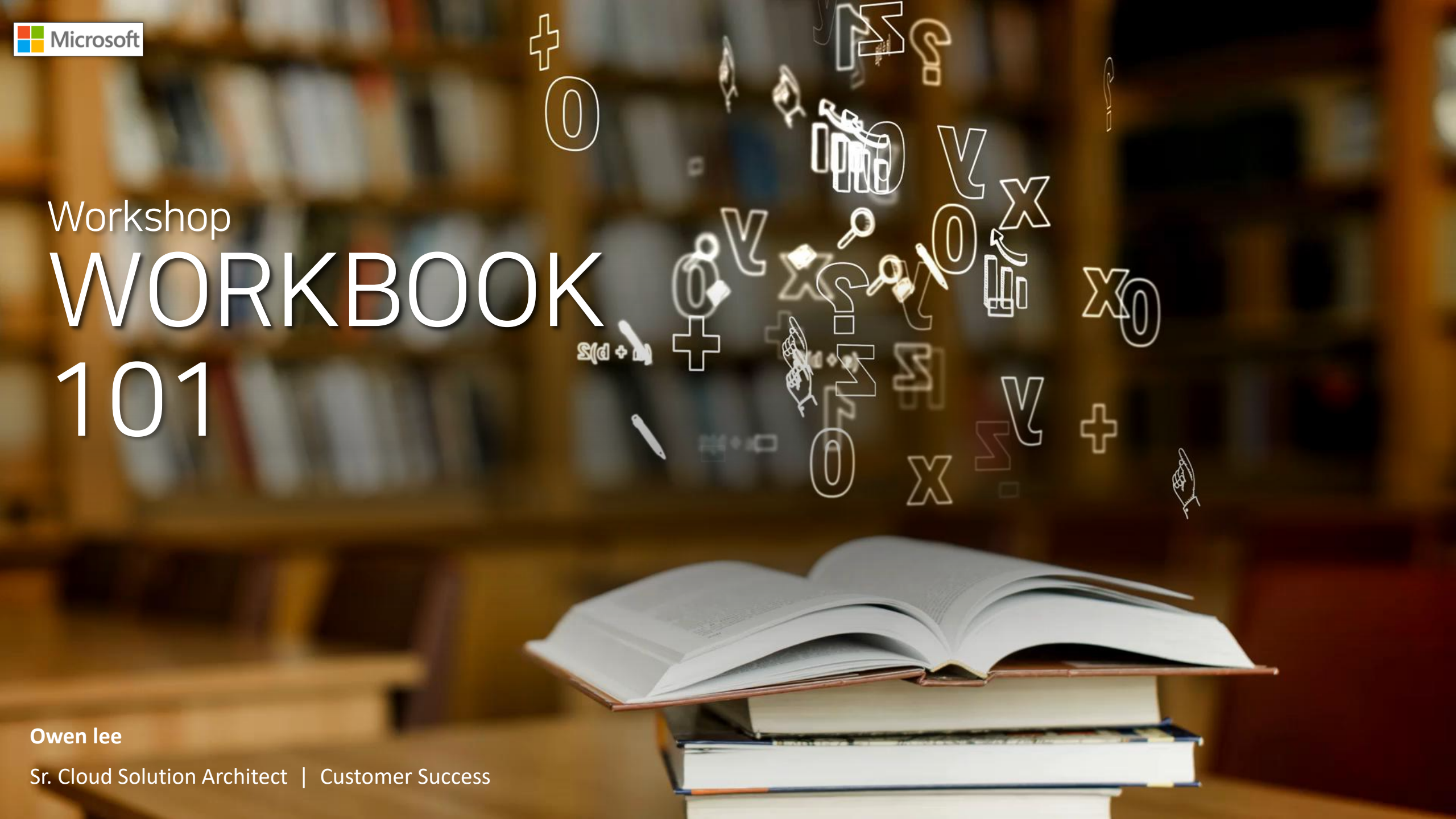
Microsoft

Workshop

WORKBOOK 101



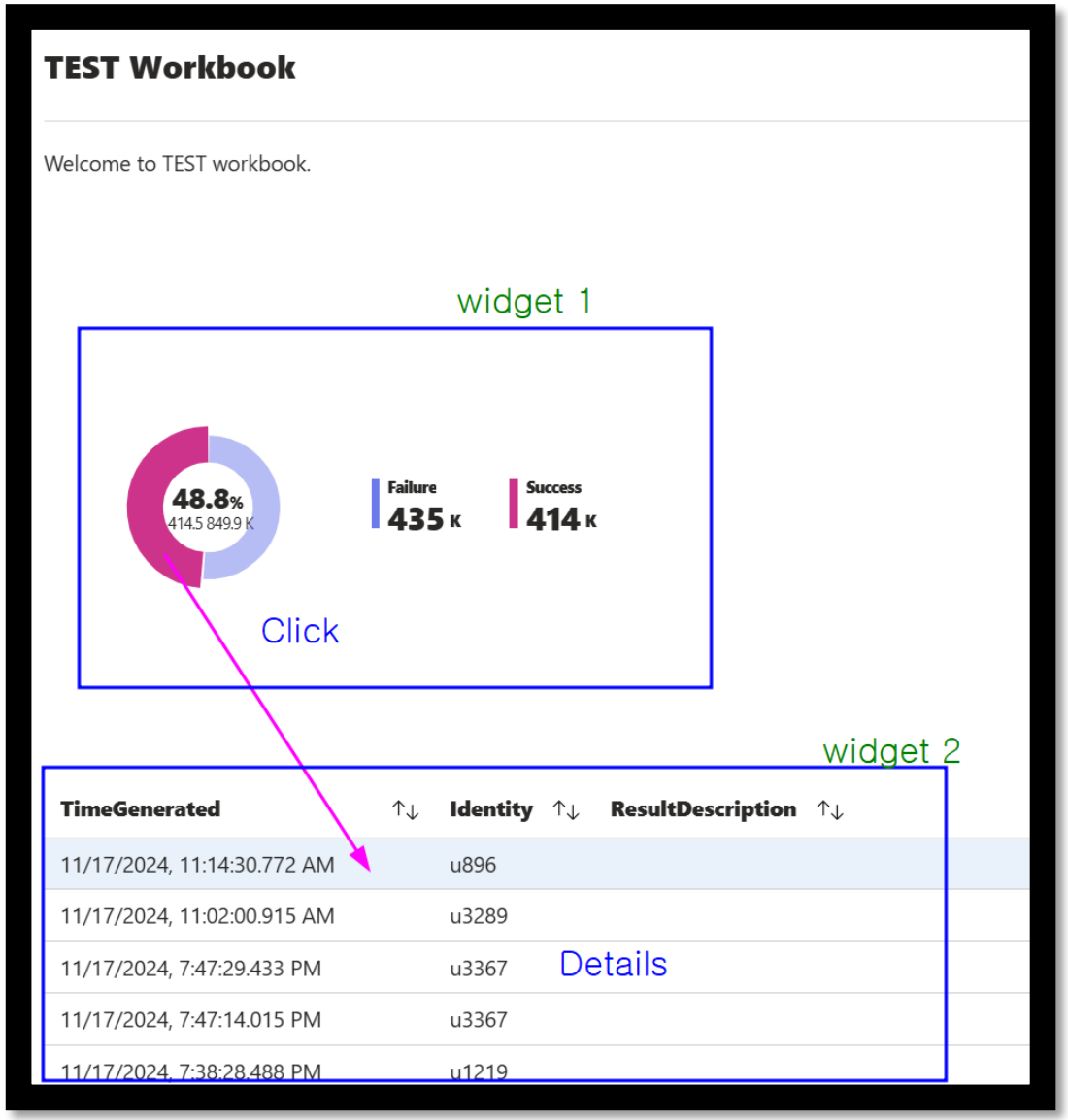
Owen lee

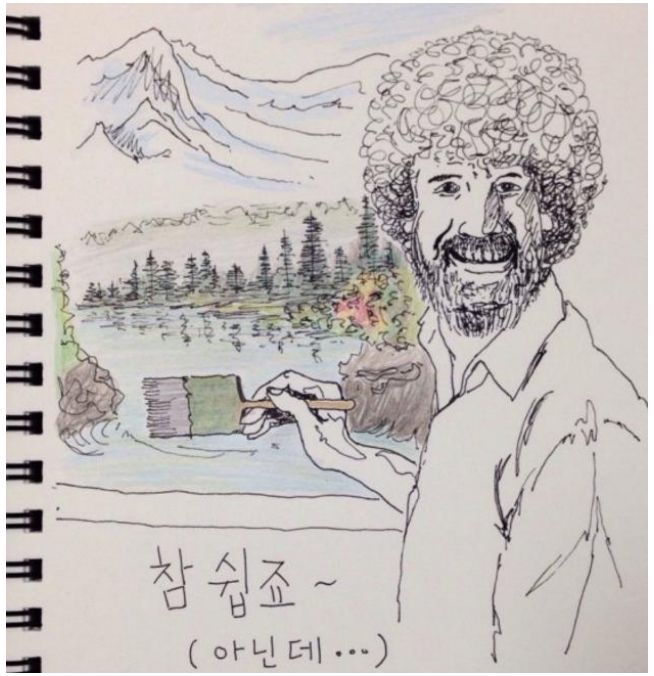
Sr. Cloud Solution Architect | Customer Success

Agenda

- Out of the box workbooks
- Custom workbooks
- Visualization types
- Parameters
- Advanced - Time brushing
- Advanced - Dynamic content in workbooks
- Advanced – Personalization
- Advanced - Tabs
- Sharing workbooks

