Session 8-2023 | Azure Resource Graph

Your | hosts

Alex Verboon

https://twitter.com/alexverboon

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

https://github.com/alexverboon

https://www.verboon.info/

MVP Microsoft® Most Valuable Professional

Gianni Castaldi

https://twitter.com/castello_johnny

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

https://github.com/KustoKing

https://www.kustoking.com/

KQL|Cafe

Show | Agenda

Welcome

What is new/updates for KQL

Our Guest Morten Waltorp Knudsen

What did you do with KQL this month?

What's New – Microsoft Graph Logs

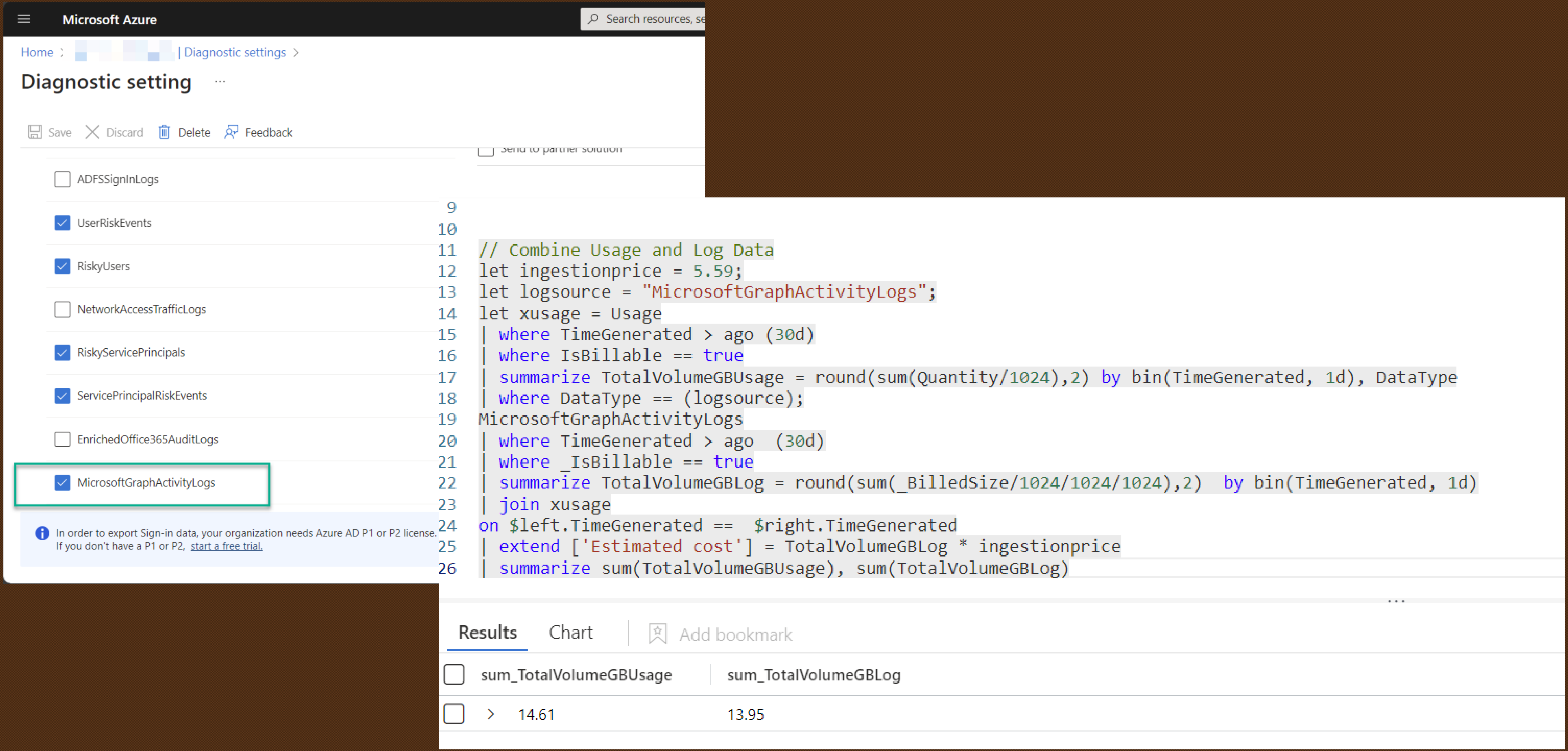
The Microsoft Graph Activity Logs include information about the request and client application. Some common use cases include:

