

# How to get hands dirty with KQL?!

Markus Lintuala, Elisa Oyj



# Markus Lintuala

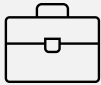


## Focus

Public and hybrid cloud solutions and architectures with a security aspect

## Certifications

Security, Azure, DevOps, Microsoft 365 Expert, MCT  
Rest here: [those](#)



## Elisa Oyj

Senior Technical Consultant

## Hobbies

IT, Aviation, Food



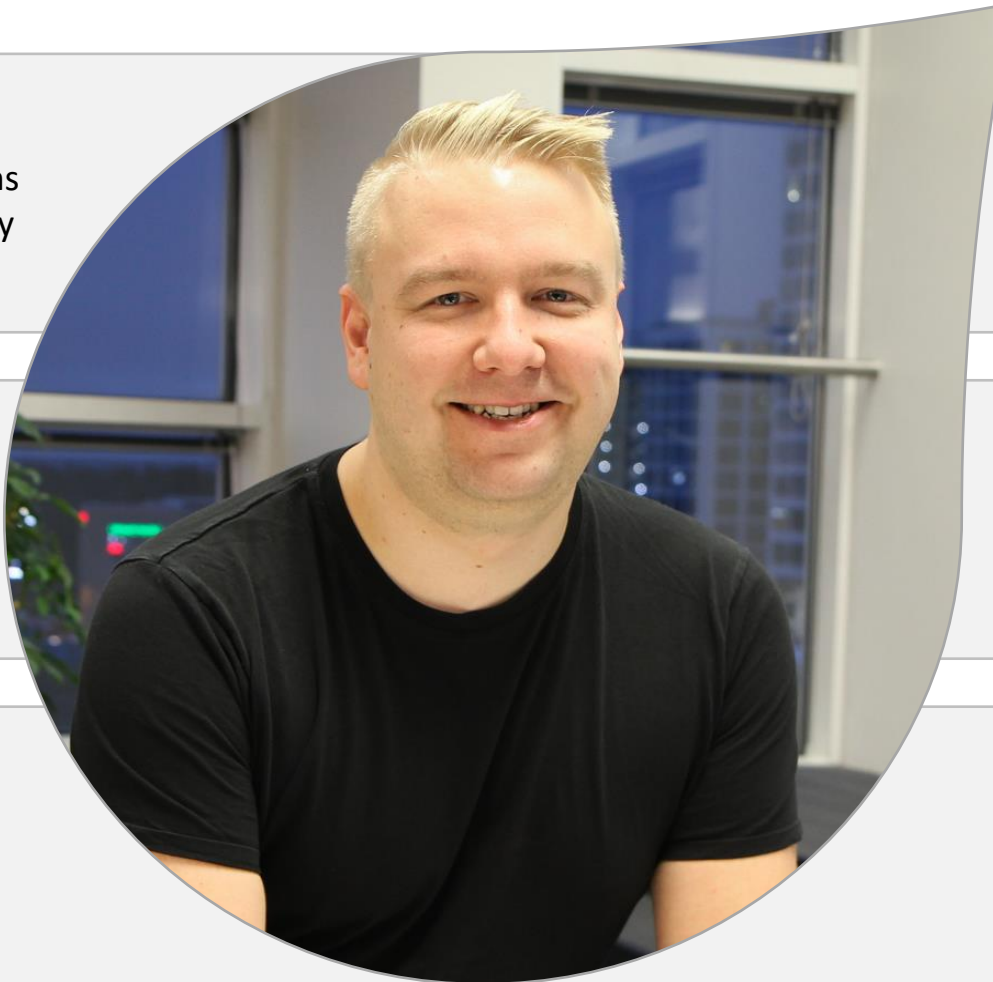
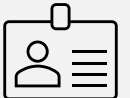
## Blog

<https://bloggerz.cloud>



## Contact

LinkedIn: [lintuala](#)  
Twitter: [@MarkusLintuala](#)  
E-mail: [markus@lintuala.fi](mailto:markus@lintuala.fi)



# Agenda

---

What is KQL

---

KQL query workflow

---

Schema & data types

---

Data aggregation and handling

---

Data ordering and projection

---

Visualize your data

---

Variables

---

Unions and Joins

---

Data export and alerts

---

KQL internal and custom functions

---

Azure Data Explorer

---

Log Analytics + Sentinel

---

Microsoft 365 Defender

---

Azure Graph Queries

---

How to train yourself

---

Kusto Detective Game

---

Q & A



What is KQL?



# Kusto query

*"A Kusto query is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model that is easy to read, author, and automate. Kusto queries are made of one or more query statements."*



# KQL query workflow

*“It’s OK not to be a pro on day 1 and still be able to use tools like Microsoft Sentinel to monitor security for the environment.”*

- Rod Trent, 19.11.2021

What you  
want to  
look for?

Is it there?

Where it is?

Why it is there?



Is it there?

Run Time range : Last 24 hours Save Share + New alert rule Export Pin to Format query

```
1 search "markus.lintuala@elisa.fi"
```

Results Chart

TimeGenerated [UTC]	Stable	Type	UserType	AccountName	AccountObjectId	AccountUPN	AccountTenantId
> 2022-11-11 23.38.10.042	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 02.39.18.424	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-11 20.38.15.597	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 05.38.09.872	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 10.39.27.565	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-11 21.38.28.592	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 00.39.17.544	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 09.38.22.318	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-11 22.38.35.626	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 01.38.12.932	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 06.39.30.000	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 07.38.40.002	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 11.40.02.833	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-12 12.40.09.496	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb
> 2022-11-11 19.38.24.043	IdentityInfo	IdentityInfo	Member	markus.lintuala	d3e9e5f6-4193-4f35-b77c-11877c5a88fe	markus.lintuala@erikoisliikemiehet.fi	5b96d754-4eef-4955-bb

Where it is?

Run Time range : Last 24 hours Save Share + New alert rule Export Pin to Format query

```
1 search "markus.lintuala@elisa.fi"
2 | distinct $table
```

Results Chart

Stable

> IdentityInfo

Columns

Why it is  
there?

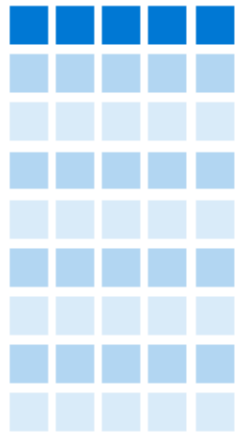
Run Time range: Last 24 hours Save Share + New alert rule Export Pin to Format query

```
1 search in (IdentityInfo) "markus.lintuala@elisa.fi"
2
```

Results Chart

TimeGenerated [UTC]	Stable	AccountName	AccountUPN	AccountObjectId	AccountTenantId
> 2022-11-12 17.38.16.801	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 14.38.05.597	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 16.37.55.676	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 15.38.46.901	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 18.37.39.445	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 13.38.14.250	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 18.36.46.694	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 18.38.35.587	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-11 23.38.10.042	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 02.39.18.424	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-11 20.38.15.597	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 05.38.09.872	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 10.39.27.565	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-11 21.38.28.592	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...
> 2022-11-12 00.39.17.544	IdentityInfo	markus.lintuala	markus.lintuala@erikoisliikemie...	d3e9e5f6-4193-4f35-b77c-118...	5b96d754-4eef-4955-bbe0-2d...