Hands-on Lab - Simple Dynamic Dashboard





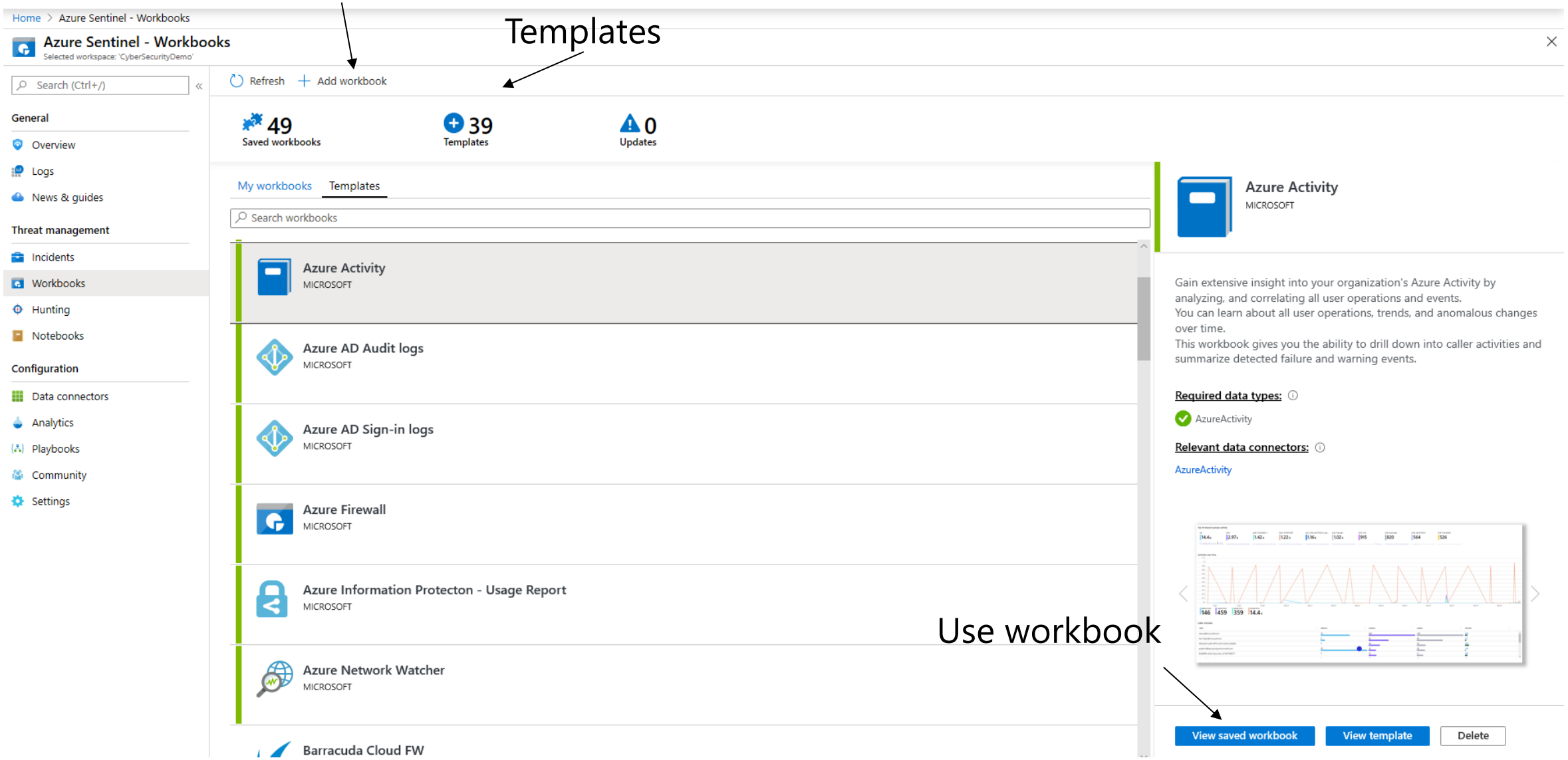
Microsoft

workbook visualizations

Out of the Box Workbooks