- Identifying the activities that a compromised user account conducted in your tenant.
- Building detections and behavioral analysis to identify suspicious or anomalous use of Microsoft Graph APIs – such as an application enumerating all users; or making probing requests with many 403 errors.
- Investigating unexpected or unnecessarily privileged assignments of application permissions.
- Identifying problematic or unexpected behaviors for client applications – such as extreme call volumes that exhaust rate-limits for the tenant.

https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/microsoft-graph-activity-log-is-now-available-in-public-preview/ba-p/3848269

https://cloudbrothers.info/en/detect-threats-microsoft-graph-logs-part-1/

What's New – Microsoft Graph Logs



Diagnostic setting

□ Send to partner solution

□ ADFSSignInLogs

☑ UserRiskEvents

☑ RiskyUsers

□ NetworkAccessTrafficLogs

☑ RiskyServicePrincipals

☑ ServicePrincipalRiskEvents

□ EnrichedOffice365AuditLogs

☑ MicrosoftGraphActivityLogs

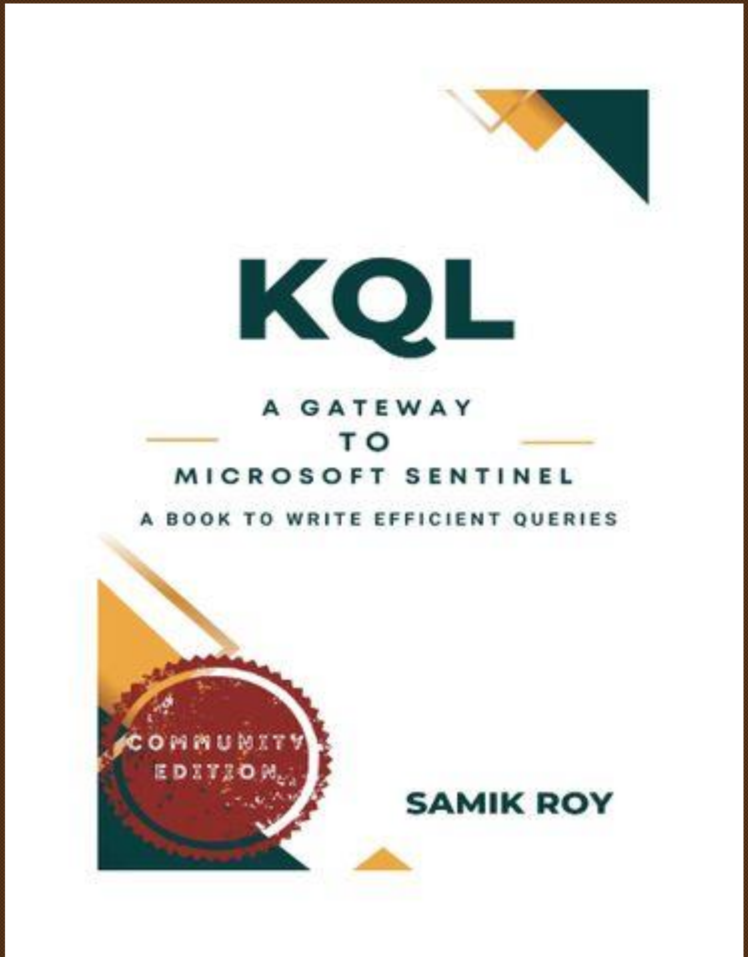
In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

```
// Combine Usage and Log Data
let ingestionprice = 5.59;
let logsource = "MicrosoftGraphActivityLogs";
let xusage = Usage
| where TimeGenerated > ago (30d)
| where IsBillable == true
| summarize TotalVolumeGBUsage = round(sum(Quantity/1024),2) by bin(TimeGenerated, 1d), DataType
| where DataType == (logsource);
MicrosoftGraphActivityLogs
| where TimeGenerated > ago  (30d)
| where _IsBillable == true
| summarize TotalVolumeGBLog = round(sum(_BilledSize/1024/1024/1024),2)  by bin(TimeGenerated, 1d)
| join xusage
on $left.TimeGenerated ==  $right.TimeGenerated
| extend ['Estimated cost'] = TotalVolumeGBLog * ingestionprice
| summarize sum(TotalVolumeGBUsage), sum(TotalVolumeGBLog)
```