SecurityEvent



— Data —

```
SecurityEvent | where EventID == "4626"
```

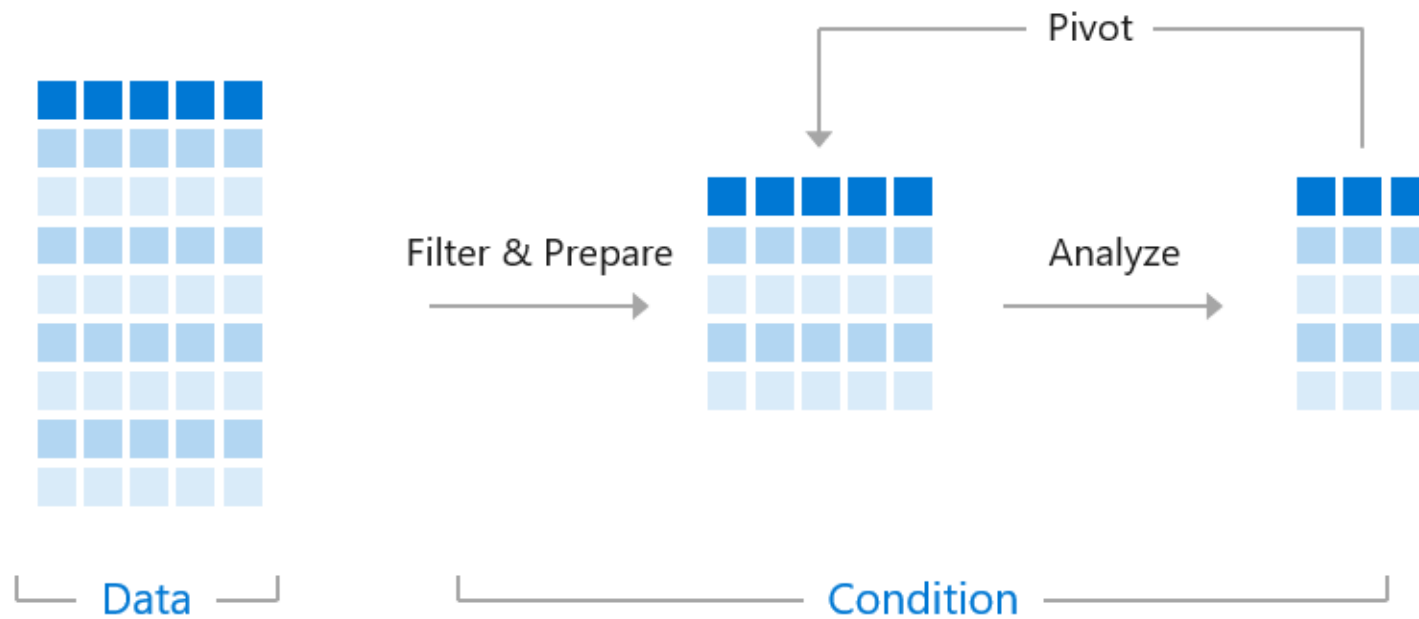


Filter & Prepare

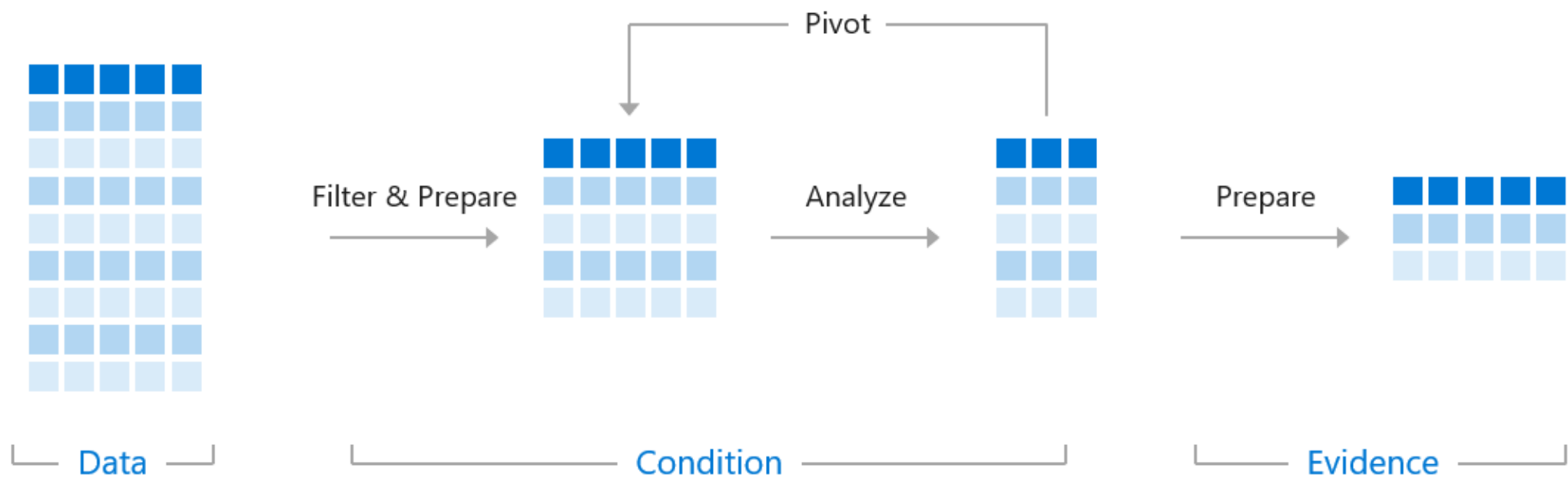


— Data —

```
SecurityEvent | where EventID == "4626" | summarize count() by Account
```



```
SecurityEvent | where EventID == "4626" | summarize count() by Account | limit 10
```



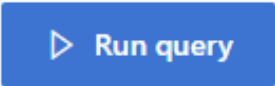




# Easy to choose!

```
SecurityEvent | where TimeGenerated >  
ago(1d) | where EventID == 4624 |  
summarize SuccessLogons =count() by  
Account, bin(TimeGenerated, 1h) | order by  
TimeGenerated desc , Account asc
```

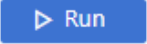



```
SecurityEvent  
| where TimeGenerated > ago(1d)  
| where EventID == 4624  
| summarize SuccessLogons=count() by  
Account, bin(TimeGenerated, 1h)  
| order by TimeGenerated desc , Account asc
```

# Copy link, query, result, share




  Save  Share link

Query

```
1 AlertInfo
2 | where Title == "Creation of forwarding/redirect rule"
```

 Time range : Last 24 hours  Save  Share  New alert rule

```
1 WVDConnections
2 | summarize Count=count() by Username, Session
```

 Copy link to query  
 Copy query text  
 Copy results

# Schema

<div><div>▶ Run</div><div>Time range : Last 24 hours</div><div>Save</div><div>Share</div><div>+ New alert rule</div><div>Export</div><div>Pin to</div><div>Format query</div></div>			
<pre>1 SecurityEvent 2   getschema</pre>			
...			
<div>ResultsChart</div>			
ColumnName	ColumnOrdinal	DataType	ColumnType
> TenantId	0	System.String	string
> TimeGenerated	1	System.DateTime	datetime
> SourceSystem	2	System.String	string
> Account	3	System.String	string
> AccountType	4	System.String	string
> Computer	5	System.String	string
> EventSourceName	6	System.String	string
> Channel	7	System.String	string
> Task	8	System.Int32	int
> Level	9	System.String	string
> EventData	10	System.String	string
> EventID	11	System.Int32	int
> Activity	12	System.String	string
> SourceComputerId	13	System.String	string
> EventOriginId	14	System.String	string
> MG	15	System.String	string

# Datatypes

int (32bit), long (64bit)

- 1, 2, 3, 10

decimal

- 1.12, 5.23, 23.00

real (double)

- 1.0, 4.2, 1e6

bool

- True/False

string

- "KQL Is Fun" or 'KQL is fun'

datetime

- datetime(2022-11-09 10:15:30), now(), ago(7d)

timespan

- 5d, 5m, 500ms

dynamic

- {"today":"tue", "tomorrow":"wed", "dayIndex":[1,2]}



# Basic data aggregation

- Summarize <HOW TO SUMMARIZE> by <WHAT TO SUMMARIZE>
    - Count()
    - Sum()
    - Avg()
    - Max()
    - Min()
-

# Basic data aggregation

▶ Run Time range : Custom 📁 Save ▼ 🔗 Share ▼ + New alert rule ↔ Export ▼ 📌 Pin to ▼ ≡ Format query ...

```
1 SigninLogs
2 | where UserType == "Guest"
3 | summarize count() by UserPrincipalName
```

Results Chart 🔍

UserPrincipalName	count_
> markus.lintuala@erikoisliikemiehet.fi	13
> mika.vilpo@elisa.fi	1
> mika.vilpo@erikoisliikemiehet.fi	7

Columns



# Advanced data aggregation

- Summarize <HOW TO SUMMARIZE> by <WHAT TO SUMMARIZE>
    - Arg\_min()
    - Arg\_max()
    - Percentiles()
    - Makelist()
    - Countif()
    - Bin()
-



# Arg\_max()

▶ Run Time range : Custom Save Share + New alert rule Export Pin to Format query ...

```
1 SigninLogs
2 | where UserType == "Guest"
3 | summarize arg_max(TimeGenerated, *) by UserPrincipalName
```

Results Chart

UserPrincipalName	TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	Columns
> mika.vilpo@elisa.fi	2022-09-29 16.42.21.369	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInLogs	
> markus.lintuala@erikoisliikemiehet.fi	2022-10-14 09.59.00.862	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInLogs	
> mika.vilpo@erikoisliikemiehet.fi	2022-11-17 11.21.58.194	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInLogs	

# Summarize without by

```
1 SigninLogs
2 | where UserType == "Guest"
3 | summarize
4     SuccessCA=countif(ConditionalAccessStatus =~ 'success'),
5     NotAppliedCA=countif(ConditionalAccessStatus =~ 'NotApplied'),
6     OtherCA=countif(ConditionalAccessStatus != 'success' or ConditionalAccessStatus != 'notApplied')
```

Results

Chart

SuccessCA

NotAppliedCA

OtherCA

> 310

678

988

# User bin and timespan

Run Time range: Custom Save Share + New alert rule Export Pin to Format query

```
1 SigninLogs
2 | where UserType == "Guest"
3 | summarize CountOfSignins=count() by UserPrincipalName, bin(TimeGenerated, 1h)
```

Results Chart

UserPrincipalName	TimeGenerated [UTC]	CountOfSignins
> markus.lintuala@erikoisliikemiehet.fi	2022-08-25 18.00.00.000	1
> markus.lintuala@erikoisliikemiehet.fi	2022-08-26 05.00.00.000	1
> mika.vilpo@erikoisliikemiehet.fi	2022-08-29 07.00.00.000	2
> markus.lintuala@erikoisliikemiehet.fi	2022-09-15 08.00.00.000	1
> markus.lintuala@erikoisliikemiehet.fi	2022-09-15 10.00.00.000	1
> markus.lintuala@erikoisliikemiehet.fi	2022-09-15 12.00.00.000	1
> markus.lintuala@erikoisliikemiehet.fi	2022-09-22 05.00.00.000	1
> mika.vilpo@elisa.fi	2022-09-29 16.00.00.000	1
> markus.lintuala@erikoisliikemiehet.fi	2022-10-05 15.00.00.000	6
> markus.lintuala@erikoisliikemiehet.fi	2022-10-14 09.00.00.000	1
> mika.vilpo@erikoisliikemiehet.fi	2022-11-01 07.00.00.000	1
> mika.vilpo@erikoisliikemiehet.fi	2022-11-02 12.00.00.000	1
> mika.vilpo@erikoisliikemiehet.fi	2022-11-07 18.00.00.000	2
> mika.vilpo@erikoisliikemiehet.fi	2022-11-17 11.00.00.000	1

0s 612ms Display time (UTC+00:00) Query details 1 - 14 of 14

# Extending and parsing

Use **extend** to  
create new columns  
based on other data

Use **parse** to split  
string in parts



1

DEMO

Parse String

# Extractjson and parse\_json

- When you have value in json and you want...
  - **one** value out, use **extractjson**
  - **multiple** values out, use **parse\_json**