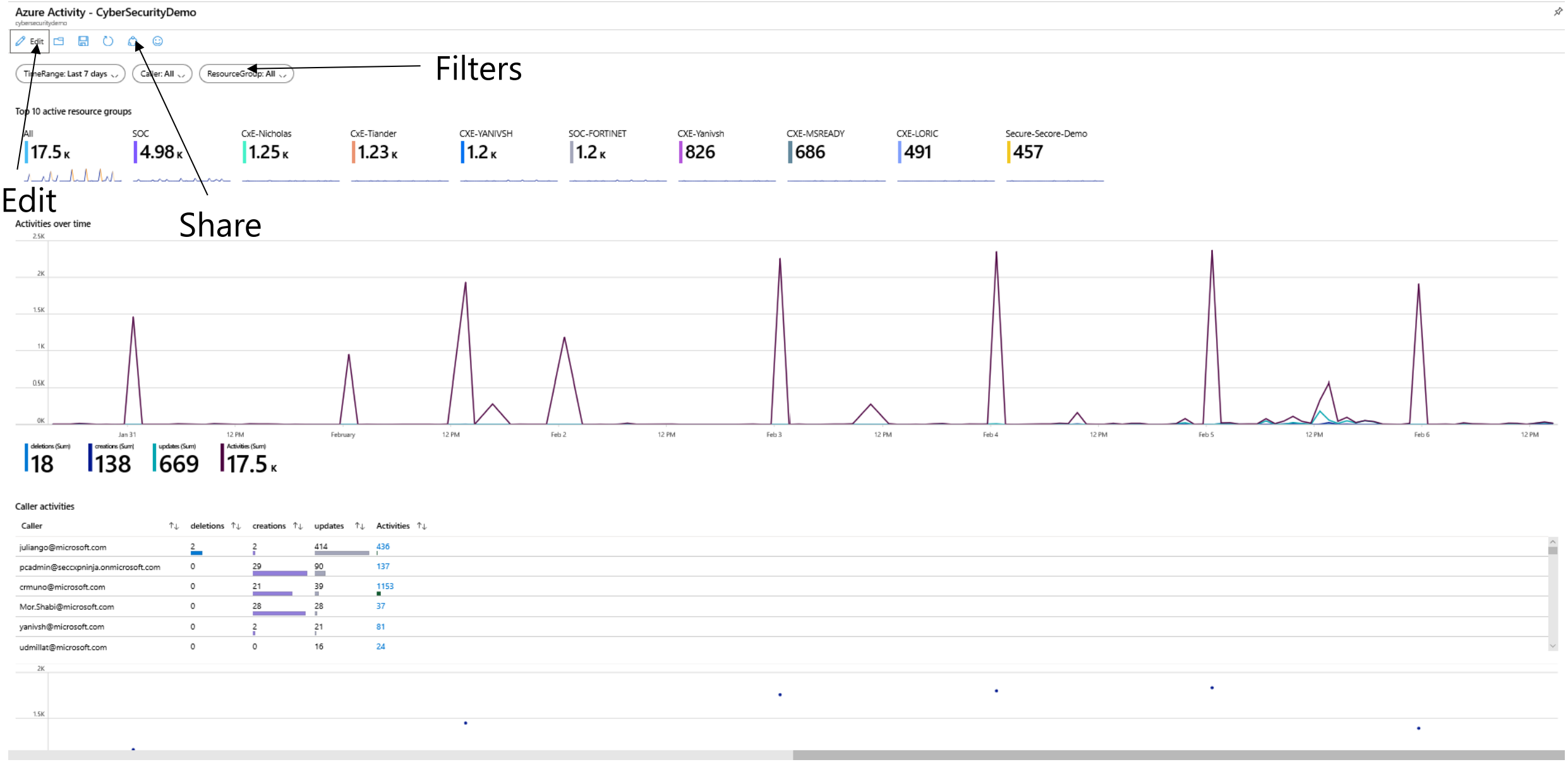
Add New Workbook

Templates

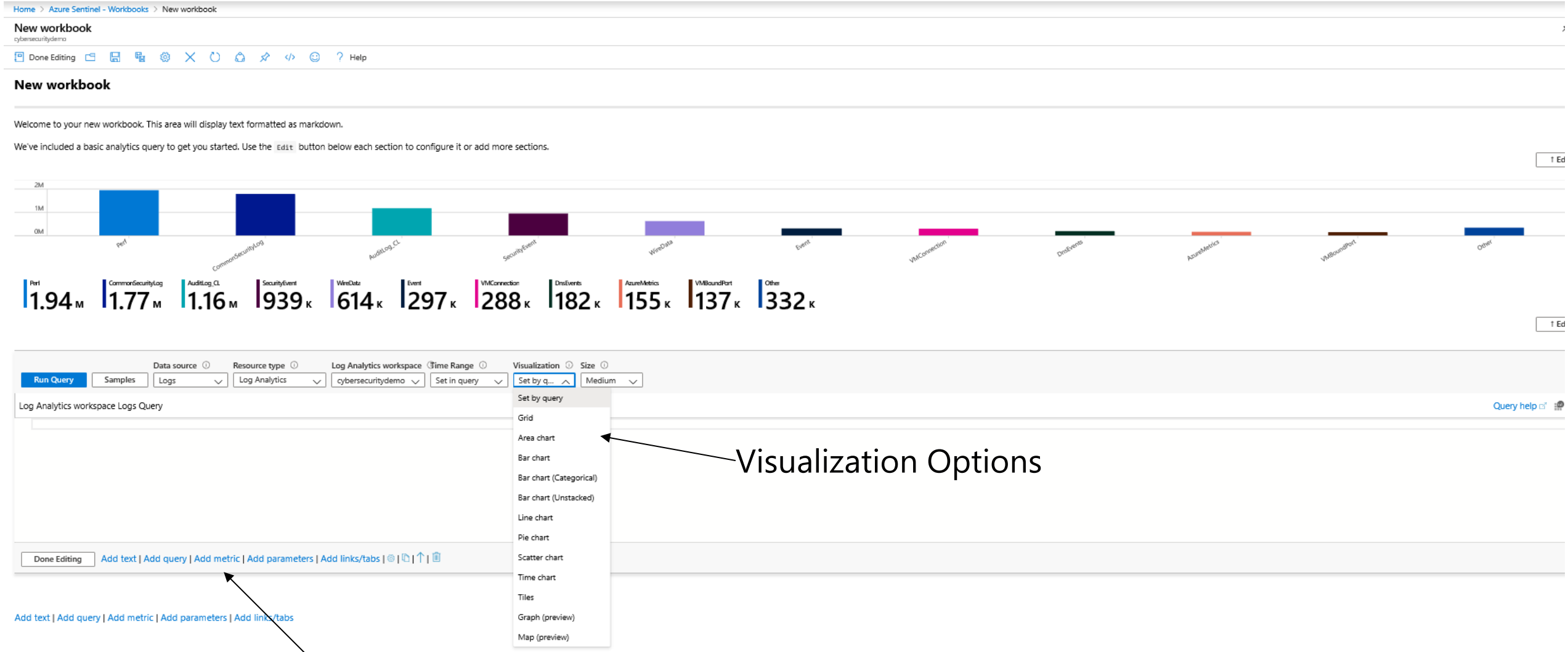


Use workbook

Workbooks in edit



Workbooks in edit