sum_TotalVolumeGBUsage	sum_TotalVolumeGBLog
14.61	13.95

What's New: KQL : A Gateway To Microsoft Sentinel (Community Edition) (eBook)

https://store.pothi.com/book/ebook-samik-roy-kql-gateway-microsoft-sentinel/



KQL

A GATEWAY
TO
MICROSOFT SENTINEL

A BOOK TO WRITE EFFICIENT QUERIES

COMMUNITY EDITION

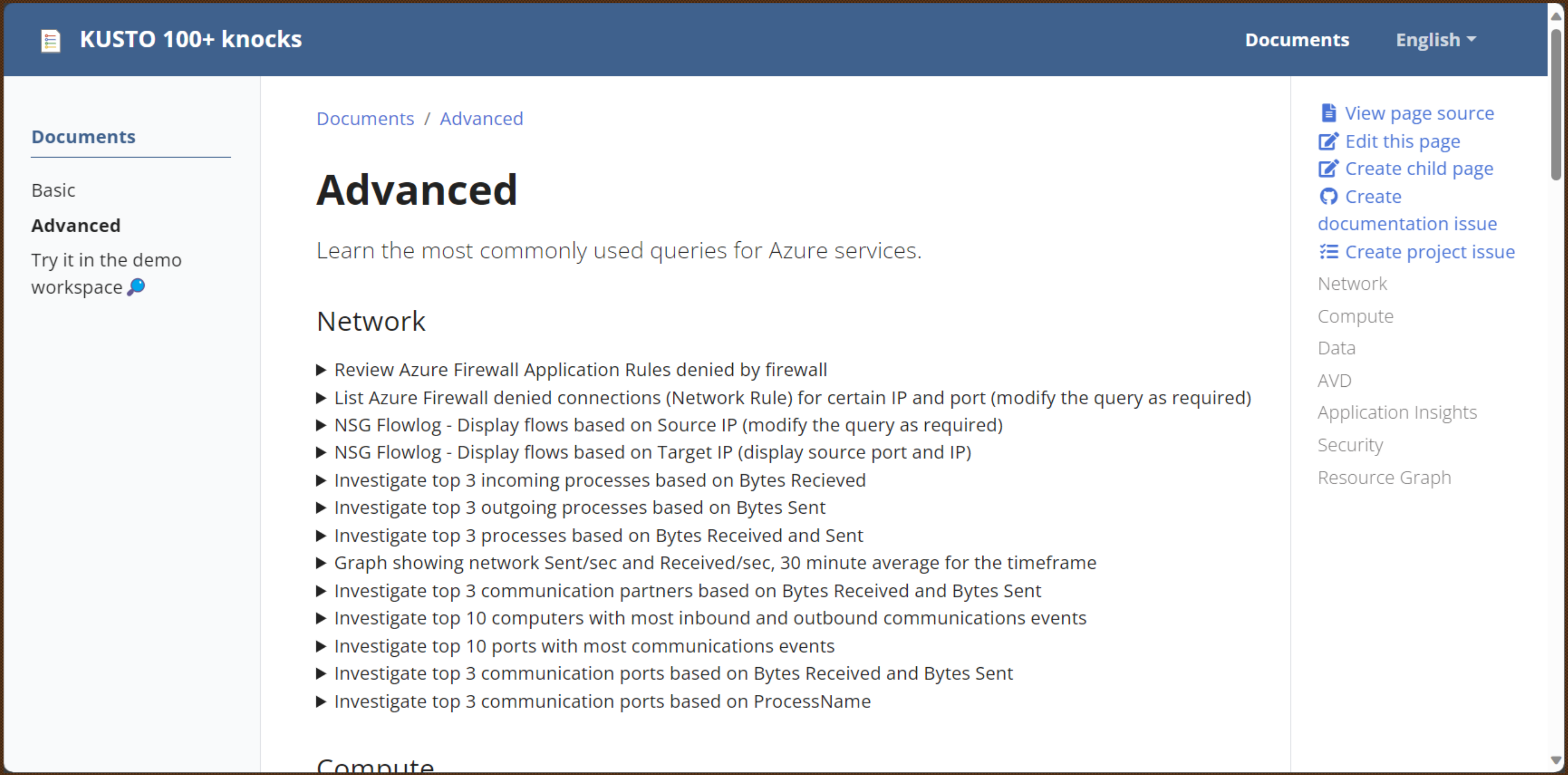
SAMIK ROY

What’s new: DefenderHarvester

https://medium.com/falconforce/microsoft-defender-for-endpoint-internals-0x05-telemetry-for-sensitive-actions-1b90439f5c25

KUSTO 100+ knocks

https://azure.github.io/fta-kusto100knocks/docs/



Documents

Basic

Advanced

Try it in the demo workspace 🔎

Documents / Advanced

Advanced

Learn the most commonly used queries for Azure services.

Network

- ▶ Review Azure Firewall Application Rules denied by firewall
- ▶ List Azure Firewall denied connections (Network Rule) for certain IP and port (modify the query as required)
- ▶ NSG Flowlog - Display flows based on Source IP (modify the query as required)
- ▶ NSG Flowlog - Display flows based on Target IP (display source port and IP)
- ▶ Investigate top 3 incoming processes based on Bytes Recieved
- ▶ Investigate top 3 outgoing processes based on Bytes Sent
- ▶ Investigate top 3 processes based on Bytes Received and Sent
- ▶ Graph showing network Sent/sec and Received/sec, 30 minute average for the timeframe
- ▶ Investigate top 3 communication partners based on Bytes Received and Bytes Sent
- ▶ Investigate top 10 computers with most inbound and outbound communications events
- ▶ Investigate top 10 ports with most communications events
- ▶ Investigate top 3 communication ports based on Bytes Received and Bytes Sent
- ▶ Investigate top 3 communication ports based on ProcessName