# DEMO

Parse JSON



# 2

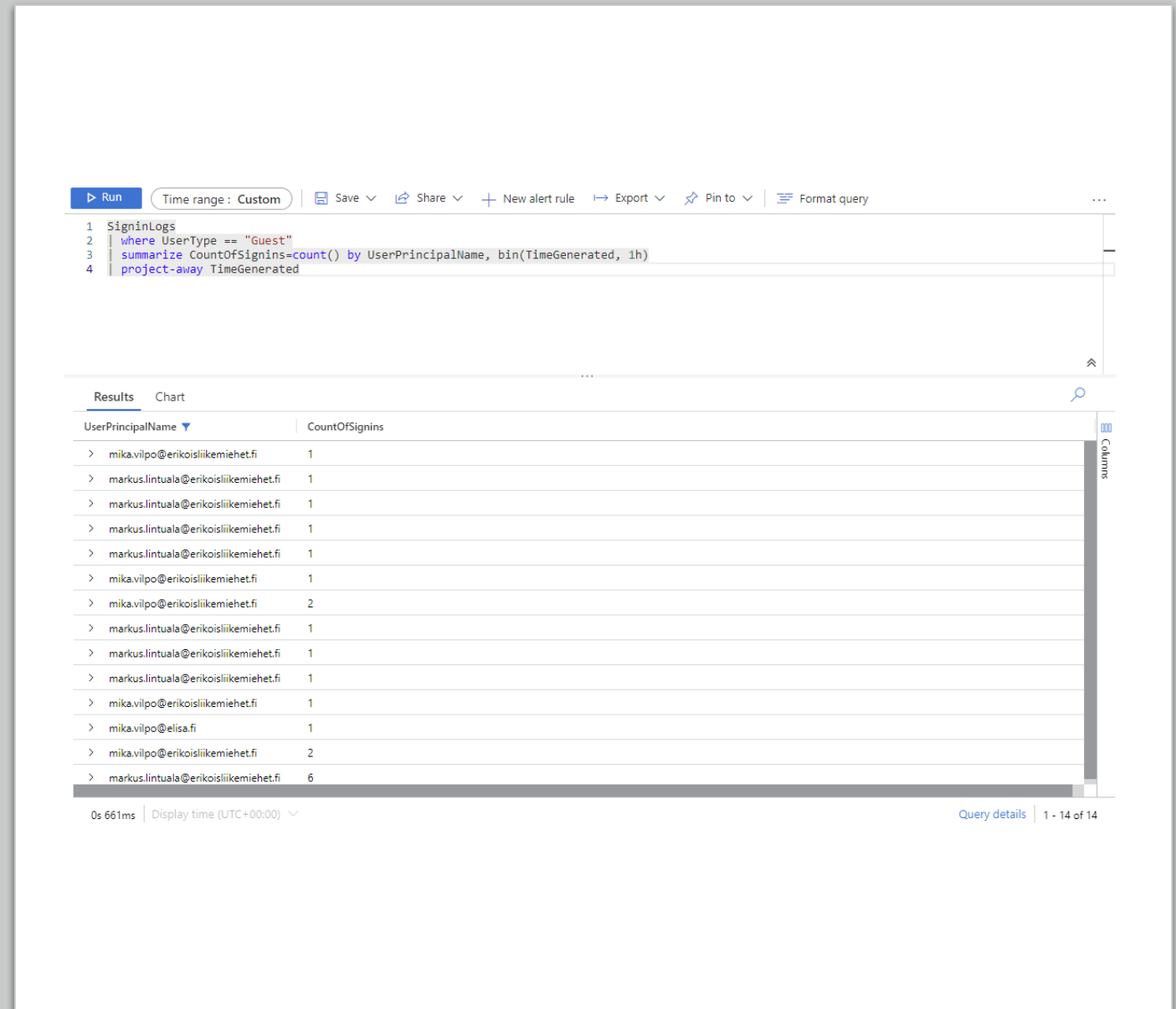




# Data ordering and projection

# Projection

- Project selected columns only for results
- Some other projects available as well
  - Project-away
  - Project-keep
  - Project-rename
  - Project-reorder
- You can manipulate results when projecting



The screenshot displays a query editor interface. At the top, there's a toolbar with buttons for 'Run', 'Save', 'Share', 'New alert rule', 'Export', 'Pin to', and 'Format query'. Below the toolbar, a SQL query is entered in a text area:

```
1 SigninLogs
2 | where UserType == "Guest"
3 | summarize CountOfSignins=count() by UserPrincipalName, bin(TimeGenerated, 1h)
4 | project-away TimeGenerated
```

Below the query editor, the 'Results' tab is active, showing a table with two columns: 'UserPrincipalName' and 'CountOfSignins'. The table contains 14 rows of data. A 'Columns' sidebar is visible on the right side of the table.

UserPrincipalName	CountOfSignins
> mika.vilpo@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> mika.vilpo@erikoisliikemiehet.fi	1
> mika.vilpo@erikoisliikemiehet.fi	2
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> mika.vilpo@erikoisliikemiehet.fi	1
> mika.vilpo@elisa.fi	1
> mika.vilpo@erikoisliikemiehet.fi	2
> markus.lintuala@erikoisliikemiehet.fi	6

At the bottom of the interface, there's a status bar showing '0s 661ms | Display time (UTC+00:00)' and a link to 'Query details'.

Run Time range: Custom Save Share + New alert rule Export Pin to Format query

```
1 SigninLogs
2 | where UserType == "Guest"
3 | summarize CountOfSignins=count() by UserPrincipalName, bin(TimeGenerated, 1h)
4 | project-away TimeGenerated
5 | order by CountOfSignins desc
```

Results Chart

UserPrincipalName	CountOfSignins
> markus.lintuala@erikoisliikemiehet.fi	6
> mika.vilpo@erikoisliikemiehet.fi	2
> mika.vilpo@erikoisliikemiehet.fi	2
> mika.vilpo@elisa.fi	1
> mika.vilpo@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> mika.vilpo@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> mika.vilpo@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1
> markus.lintuala@erikoisliikemiehet.fi	1

0s 633ms Display time (UTC+00:00) Query details 1 - 14 of 14

# Ordering

- Order and sort are same
- Descending is the default order method
- Nulls can be defined separately