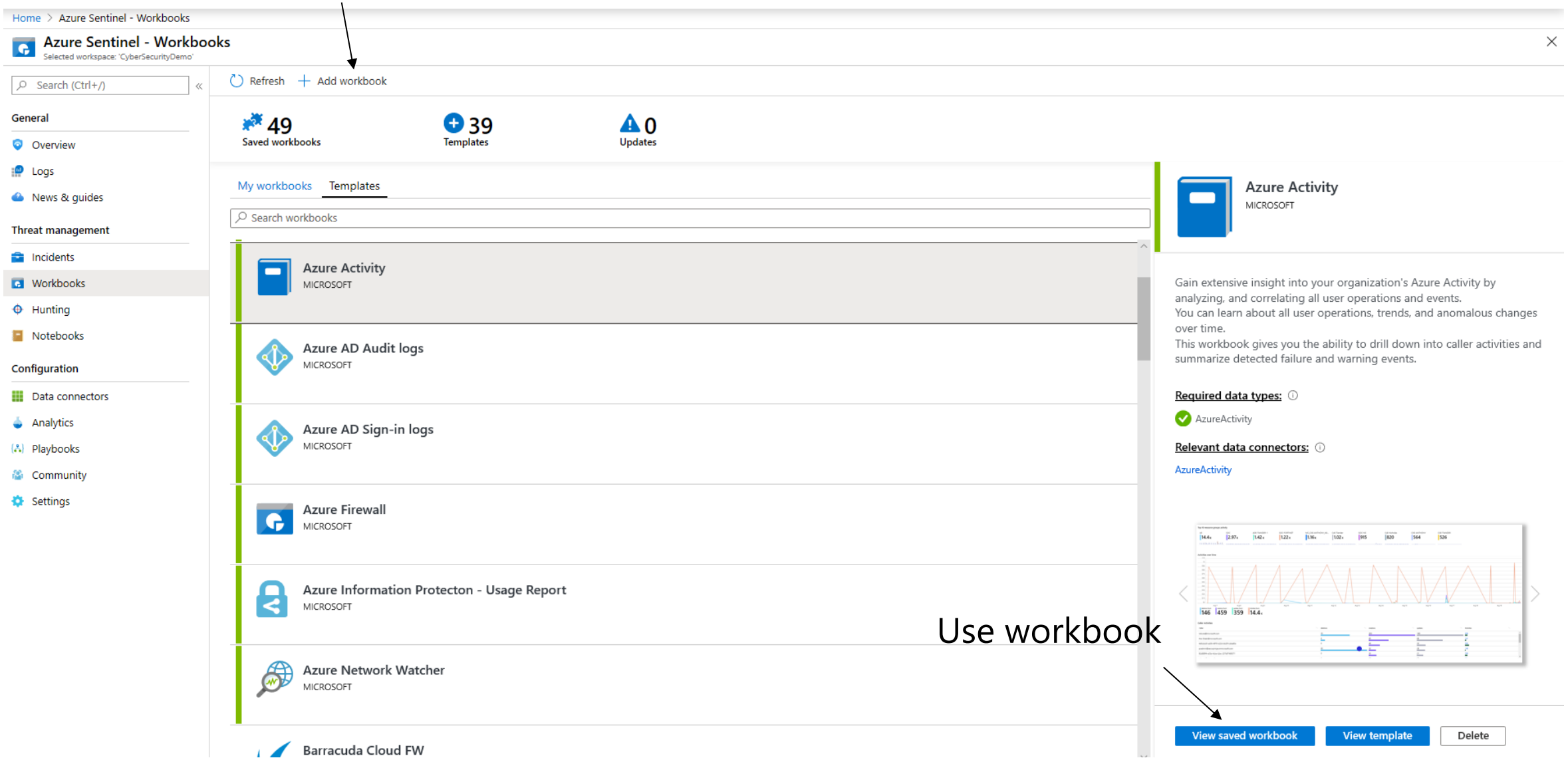


Visualization Options

Add Text, Query, Metric, Parameters, Links/tabs

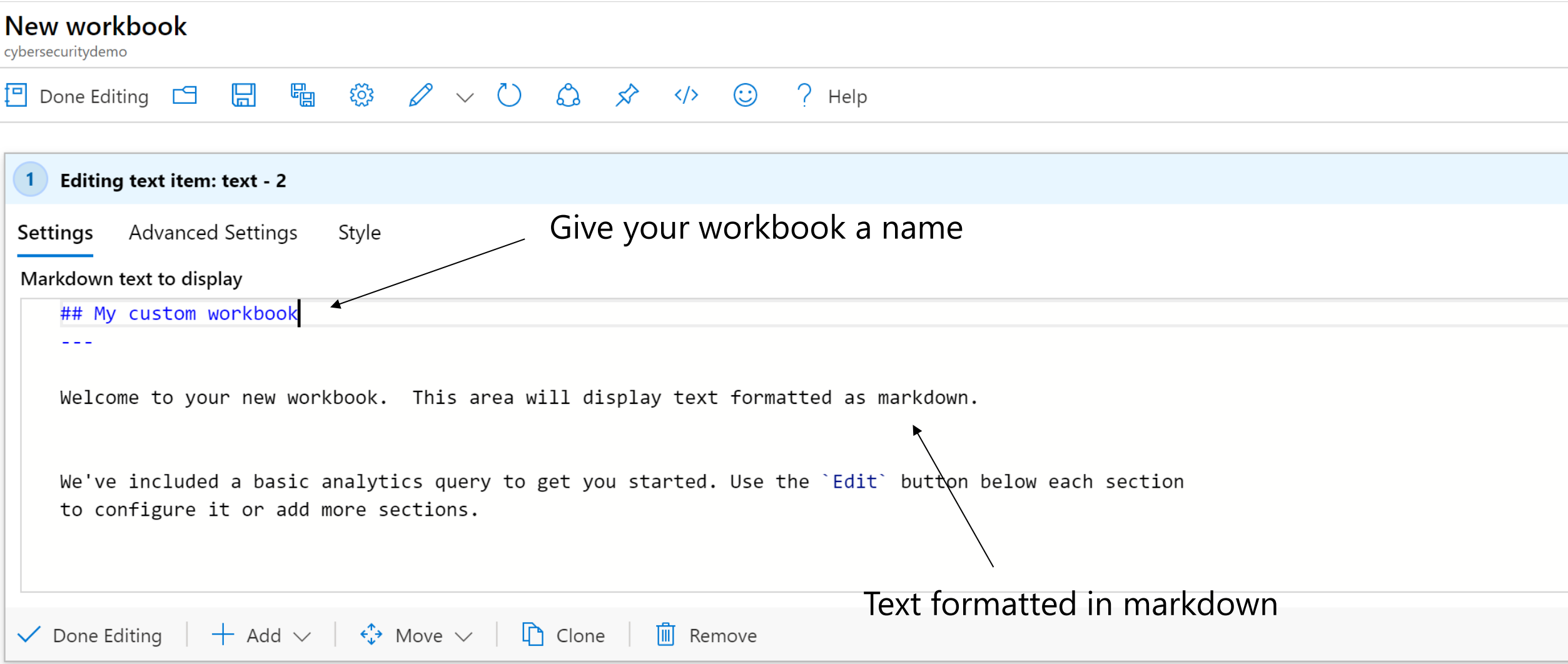
Custom Workbooks