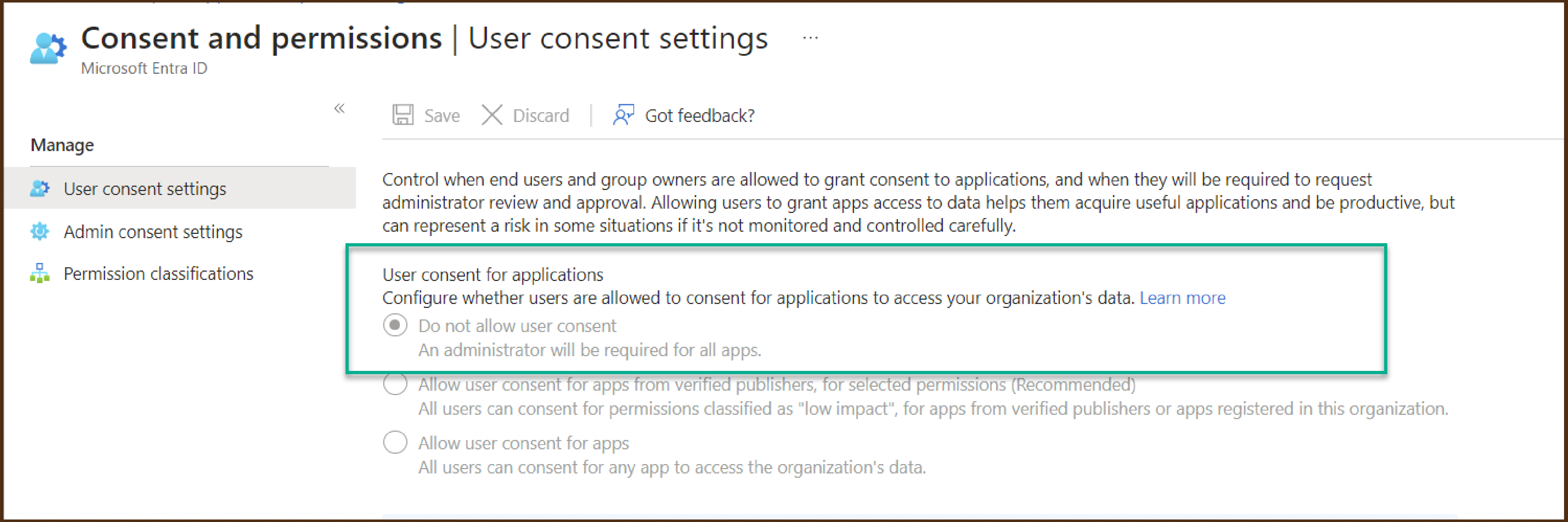
Compute

Guest: Morten Waltorp Knudsen

[(7) Morten Waltorp Knudsen [MVP] | LinkedIn]

What did you do with KQL this month?

Entra ID consented Apps Cleanup



Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

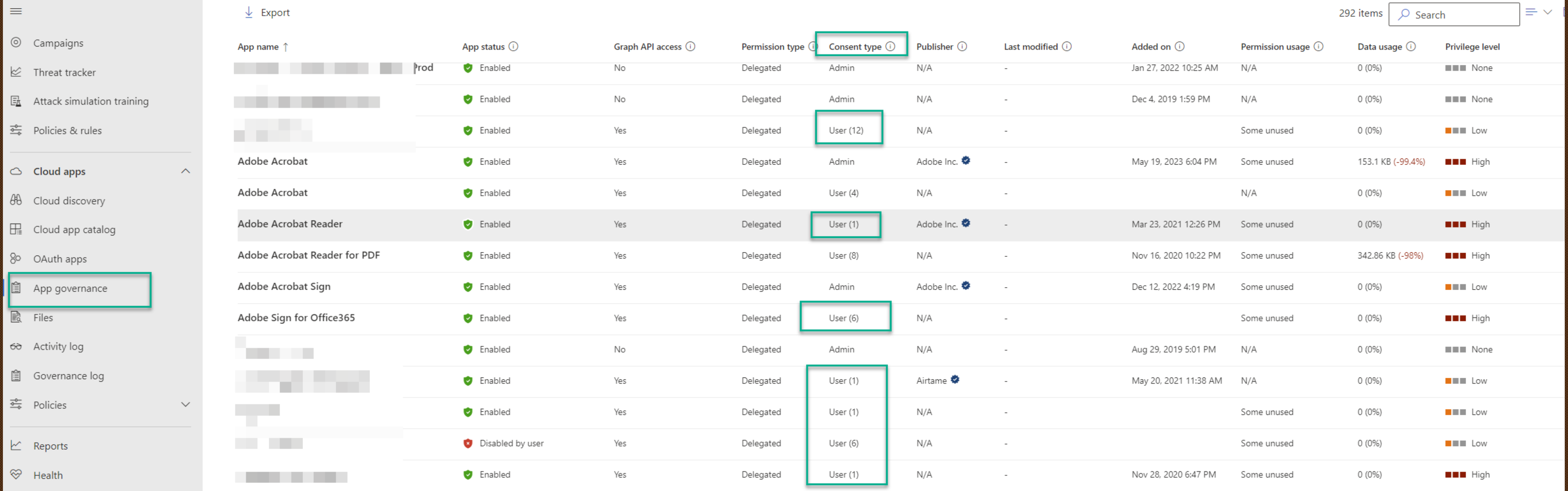
● Do not allow user consent
An administrator will be required for all apps.

○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

○ Allow user consent for apps
All users can consent for any app to access the organization's data.

What did you do with KQL this month?