Visualize your data

1 SignInLogs  
2

Results	Chart																				
TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	ResultType	ResultSignature	ResultDescription	DurationMs	CorrelationId	Resource	ResourceGroup	Identity	Level	Location	AlternateSignInName	AppDisplayName	AppId				
>	2022-11-12 01.55.33.938	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	334d4aff-75ae-4072-8202-17bea8e67059	Microsoft.aadim	Microsoft.aadim	Semen Kotov	4	TR		Azure Portal	c44b4083-3bb6				
>	2022-11-12 02.19.36.365	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	62ac2Zee-2746-44bb-bdac-b759ae5aad55	Microsoft.aadim	Microsoft.aadim	Rutger Schenk	4	BE		Azure Portal	c44b4083-3bb6				
>	2022-11-12 02.19.05.656	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	68430827-b6d4-4073-9a7b-3a311903db22	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 02.18.40.848	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	22595df8-35ee-4d60-b1f5-76c3375e7a24	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_AADCON_a5225d32ba79...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 02.19.20.578	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	dc65bf97-14fc-4ae8-f631-690f2ce2ae8a	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 02.18.33.600	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	cc61bb70-5ad6-4627-962b-4f51cbb6cc04	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_AADCON_a5225d32ba79...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 02.19.13.671	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	13709b12-9a90-4894-97fc-c8d16857ea61	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 02.34.18.097	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	604e164d-7fda-42e2-8940-bed0e4a068bd	Microsoft.aadim	Microsoft.aadim	Henry Yang	4	AU		Azure Portal	c44b4083-3bb6				
>	2022-11-12 03.08.33.845	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	b1d85d1f-e548-4e50-9cae-9b67e745fab38	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 03.18.35.857	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	3835cb3c-2f20-45b3-96de-f250b1628568	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_AADCON_a5225d32ba79...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 03.19.08.150	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	9a63a150-7f93-4ab1-a6f1-efc084c5a60	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 03.19.14.328	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	51edf9d9-1bd8-49a2-a1db-9003a6ab136a	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 03.19.19.751	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	63296b6c-53bb-459c-912a-b8716bbfb433	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 03.57.27.556	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50055	None	Invalid password, entered expired password.	0	b696ae915-73d8-4252-af61-ee6f48d34cfb7	Microsoft.aadim	Microsoft.aadim	Joanne Sensitive	4	AU	joannesensitive@contosohotel...	CATTack	d73513d5-ad26			
>	2022-11-12 04.18.43.825	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	7d510df8-c2c4-4610-adaf-725b46010060	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_AADCON_a5225d32ba79...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 04.19.12.657	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	8205cfc7-3ba8-4642-b652-538709968fc	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 04.19.25.267	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	aadc2436-bddd-4a08-b859-bf81b070136b	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.18.39.323	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	eb6c98b8-3789-461e-9b6b-6703bbce7e2f	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_AADCON_a5225d32ba79...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.18.45.332	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	09c6559-a88a-4e68-ac8d-44f43c3ac1b2	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.19.16.523	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	8f65223a-34e2-449e-a672-86c16bc13000	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.19.30.031	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	2d1490d4-12d0-4ae7-9537-06af9c0e407	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.19.23.782	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	0c30adec-cd6c-4f0f-9929-4745af00948	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_DC01_3862ce34675f@sec...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.39.02.179	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	4a3ecdfc-1b76-4e87-b56c-6eb00a1e29	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.38.48.078	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	615132f3-a314-49-82da-48c1f1f410cf	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 05.40.52.013	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50126	None	Invalid password, entered expired password.	0	c14aa1-26aa-482-9047-441bbf1f43e	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	IL	pdemo@seccpninja.onmicrosoft...	OfficeHome	4765445b-32c6			
>	2022-11-12 05.41.08.233	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	fb285140-3c7c-4977-84b4-a075989b637e	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	US	Office365 Shell WCSS-Client	89bee177-5ee6					
>	2022-11-12 06.03.37.057	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50140	None	This error occurred due to 'Keep me signed...	0	a864e454-d612-4d49-bc03-8648a9430737	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	GB	pdemo@seccpninja.onmicrosoft...	Microsoft 365 Security and Co...	80cca675-54bd			
>	2022-11-12 06.03.42.641	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50140	None	This error occurred due to 'Keep me signed...	0	0a5ce15f-160d-4d0b-9c2b-46e1fb28f63a	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	IE	pdemo@seccpninja.onmicrosoft...	Microsoft 365 Security and Co...	80cca675-54bd			
>	2022-11-12 05.40.57.798	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50140	None	This error occurred due to 'Keep me signed...	0	c14acadb-26ac-41d2-9047-f41bbf19a43	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	US	pdemo@seccpninja.onmicrosoft...	OfficeHome	4765445b-32c6			
>	2022-11-12 06.04.19.245	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50140	None	This error occurred due to 'Keep me signed...	0	62d16b9d-873b-44e2-b33c-90d68df41ac	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	CH	pdemo@seccpninja.onmicrosoft...	Modern Workplace Tools	fe6aa35b-7da8			
>	2022-11-12 06.04.24.980	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50140	None	This error occurred due to 'Keep me signed...	0	f724e7a8-5826-4e0d-8064-eecca26e1017	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	US	pdemo@seccpninja.onmicrosoft...	OfficeHome	4765445b-32c6			
>	2022-11-12 06.08.57.559	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	1f999d4f-6c68-42e1-b831-69df6a0576d	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 06.08.49.728	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	ce43cb03-0d7f-48ab-8eb1-6aa8dd32ab0c	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 06.18.41.595	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	4e637d7d-3d8e-4a10-a4d1-61e139028889	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_AADCON_a5225d32ba79...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 06.46.27.536	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	4f97b044-ac16-47f1-a746-b1e957843b9	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	IL		Azure Portal	c44b4083-3bb6				
>	2022-11-12 06.46.06.055	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	20b9fb54-f6b2-43dd-ac78-2258d41eb50a	Microsoft.aadim	Microsoft.aadim	Ivett Sándor	4	AU	ivett.sandor@contosohotels.com	CATTack	d73513d5-ad26				
>	2022-11-12 06.50.07.213	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	8441928f-c439-4a18-a330-cf6bc9a96137	Microsoft.aadim	Microsoft.aadim	Eloisa Cloutier	4	AU	eloisa.cloutier@contosohotels.c...	CATTack	d73513d5-ad26				
>	2022-11-12 06.51.19.085	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	a1371ae1-e3c8-4033-a7ed-fd93e0d04c310	Microsoft.aadim	Microsoft.aadim	Eloisa Cloutier	4	AU	eloisa.cloutier@contosohotels.c...	CATTack	d73513d5-ad26				
>	2022-11-12 06.51.27.289	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	d40a2136-1243-429c-8351-31116655385f	Microsoft.aadim	Microsoft.aadim	Lana Walker	4	AU	lana.walker@contosohotels.com	CATTack	d73513d5-ad26				
>	2022-11-12 06.51.06.920	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	22e944e4-0c4b-4767-858c-6e7f020a1d3	Microsoft.aadim	Microsoft.aadim	Eloisa Cloutier	4	AU	eloisa.cloutier@contosohotels.c...	CATTack	d73513d5-ad26				
>	2022-11-12 06.51.01.951	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	b5b27123-abd1-4860-afdd-430959fbf400	Microsoft.aadim	Microsoft.aadim	Ivett Sándor	4	AU	ivett.sandor@contosohotels.com	CATTack	d73513d5-ad26				
>	2022-11-12 07.03.21.982	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	50055	None	Invalid password, entered expired password.	0	6c008a30-9ed7-4653-b6db-d26be5319c15	Microsoft.aadim	Microsoft.aadim	Joanne Sensitive	4	AU	joannesensitive@contosohotel...	CATTack	d73513d5-ad26			
>	2022-11-12 07.08.53.973	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	af9f1c7-0835-478b-9406-723a607fe037	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 07.09.01.383	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	f2c18b5e-d85f-4e9a-ac41-5900e84fe628	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 07.10.35.777	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	e7c4d264-0b2b-45da-8a7a-341112699f1c	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	TH	89bee177-5ee6	Office365 Shell WCSS-Client	cb1056e2-e479				
>	2022-11-12 07.10.35.625	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	c5b57eae-1069-4e9f-9c12-48672f93da2a	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	TH	89bee177-5ee6	Office365 Shell WCSS-Client	cb1056e2-e479				
>	2022-11-12 07.09.01.255	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	e9c186d1-17aa-4d86-9c5b-9da0ded17753	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	TH	pdemo@seccpninja.onmicrosoft...	Microsoft Office 365 Portal	00000006-000000				
>	2022-11-12 07.09.08.985	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	2ab5c6bb-fa3c-4e68-b68c-f935e57d2210	Microsoft.aadim	Microsoft.aadim	On-Premises Directory Synchro...	4	US	Sync_NINJA-DC_9d913db9df8d...	Microsoft Azure Active Director...	cb1056e2-e479				
>	2022-11-12 07.10.23.053	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	f8f28a59-d8e2-476d-99a2-ee3676bc556	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	TH		Azure Portal	c44b4083-3bb6				
>	2022-11-12 07.10.35.655	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None	0	e77f0e04-3f2f-47d1-a279-c76a9a980f3a	Microsoft.aadim	Microsoft.aadim	Partner Demo	4	TH	Office						

Less is more  
– show what  
is necessary

Run Time range: Custom Save Share + New alert rule Export Pin to Format query

```
1 SigninLogs
2 | where UserType == "Member"
3 | extend Domain=split(UserPrincipalName, '@', 1)
4 | project TimeGenerated, UserPrincipalName, Domain=tostring(Domain[0])
```

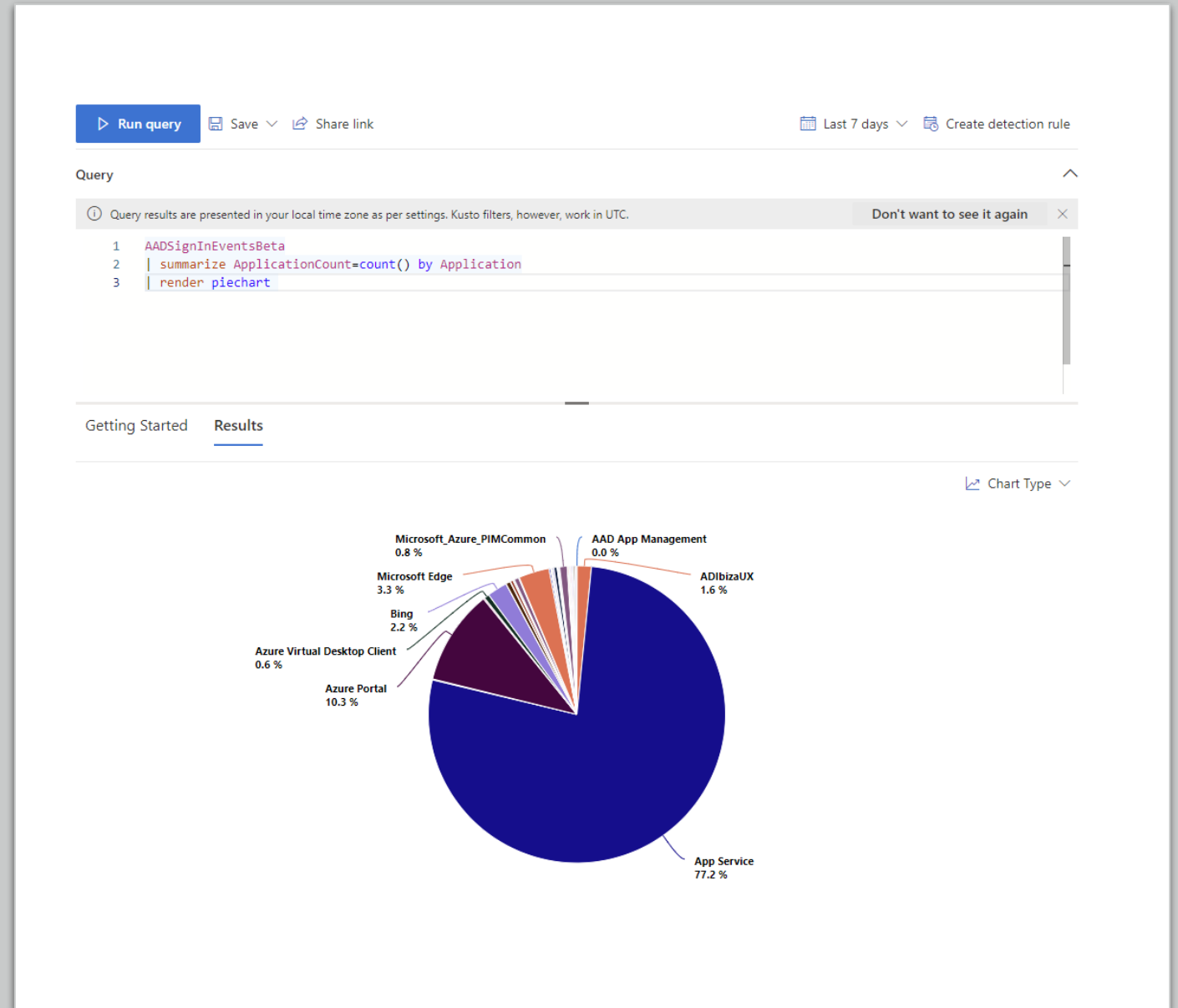
Results Chart

TimeGenerated [UTC]	UserPrincipalName	Domain
> 2022-11-18 19.01.36.253	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.01.36.251	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 18.49.51.934	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 18.49.46.888	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 18.49.57.711	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.26.33.004	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.19.715	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.27.747	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.33.582	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.28.005	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.28.651	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.23.239	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.33.720	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi
> 2022-11-18 19.27.29.599	markus.lintuala@erikoisliikemie...	erikoisliikemiehet.fi

