```
# Connect to the Security & Compliance PowerShell  
Connect-IPPSSession
```

```
# Get a CSV report of your current sensitivity labels  
Get-Label | Select guid,  
@{Name="LabelDisplayName";Expression={if  
($_.parentlabeldisplayname)  
{"$($_.parentlabeldisplayname)/$($_.displayname)"} else  
{$_.displayname}}} | Export-CSV  
C:\Temp\SensitivityLabels.csv -NTI
```



Add sensitivity label insights

Guid	LabelDisplayName
defa4170-0d19-0005-0000-bc88714345d2	Personal
94774665-6c19-4675-8464-17a2a1e7d3ca	Public
defa4170-0d19-0005-0002-bc88714345d2	General
f11eccd2-5707-42d1-bbf7-687810ed9f86	Confidential
5948967a-be92-4652-bda9-521b79f86c10	Confidential/Unrestricted
50f416be-deb7-416d-b102-426405ae1176	Confidential/Secure email 
c2faab4d-519f-4812-af32-dabe19d53e73	Confidential/Internal only 
beddede8-e9b6-4986-b4a2-2d8242d4b8b4	Confidential/Custom permissions 
22b40fa4-b0cf-4a88-a1f3-270d8d225816	Secret
85a26ec7-98d3-41fb-a12f-d7e6dff2da9c	Secret/Unrestricted
35057bd7-9717-450a-9f31-41391c20e6e9	Secret/Secure email (forwarding restricted) 
b271c7cf-b2cd-4933-abf8-ee1bb529522d	Secret/Internal only 
a8188293-3685-42d7-abfd-fca01125c682	Secret/Custom permissions 



Add results from sentiment questionnaires



Copilot threads by UPN



❓ How much time do you feel you save with Copilot per week?



5h



3h



2h



0,5h



Summary



Summary

-  Get **CopilotInteraction** events from the UAL
-  Get **Entra ID** identity data
-  Combine in **Power BI**
-  **Analyze** M365 Copilot use in-depth across roles and more
-  **Automate** audit event & identity data refresh
-  **Expand** your analytics to offer more insights
-  **Apply** gathered insights to adoption and upskilling efforts
-  ? ? ?
-  **Profit!**



Comments or
questions?

Connect with me!