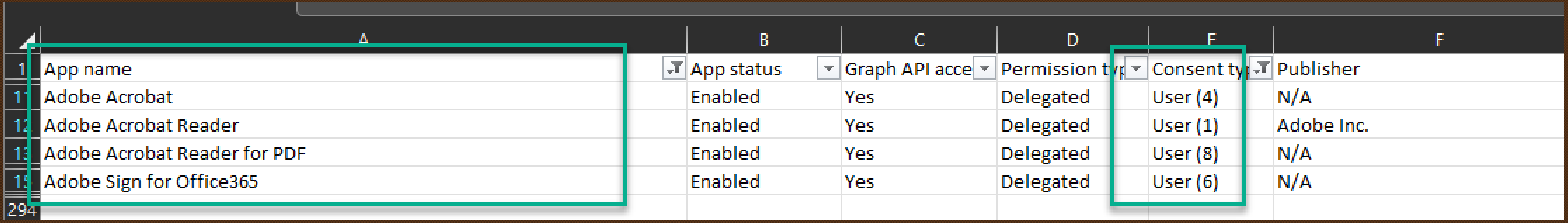
Entra ID consented Apps Cleanup



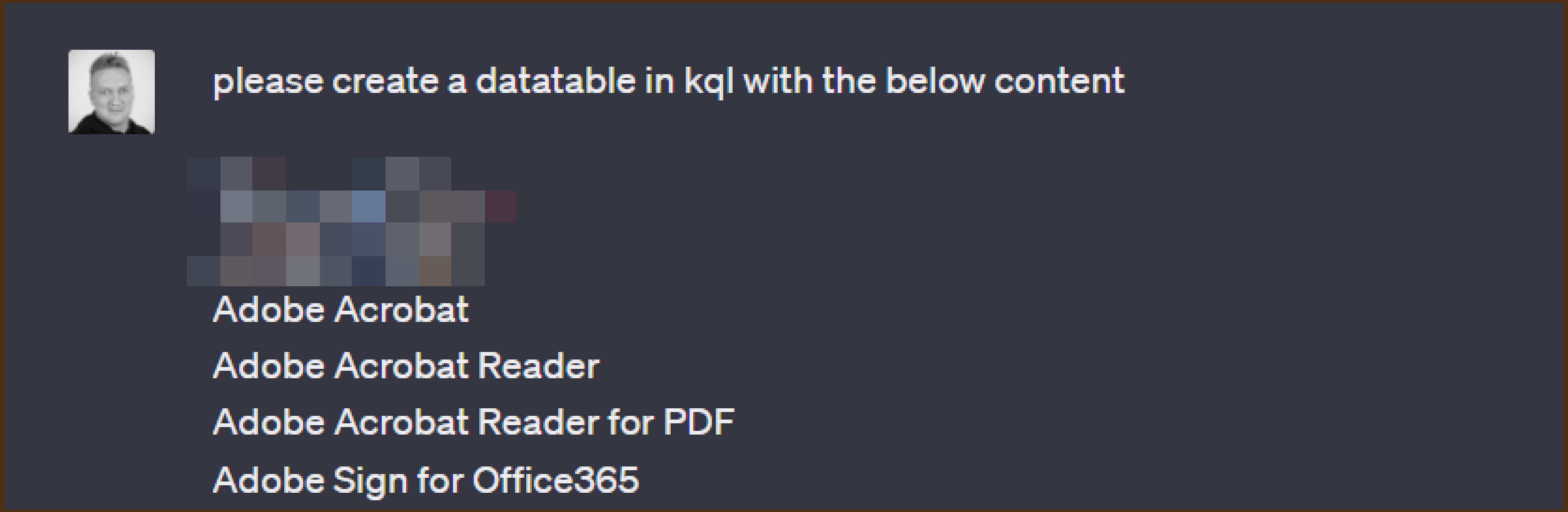
App name ↑	App status	Graph API access	Permission type	Consent type	Publisher	Last modified	Added on	Permission usage	Data usage	Privilege level
[redacted]	Enabled	No	Delegated	Admin	N/A	-	Jan 27, 2022 10:25 AM	N/A	0 (0%)	None
[redacted]	Enabled	No	Delegated	Admin	N/A	-	Dec 4, 2019 1:59 PM	N/A	0 (0%)	None
[redacted]	Enabled	Yes	Delegated	User (12)	N/A	-		Some unused	0 (0%)	Low
Adobe Acrobat	Enabled	Yes	Delegated	Admin	Adobe Inc.	-	May 19, 2023 6:04 PM	Some unused	153.1 KB (-99.4%)	High
Adobe Acrobat	Enabled	Yes	Delegated	User (4)	N/A	-		N/A	0 (0%)	Low
Adobe Acrobat Reader	Enabled	Yes	Delegated	User (1)	Adobe Inc.	-	Mar 23, 2021 12:26 PM	Some unused	0 (0%)	High
Adobe Acrobat Reader for PDF	Enabled	Yes	Delegated	User (8)	N/A	-	Nov 16, 2020 10:22 PM	Some unused	342.86 KB (-98%)	High
Adobe Acrobat Sign	Enabled	Yes	Delegated	Admin	Adobe Inc.	-	Dec 12, 2022 4:19 PM	Some unused	0 (0%)	Low
Adobe Sign for Office365	Enabled	Yes	Delegated	User (6)	N/A	-		Some unused	0 (0%)	High
[redacted]	Enabled	No	Delegated	Admin	N/A	-	Aug 29, 2019 5:01 PM	N/A	0 (0%)	None
[redacted]	Enabled	Yes	Delegated	User (1)	Airtame	-	May 20, 2021 11:38 AM	N/A	0 (0%)	Low
[redacted]	Enabled	Yes	Delegated	User (1)	N/A	-		Some unused	0 (0%)	Low
[redacted]	Disabled by user	Yes	Delegated	User (6)	N/A	-		Some unused	0 (0%)	Low
[redacted]	Enabled	Yes	Delegated	User (1)	N/A	-	Nov 28, 2020 6:47 PM	Some unused	0 (0%)	High