2s 105ms | Display time (UTC+00:00) Query details | 1 - 14 of 11404

# Rendering

- Available visualizations
  - areachart
  - barchart
  - columnchart
  - piechart
  - scatterchart
  - timechart
- X-axis comes first except in columnchart and piechart

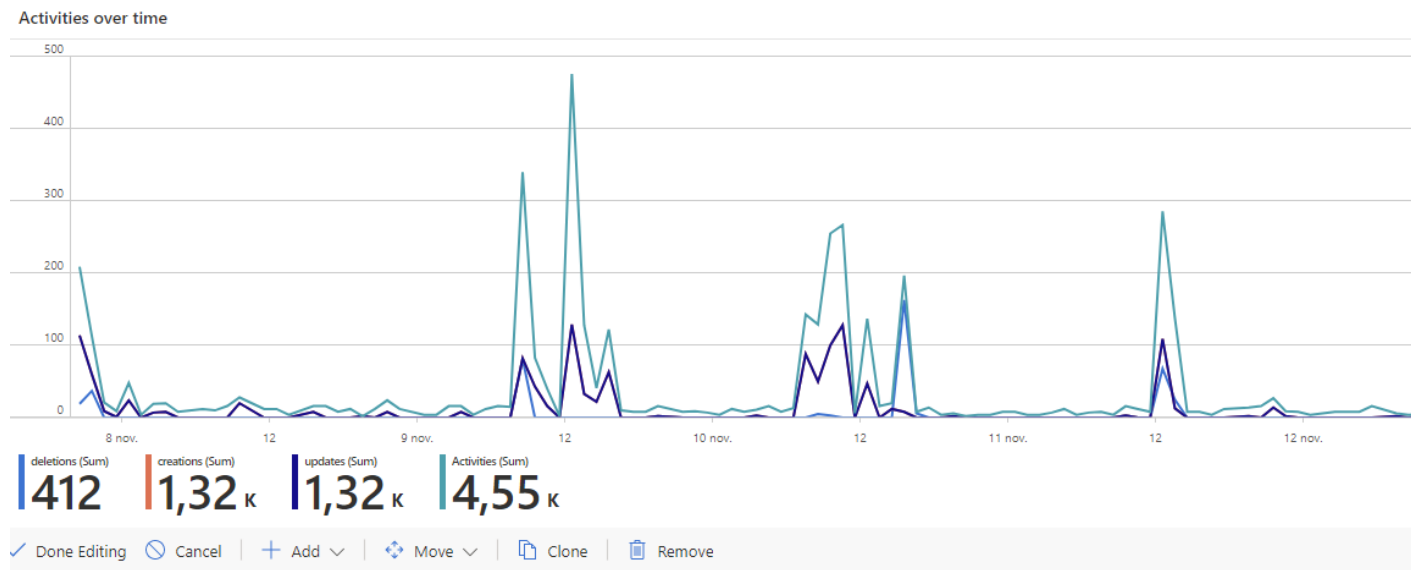




# Workbooks

- KQL can be used as well in Azure Monitor Workbooks
- Dynamic filtering in the workbook helps a lot of in data visualization

```
AzureActivity
| where "{Caller:table}" == "All" or Caller in ({Caller})
| where "{ResourceGroup:table}" == "All" or ResourceGroup in ({ResourceGroup})
| summarize deletions = countif(OperationNameValue hassuffix "delete"), creations = countif(OperationNameValue hassuffix "write"), updates = countif(
OperationNameValue) by bin_at(TimeGenerated, 1h, now())
```



# Variables

▶ Run Time range : Set in query Save Share + New alert rule Export Pin to ...

```
1 let start_time = ago(2d);
2 let end_time = start_time + 12h;
3 SigninLogs
4 | where TimeGenerated > start_time and TimeGenerated < end_time
5 | summarize count() by UserPrincipalName, AppDisplayName, bin(TimeGenerated, 1h)
```

Results Chart Add bookmark 🔍

<input type="checkbox"/> TimeGenerated [UTC]	UserPrincipalName	AppDisplayName	count_
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1
<input type="checkbox"/> > 2022-11-13 06.00.00.000	mika.vilpo@erikoisliikemiehet.fi	Kusto Web Explorer	5
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	1
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1

Columns

# DEMO

- Variable Query
- Variable Query Parameter
- Variable Dynamic

A large, bold black number '3' is centered on a gray background. A white circle is centered behind the number, and a vertical white line passes through its center. The background is divided into a dark gray upper-left quadrant and a lighter gray lower-right quadrant by a diagonal line.

# Variables, queries and materialization

```
1 let start_time = ago(2d);
2 let end_time = start_time + 12h;
3 let userTitles=
4   materialize(IdentityInfo
5   | project UserPrincipalName=AccountUPN, JobTitle);
6 SigninLogs
7   | where TimeGenerated > start_time and TimeGenerated < end_time
8   | summarize count() by UserPrincipalName, AppDisplayName, bin(TimeGenerated, 1h)
9   | join kind=inner userTitles on $left.UserPrincipalName == $right.UserPrincipalName
10  | project UserPrincipalName, AppDisplayName, TimeGenerated, count_, JobTitle
```

Results Chart				
UserPrincipalName	AppDisplayName	TimeGenerated [UTC]	count_	JobTitle
> markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	2022-11-14 05.00.00.000	1	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-14 05.00.00.000	57	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-13 22.00.00.000	178	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	2022-11-13 21.00.00.000	1	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-13 21.00.00.000	55	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	2022-11-14 05.00.00.000	1	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-14 05.00.00.000	57	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-13 22.00.00.000	178	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	2022-11-13 21.00.00.000	1	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-13 21.00.00.000	55	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	2022-11-14 05.00.00.000	1	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-14 05.00.00.000	57	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2022-11-13 22.00.00.000	178	Regional Director, Containerization
> markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	2022-11-13 21.00.00.000	1	Regional Director, Containerization

# Variables in queries with parameters

[Run](#) | Time range: Last 24 hours | [Save](#) | [Share](#) | [New alert rule](#) | [Export](#) | [Pin to](#) | [Format query](#) | ...

```
1 let HelloX = (s:string) { strcat("Hello, ", s, "!")};
2 IdentityInfo
3 | where GivenName != ""
4 | distinct GivenName
5 | extend Greetings=HelloX(GivenName)|
```

[Results](#) | [Chart](#)

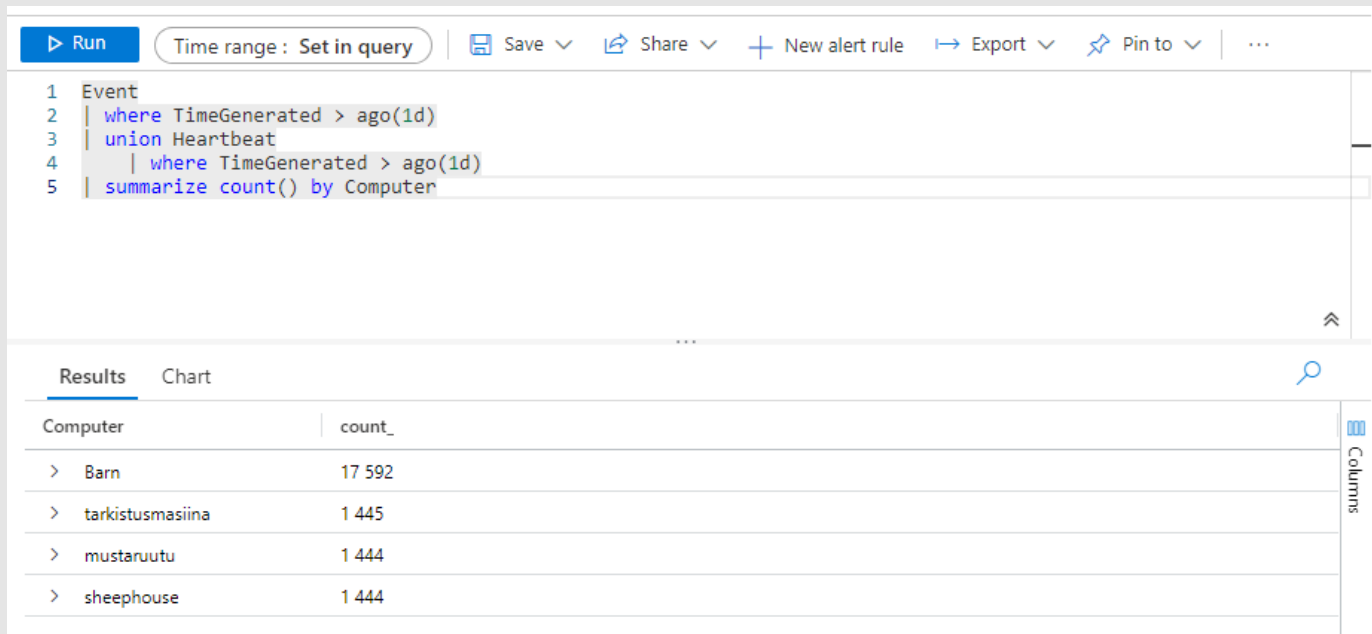
Greetings	GivenName
> Hello, Antti!	Antti
> Hello, Essi!	Essi
> Hello, Markus!	Markus
> Hello, Mika!	Mika
> Hello, ERP!	ERP
> Hello, Subscription!	Subscription
> Hello, Jani!	Jani
> Hello, Jari!	Jari
> Hello, Atte!	Atte

0s 589ms | Display time (UTC+00:00) | [Query details](#) | 1 - 9 of 9



# Unions and Joins

# Union



The screenshot shows a query editor interface. At the top, there's a toolbar with buttons for 'Run', 'Save', 'Share', 'New alert rule', 'Export', 'Pin to', and a menu icon. Below the toolbar, the query text is as follows:

```
1 Event
2 | where TimeGenerated > ago(1d)
3 | union Heartbeat
4 |   where TimeGenerated > ago(1d)
5 | summarize count() by Computer
```