What did you do with KQL this month?

Entra ID consented Apps Cleanup



	A	B	C	D	E	F
1	App name	App status	Graph API acce	Permission typ	Consent ty	Publisher
11	Adobe Acrobat	Enabled	Yes	Delegated	User (4)	N/A
12	Adobe Acrobat Reader	Enabled	Yes	Delegated	User (1)	Adobe Inc.
13	Adobe Acrobat Reader for PDF	Enabled	Yes	Delegated	User (8)	N/A
15	Adobe Sign for Office365	Enabled	Yes	Delegated	User (6)	N/A
294						



please create a datatable in kql with the below content

[redacted]

Adobe Acrobat

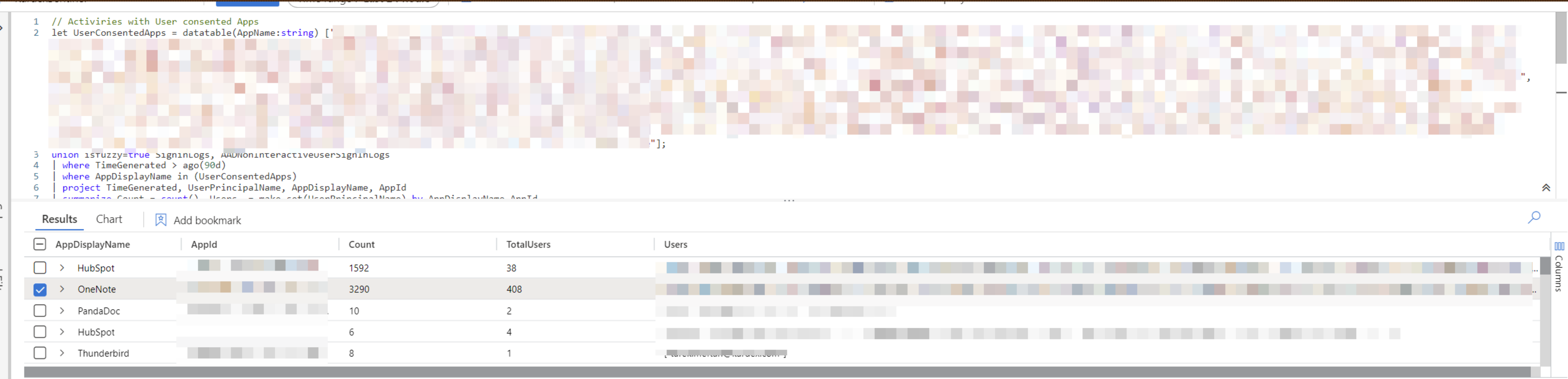
Adobe Acrobat Reader

Adobe Acrobat Reader for PDF

Adobe Sign for Office365

What did you do with KQL this month?

Entra ID consented Apps Cleanup

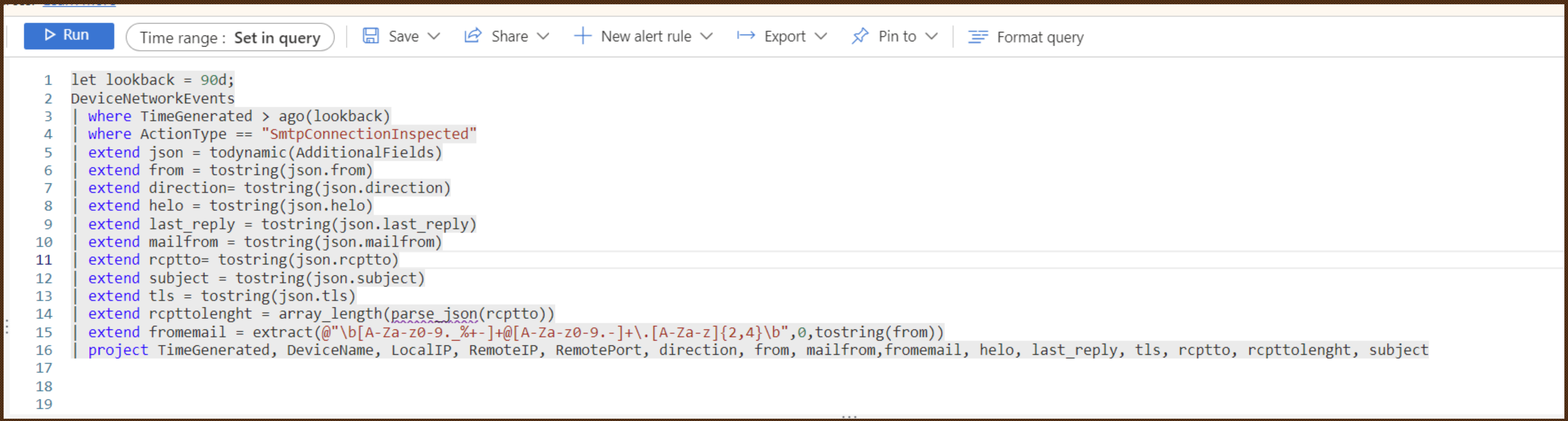


```
// Activiries with User consented Apps
let UserConsentedApps = datatable(AppName:string) ['[redacted]"];
union isfuzzy=true SigninLogs, AADNonInteractiveUserSignInLogs
| where TimeGenerated > ago(90d)
| where AppDisplayName in (UserConsentedApps)
| project TimeGenerated, UserPrincipalName, AppDisplayName, AppId
| summarize Count = count(), Users = make_set(UserPrincipalName) by AppDisplayName, AppId
```

□ AppDisplayName	AppId	Count	TotalUsers	Users
□ › HubSpot	[redacted]	1592	38	[redacted]
☑ › OneNote	[redacted]	3290	408	[redacted]
□ › PandaDoc	[redacted]	10	2	[redacted]
□ › HubSpot		6	4	[redacted]
□ › Thunderbird	[redacted]	8	1	[redacted]

What did you do with KQL this month?

Zeek SMTP Traffic



```
let lookback = 90d;
DeviceNetworkEvents
| where TimeGenerated > ago(lookback)
| where ActionType == "SmtpConnectionInspected"
| extend json = todynamic(AdditionalFields)
| extend from = tostring(json.from)
| extend direction= tostring(json.direction)
| extend helo = tostring(json.helo)
| extend last_reply = tostring(json.last_reply)
| extend mailfrom = tostring(json.mailfrom)
| extend rcptto= tostring(json.rcptto)
| extend subject = tostring(json.subject)
| extend tls = tostring(json.tls)
| extend rcpttolenght = array_length(parse_json(rcptto))
| extend fromemail = extract(@"\b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b",0,tostring(from))
| project TimeGenerated, DeviceName, LocalIP, RemoteIP, RemotePort, direction, from, mailfrom,fromemail, helo, last_reply, tls, rcptto, rcpttolenght, subject
```

What did you do with KQL this month?

Are we impacted by CVE-2023-38545?

Thanks for attending

KQL|Cafe