Below the query editor, there's a 'Results' tab selected, showing a table with two columns: 'Computer' and 'count\_'. The table contains four rows of data:

Computer	count_
> Barn	17 592
> tarkistusmasiina	1 445
> mustaruutu	1 444
> sheephouse	1 444

- Join two tables together
- Kinds available **inner** or **outer**
- Outer is default and results everything, inner only columns with same name

# Joins

▶ Run

Time range: Set in query

Save

Share

New alert rule

Export

Pin to

Format query

```
1 let start_time = ago(2d);
2 let end_time = start_time + 12h;
3 SigninLogs
4 | where TimeGenerated > start_time and TimeGenerated < end_time
5 | summarize count() by UserPrincipalName, AppDisplayName, bin(TimeGenerated, 1h)
6 | join kind=inner IdentityInfo on $left.UserPrincipalName == $right.AccountUPN
7 | project UserPrincipalName, AppDisplayName, TimeGenerated, count_, JobTitle
```

Results | Chart | Add bookmark

<input type="checkbox"/> TimeGenerated [UTC]	UserPrincipalName	AppDisplayName	count_	JobTitle
<input type="checkbox"/> > 2022-11-13 06.00.00.000	mika.vilpo@erikoisliikemiehet.fi	Kusto Web Explorer	5	Nordic Director, Azure Identity Services
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 06.00.00.000	mika.vilpo@erikoisliikemiehet.fi	Kusto Web Explorer	5	Nordic Director, Azure Identity Services
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	2	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 06.00.00.000	mika.vilpo@erikoisliikemiehet.fi	Kusto Web Explorer	5	Nordic Director, Azure Identity Services
<input type="checkbox"/> > 2022-11-13 06.00.00.000	mika.vilpo@erikoisliikemiehet.fi	Kusto Web Explorer	5	Nordic Director, Azure Identity Services
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Portal	1	Regional Director, Containerization
<input type="checkbox"/> > 2022-11-13 04.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regional Director, Containerization



# Left or Right?

LEFT

▶ Run

Time range : Set in query

Save

Share

+ New alert rule

Export

Pin to

Format query

```
1 let start_time = ago(2d);
2 let end_time = start_time + 12h;
3 SigninLogs
4 | where TimeGenerated > start_time and TimeGenerated < end_time
5 | summarize count() by UserPrincipalName, AppDisplayName, bin(TimeGenerated, 1h)
6 | join kind=inner IdentityInfo on $left.UserPrincipalName == $right.AccountUPN
7 | project UserPrincipalName, AppDisplayName, TimeGenerated, count_, JobTitle
```

RIGHT

Results

Chart

Add bookmark

<input type="checkbox"/> TimeGenerated [UTC]	UserPrincipalName	AppDisplayName	count_	JobTitle
<input type="checkbox"/> > 2022-11-13 06.00.00.000	mika.vilpo@erikoisliikemiehet.fi	Kusto Web Explorer	5	Nord
<input type="checkbox"/> > 2022-11-13 07.00.00.000	markus.lintuala@erikoisliikemiehet.fi	Azure Virtual Desktop Client	1	Regio



## Join return – Output schema

- Leftanti, leftsemi
  - The result has columns from the **LEFT** side only
- Rightanti, rightsemi
  - The result has columns from the **RIGHT** side only
- Innerunique, inner ,leftouer, rightouter, fullouter
  - All columns, if columns with a same name **RIGHT** columns will be renamed

- leftanti, leftantisemi
  - All records from the **left** side that do not have a match on **right**
- rightanti, rightantisemi
  - All records from the **right** side that do not have a match on **left**
- innerunique (or unspecified)
  - One row from **left** side that outputs all rows from the **right** side
- leftsemi
  - Returns all the records from **left** side that have a match on **right** side
- rightsemi
  - Returns all the records from **right** side that have a match on **left** side

Join return –  
Output  
records 1/2

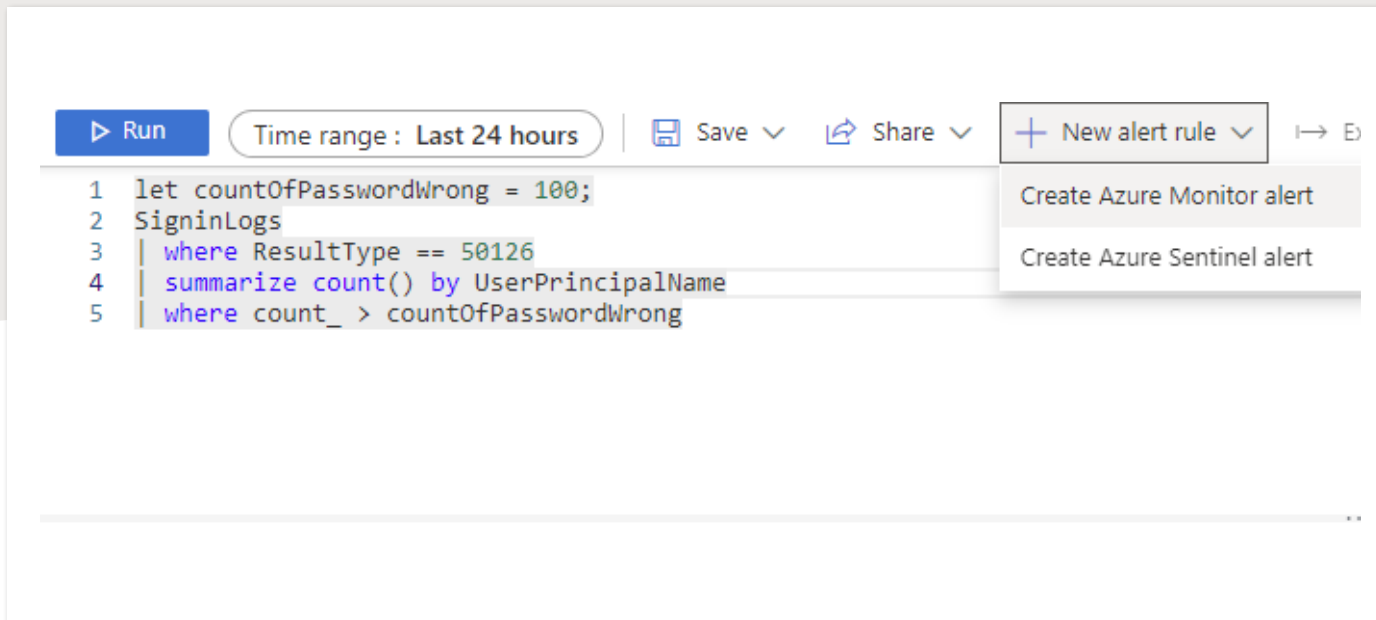
- inner
  - Returns all the records from **both** sides that have a match
- fullouter
  - Returns all the records from **both** sides also the null ones
- leftouter
  - Returns all the records from **left** side and only matched records from the **right** side
- rightouter
  - Returns all the records from **right** side and only matched records from the **left** side

Join return –  
Output  
records 2/2



Data alerts and exports

# Data alerts




- When you have a great KQL query for alert rule in Sentinel logs, you can transfer it straight to new scheduled query wizard
- Use variables to customize your alert thresholds and document it to description of query – no need to be KQL guru for changes

# Data exports

- Microsoft 365 Defender connector allows you to bring a raw data from Defender to Sentinel
- Why you want to do it?

Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >

## Microsoft 365 Defender (Preview) ...

**Microsoft 365 Defender (Preview)**

Connected Status

Microsoft Provider

⌚ -- Last Log Received

**Description**


Microsoft 365 Defender 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 365 Defender suite includes:


- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence
- Microsoft Defender Vulnerability Management
- Microsoft Purview Data Loss Prevention
- Azure Active Directory Identity Protection

Last data received  
--

**Related content**

 **2**  
Workbooks


 **4**  
Queries

 **72**  
Analytics rules templates

Data received [Go to log analytics](#)

**Note:** Office 365 da

**Instructions** Next s


 **Prerequ**

To integr

✓ **Wor**

✓ **Teni**

ⓘ **Lice**

 **Configi**

Connect  
Connect


[Discor](#)

# Data exports

- Microsoft 365 Defender connector allows you to bring a raw data from Defender to Sentinel
- You want to correlate the data with other sources in your Sentinel

Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >

## Microsoft 365 Defender (Preview) ...

**Microsoft 365 Defender (Preview)**

Connected Status

Microsoft Provider

⌚ -- Last Log Received

Description

Microsoft 365 Defender 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 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence
- Microsoft Defender Vulnerability Management
- Microsoft Purview Data Loss Prevention
- Azure Active Directory Identity Protection

Last data received

--

Related content

2 Workbooks

4 Queries


72 Analytics rules templates

Data received

[Go to log analytics](#)


Note: Office 365 da

Instructions Next s

 **Prerequ**

To integr

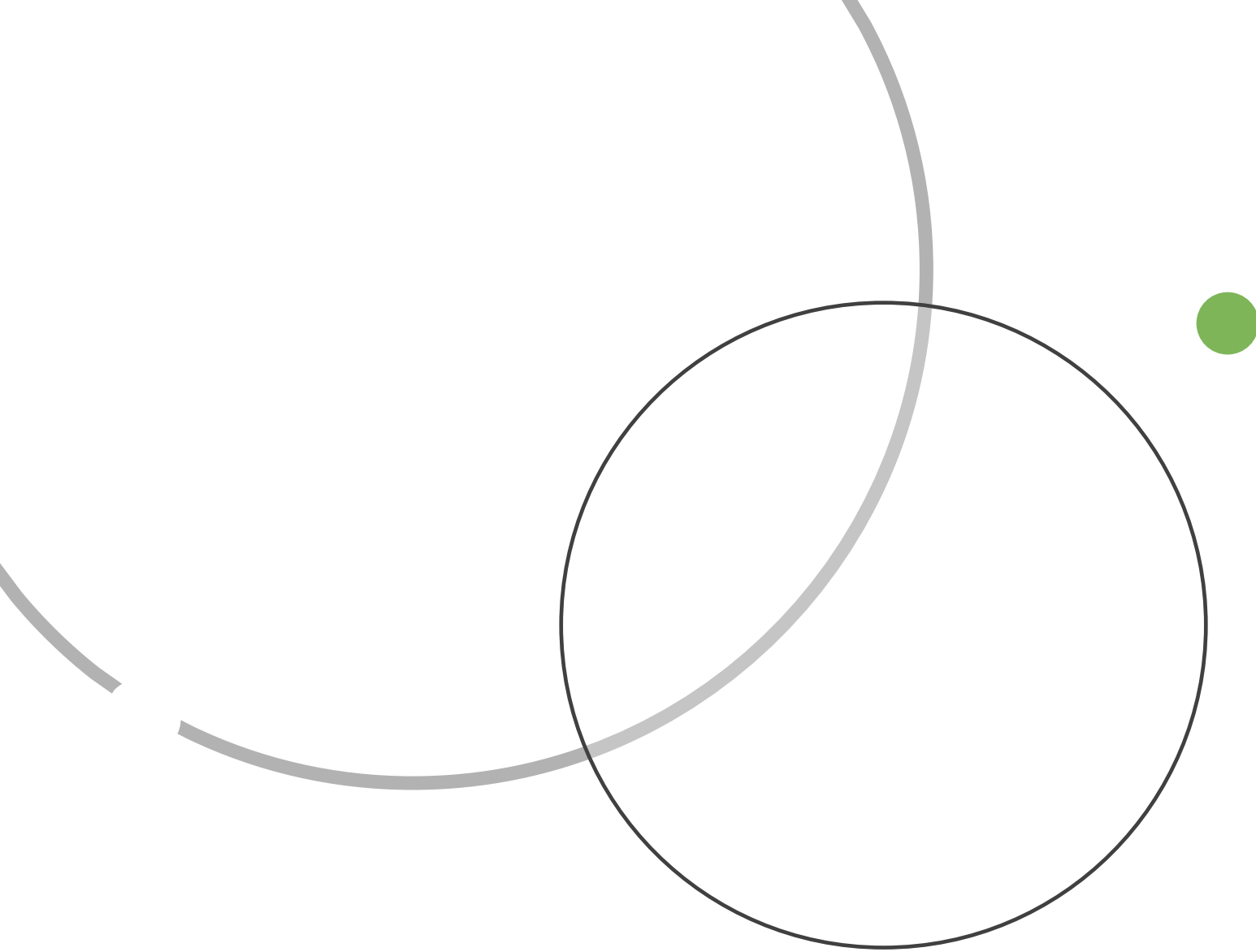
- ✓ **Wor**
- ✓ **Teni**
- ⓘ **Lice**

 **Config**

Connect Connect

[Discor](#)





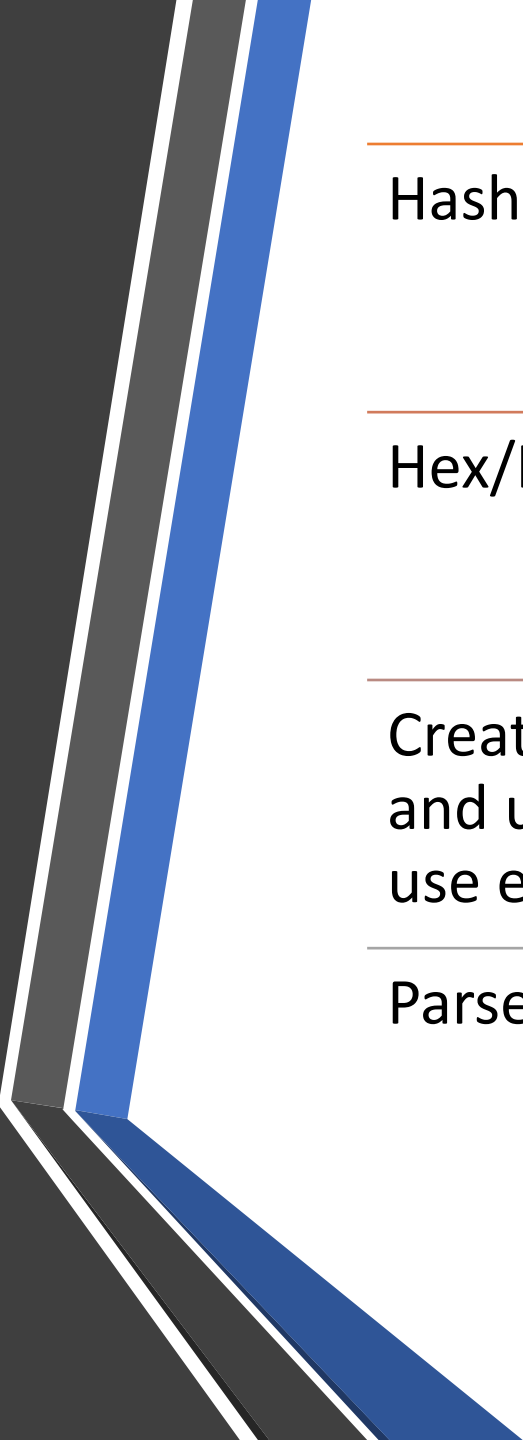
# KQL Functions

# KQL functions

Stored functions can be saved to KQL database for later usage

Query-defined functions in let-variables can be used later in that specific query

Built-in functions that are hard-coded defined by Microsoft



Good  
functions for  
endpoint  
specialists

---

Hash-functions (md5/sha1/sha256)

---

Hex/Int-conversion

---

Create troubleshooting queries to log analytics  
and upload problematic logs to blob storage and  
use externaldata function to query results

---

Parse function for text logs

# External data

▶ Run

Time range : Last 24 hours

Save

Share

New alert rule

Export

Pin to

Format query

...

```
1 externaldata(name:string, timestamp:datetime)
2 [
3   @"https://sademomatskua.blob.core.windows.net/kql/externaldata-demo.txt"
4   h@"?sp=r&st=2022-11-17T19:58:16Z&se=2022-11-22T14:30:00Z&spr=https&sv=2021-06-08&sr=b&
5   sig=8reYuvA7U%2FtkNpw%2BofKqt02rD2c9gEZEupPfC5bH%2FfM%3D"
6 ]
7 | join kind=inner ( IdentityInfo | where GivenName != "" | project gn=tolower(GivenName), AccountUPN ) on $left.name ==
8   $right.gn
```

Results

Chart

🔍

name	timestamp [UTC]	gn	AccountUPN
> markus	2022-11-22 12.00.00.000	markus	markus.demo@erikoisliikemiehet.fi
> mika	2022-11-22 12.02.00.000	mika	mika.ketola@elisacloud.onmicrosoft.com
> mika	2022-11-22 12.02.00.000	mika	mika.vilpo@elisa.fi
> mika	2022-11-22 12.02.00.000	mika	mikan.demo@erikoisliikemiehet.fi
> mika	2022-11-22 12.02.00.000	mika	mika.vilpo@erikoisliikemiehet.fi
> markus	2022-11-22 12.00.00.000	markus	markus.lintuala@erikoisliikemiehet.fi
> mika	2022-11-22 12.02.00.000	mika	mika.tolvanen@partners.erikoisliikemiehet.fi
> markus	2022-11-22 12.00.00.000	markus	markus.lintuala@erikoisliikemiehet.fi
> markus	2022-11-22 12.00.00.000	markus	markus.lintuala@erikoisliikemiehet.fi
> mika	2022-11-22 12.02.00.000	mika	mika.ketola@elisacloud.onmicrosoft.com
> markus	2022-11-22 12.00.00.000	markus	markus.demo@erikoisliikemiehet.fi
> mika	2022-11-22 12.02.00.000	mika	mika.tolvanen@partners.erikoisliikemiehet.fi

0s 652ms | Display time (UTC+00:00) ▼

Query details | 1 - 12 of 179

The background features a dark gray field with a large, light gray circle on the right and a smaller, white circle on the left. A thin white line forms a crosshair, intersecting at the center. A thick black number '4' is positioned in the center, partially overlapping the circles and the crosshair.

# 4

DEMO

---

External data

Good  
functions for  
security  
specialists

- base64 encoders/decoders
- Hash-functions (md5/sha1/sha256)
- ipv4 functions
- Text parsers
- JSON parsers
- URL decoder
- Anomaly detection functions










# Hidden gems, tips, best practices

---



# Hidden columns

	<b>_TimeReceived</b>	Date and time, when the row was received through the ingestion
	<b>Type</b>	Name of the table
	<b>_ItemId</b>	Record's unique identifier
	<b>_ResourceId</b>	Azure Resource ID
	<b>_SubscriptionId</b>	Azure Subscription ID
	<b>_IsBillable</b>	Tue/false
	<b>_BilledSize</b>	Amount of data in bytes that is billed, if <b>_IsBillable</b> is <b>true</b>

[Run](#) | Time range: Last 24 hours | [Save](#) | [Share](#) | [New alert rule](#) | [Export](#) | [Pin to](#) | [Format query](#)

```
1 SigninLogs
2 | project UserPrincipalName, _TimeReceived, _ItemId, _IsBillable, BilledSizeKB=round(_BilledSize/1000,1)
3 | union (AzureActivity | project _IsBillable, BilledSizeKB=round(_BilledSize/1000,1), _ResourceId, _SubscriptionId)
4
5 | summarize sum(BilledSizeKB) by _IsBillable
```

Results | Chart

UserPrincipalName	_TimeReceived [UTC]	_ItemId	_IsBillable	BilledSizeKB	_ResourceId
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.03.45.000	bb64cde4-6773-11ed-94ee-60...	True	4,2	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.04.24.000	d53a5372-6773-11ed-9983-00...	True	4,1	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.58.17.000	59050937-677b-11ed-9983-00...	True	4,2	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 20.00.29.000	a7e2e006-677b-11ed-9983-60...	True	4,2	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 20.33.46.000	4e82a09d-6780-11ed-9983-60...	True	4	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.05.05.000	eb339490-6773-11ed-9983-00...	True	4,2	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.05.20.000	f318eb26-6773-11ed-9983-604...	True	4,1	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 18.52.01.000	16f62587-6772-11ed-94ee-000...	True	4,2	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 18.52.39.000	2e5176be-6772-11ed-9983-60...	True	4,2	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 18.52.41.000	2f5e4f8a-6772-11ed-94ee-604...	True	4,2	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.28.28.000	2faa4303-6777-11ed-9983-604...	True	4,1	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.29.33.000	5557106e-6777-11ed-9983-00...	True	4,7	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.29.33.000	55571070-6777-11ed-9983-00...	True	4,3	
> markus.lintuala@erikoisliikemiehet.fi	2022-11-18 19.29.33.000	55e03da2-6777-11ed-9981-00...	True	4,2	

0s 681ms | Display time (UTC+00:00) | [Query details](#) | 1 - 14 of 1117



```
▶ Run | Time range : Last 24 hours | Save | Share | + New alert rule | Export | Pin to | Format query | ...  
1 print x="https://contoso.blob.core.windows.net/container/blob.txt?"  
2 ..h'sv=2022-11-12&se=2022-11-13T0...
```

# String obfuscation

When you want to hide something from logs, telemetry etc.

# Tips & Tricks

- Escape “Demo \ or more” in strings with another backslash “Demo \\ or more” or by @ sign in front of the string @”Demo \ or more”
- Give all columns descriptive names – you are not always the one who is looking for the query
- Use **h** in-front of string to obfuscate it from logs/telemetry/analysis
- Use let-variables when you are creating a query that is going to be saved for later use



# Best practices



Less is more



# Best practices

- Start always with a time filter
- If looking for full strings, use **has** instead of **contains**
- Use case sensitive operators if possible **==** vs. **=~** or **contains\_cs** vs. **contains**
- Limit search by column, avoid **\*** if possible
- Extract fields from dynamic objects instead of querying the whole object
- When using data more than once, put it on variable and materialize it, if the query takes a long time
- Use **Column1 =~ "low str"** instead of **tolower(Column1) == "low str"**
- Use column with fewer rows on the left when joining

Azure Data Explorer

MarkusFreeCluster. MarkusFreeCluster.mydb 5-morning Get the channel MessageDecrypter x +

Home Data Query Dashboards (Preview) My cluster (Preview)

Filter...

MarkusFreeCluster

mydb

Functions

Onboarding

Scope: @MarkusFreeCluster/mydb

Table 1 Stats

Search UTC Done (0.541 s) 1 records

print\_0

Columns

# Azure Data Exploer

Home > Microsoft Sentinel > Microsoft Sentinel

# Microsoft Sentinel

Erikosliikemiehet

+ Create Manage view ...

Filter for any field...

Name ↑↓

erikosliikemiehet

Microsoft Sentinel | Logs

Selected workspace: 'erikosliikemiehet'

Search

New Query 1\* x +

erikosliikemiehet

Run Time range : Last 24 hours Save Share + New alert rule Export Pin to ...

1 SigninLogs

2 | take 100

Results Chart Add bookmark

<input type="checkbox"/>	TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category
<input type="checkbox"/>	> 2022-11-15 19.27.00.182	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 19.28.42.942	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 18.49.26.123	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 18.49.26.153	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 18.50.06.448	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 18.50.06.448	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 19.28.42.699	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 19.28.33.599	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 19.28.34.489	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 19.28.43.039	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 19.28.43.327	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 19.28.33.748	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 18.26.58.883	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-14 20.50.43.000	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL
<input type="checkbox"/>	> 2022-11-15 08.26.49.204	/tenants/5b96d754-4eef-4955-...	Sign-in activity	1.0	SignInL

0s 745ms | Display time (UTC+00:00) Query details | 1 - 15 of 100

# Log Analytics + Sentinel

## Advanced Hunting

Help resources Schema reference Try the new Hunting page

New query Create new

Schema Functions Queries

### Alerts

- AlertInfo
- AlertEvidence

### Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

### Email & collaboration

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
- UrlClickEvents

### Devices

Run query Save Share link

Last 7 days Create detection rule

### Query

```
1 DeviceInfo
2
```

Getting Started Results

Export

3006 items

Search

0:0.47

Low

Chart Type

Customize columns

<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	ClientVersion	PublicIP	OSArchitecture
<input type="checkbox"/>	Nov 15, 2022 9:04:12 PM	726dd4a54cacac4726...	mustaruutu.44hb54o...	30.122092.18527.0	(info)	64-bit
<input type="checkbox"/>	Nov 15, 2022 9:08:45 PM	864f930135b62bbcc3...	sheephouse	30.122092.18527.0	(info)	64-bit
<input type="checkbox"/>	Nov 15, 2022 9:14:12 PM	726dd4a54cacac4726...	mustaruutu.44hb54o...	30.122092.18527.0	(info)	64-bit
<input type="checkbox"/>	Nov 15, 2022 9:12:54 PM	64128aaccfa265e3e7...	barn	10.8210.17763.3650	(info)	64-bit
<input type="checkbox"/>	Nov 15, 2022 9:18:45 PM	864f930135b62bbcc3...	sheephouse	30.122092.18527.0	(info)	64-bit
<input type="checkbox"/>	Nov 15, 2022 9:24:12 PM	726dd4a54cacac4726...	mustaruutu.44hb54o...	30.122092.18527.0	(info)	64-bit
<input type="checkbox"/>	Nov 15, 2022 8:48:44 PM	864f930135b62bbcc3...	sheephouse	30.122092.18527.0	(info)	64-bit

# Microsoft 365 Defender

[Home](#) >

## Azure Resource Graph Explorer

×

scope

More (1)

Categories Table

Search

- > General
- > AI + machine learning
- > Analytics
- ▼ Compute
  - > Citrix Virtual Apps Essentials
  - > Citrix Virtual Desktops Essentials
  - > Container Apps
  - > Cloud services (classic)
  - > Virtual machines (classic)
  - > Availability sets
  - > Disks
  - > Azure compute galleries
  - > VM image definitions
  - > VM image versions
  - > Host groups
  - > Hosts
  - > Images
  - > Proximity placement groups
  - > Snapshots
  - > Virtual machines
  - > Virtual machine scale sets
  - > Application groups
  - > SAP HANA on Azure
  - > Maintenance Configurations
- > Containers
- > Databases

+ New query Open a query Run query Save Save as Feedback

Query 1

```
1 resources
2 | where type == "microsoft.compute/virtualmachines"
```

Get started Results Charts Messages

Download as CSV Pin to dashboard

Formatted results Off

id ↑↓	name ↑↓	type ↑↓	tenantId ↑↓	kind ↑↓	location ↑↓	resourceGroup ↑↓	subscriptionId ↑↓	managedBy ↑↓	sku
/subscriptions/0db8ef...	tarkistusmasiina	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		0db8efd5-242d-404a-...		null
/subscriptions/7d2f7fb...	MEMCM	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		7d2f7fb8-ed30-46c4-b...		null
/subscriptions/983bfa...	refsql2019n01	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		983bfa76-cb6e-4ab2-...		null
/subscriptions/985a20...	VM-wintest01	microsoft.compute/vir...	5b96d754-4eef-4955-...		northeurope		985a2000-f34e-428e-...		null
/subscriptions/985a20...	VM-wintest02	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		985a2000-f34e-428e-...		null
/subscriptions/985a20...	VM-wintest03	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		985a2000-f34e-428e-...		null
/subscriptions/9ca723...	labvm01	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		9ca7237e-1d89-43f8-a...		null
/subscriptions/9ca723...	labvm02	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		9ca7237e-1d89-43f8-a...		null
/subscriptions/9ca723...	mustaruutu	microsoft.compute/vir...	5b96d754-4eef-4955-...		swedencentral		9ca7237e-1d89-43f8-a...		null
/subscriptions/45687e...	markusavd-0	microsoft.compute/vir...	5b96d754-4eef-4955-...		westeurope		45687e3b-908d-4f2d-		null

< Previous Page 1 of 1 Next >

Results: 10 (Duration: 00:00.368)

# Azure Graph Queries



# How to train yourself?

- [SC-200: Create queries for Microsoft Sentinel using Kusto Query Language \(KQL\) - Training | Microsoft Learn](#)
- [rod-trent/MustLearnKQL: Code included as part of the MustLearnKQL blog series \(github.com\)](#)
- [KQL/kql cheat sheet v01.pdf at master · marcusbakker/KQL · GitHub](#)
- [Kusto Detective Agency](#)
- [KQL Online Course: The Basics of Kusto Query Language | Pluralsight](#)



# Kusto Detective Agency 2022

<https://detective.kusto.io/>



KQL is the new  
PowerShell



# **Key takeaway**

## Key takeaway

*“It’s OK not to be a pro on day 1 and still be able to use tools like Microsoft Sentinel to monitor security for the environment.”*

- Rod Trent, 19.11.2021

Q & A



Markus Lintuala  
+358 40 585 5531  
markus.lintuala@elisa.fi

Slides available: [cloud/PublicSpeaking/MicrosoftArchitectDay2022](https://github.com/mmaraa/cloud) at main ·  
[mmaraa/cloud \(github.com\)](https://github.com/mmaraa/cloud)



# Kiitos!

Esitykset ja tallenteet on ladattavissa osoitteessa:  
<https://aka.ms/kumppaniarkkitehtiseminaari>

Microsoft Kumppaniarkkitehtiseminaari 22.11.2022