Add New Workbook



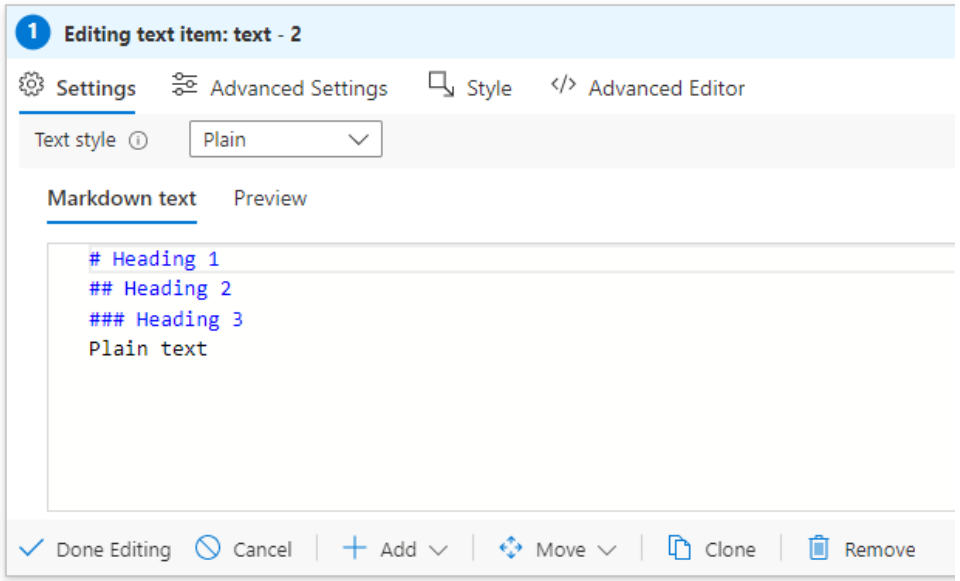
Use workbook

Custom Workbooks - Text



Custom Workbooks - Text

By typing this:



You'll get this:

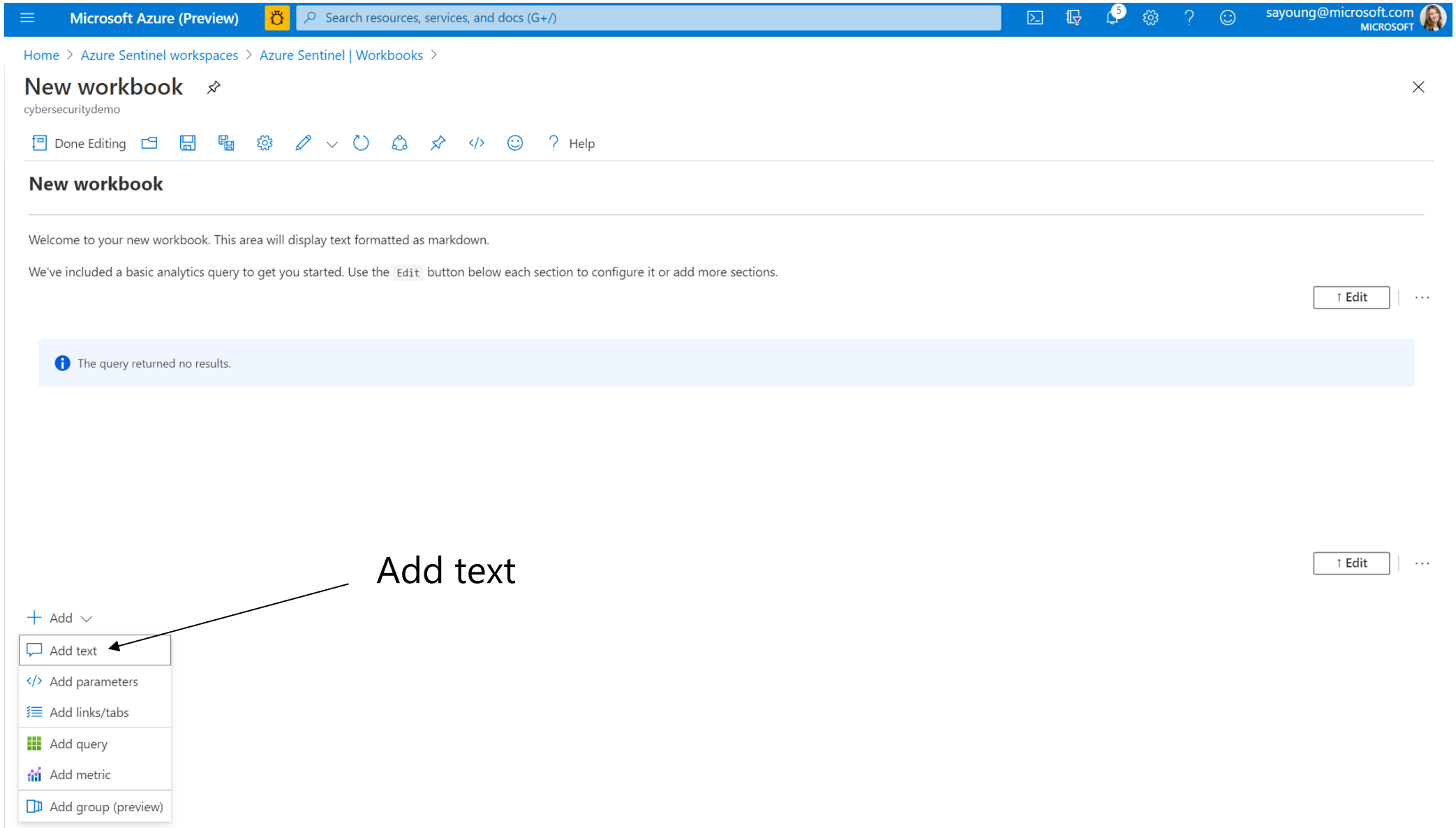
Heading 1

Heading 2

Heading 3

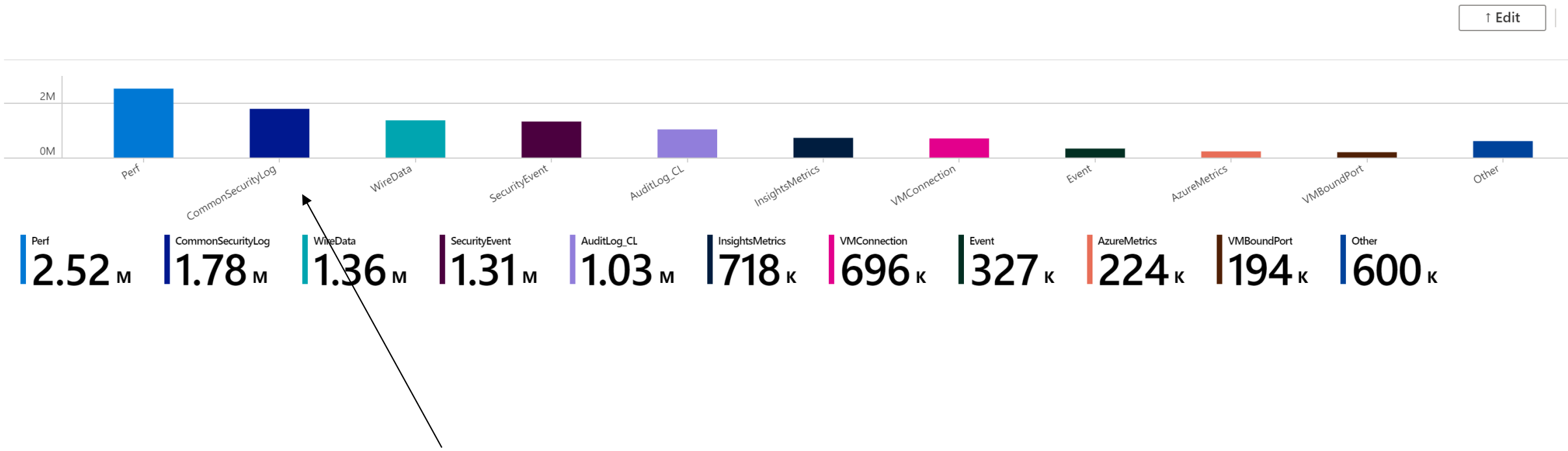
Plain text

Custom Workbooks - Text



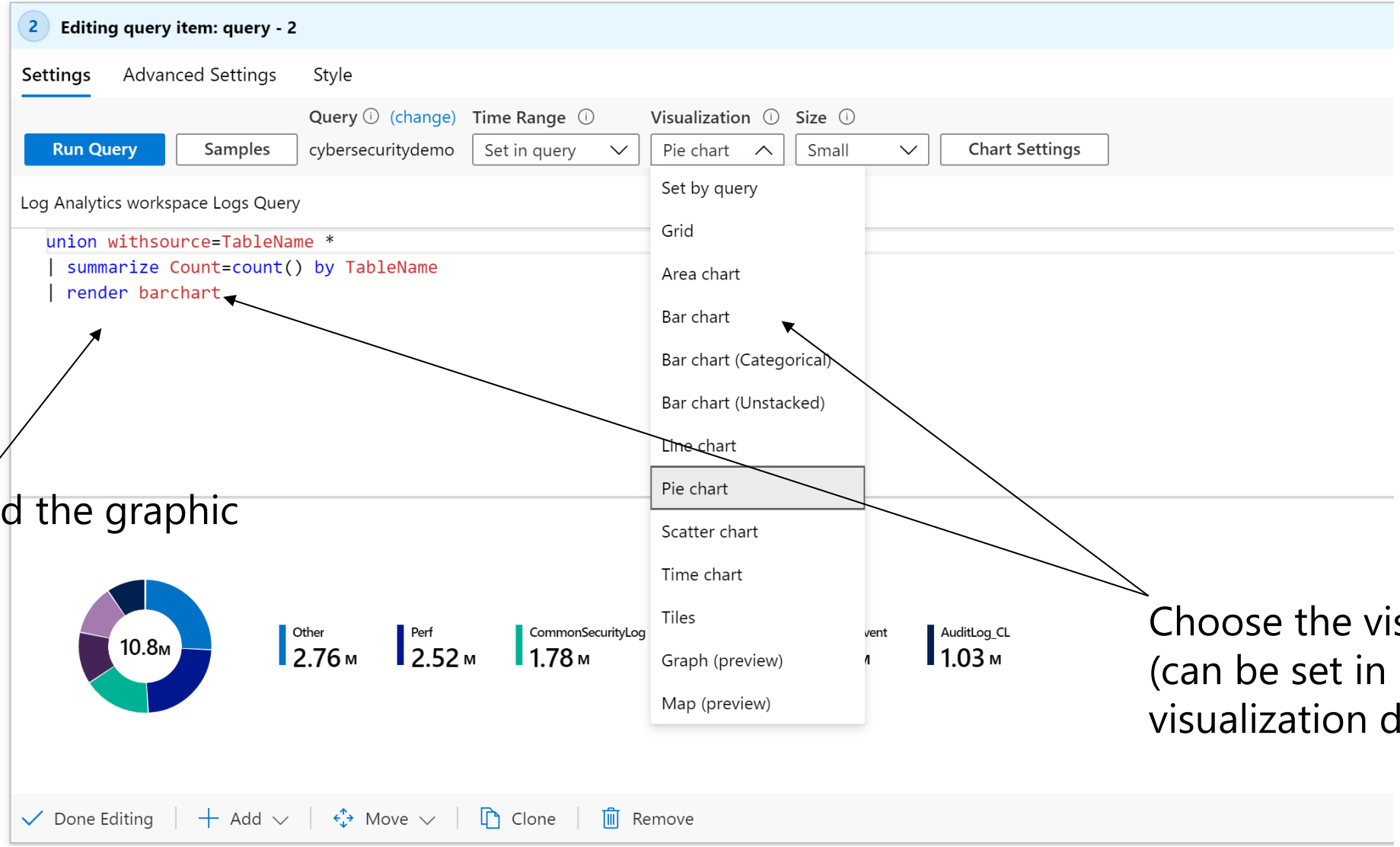
Custom Workbooks - Charts

We've included a basic analytics query to get you started. Use the `Edit` button below each section to configure it or add more sections.



A basic event ingestion query gets you started

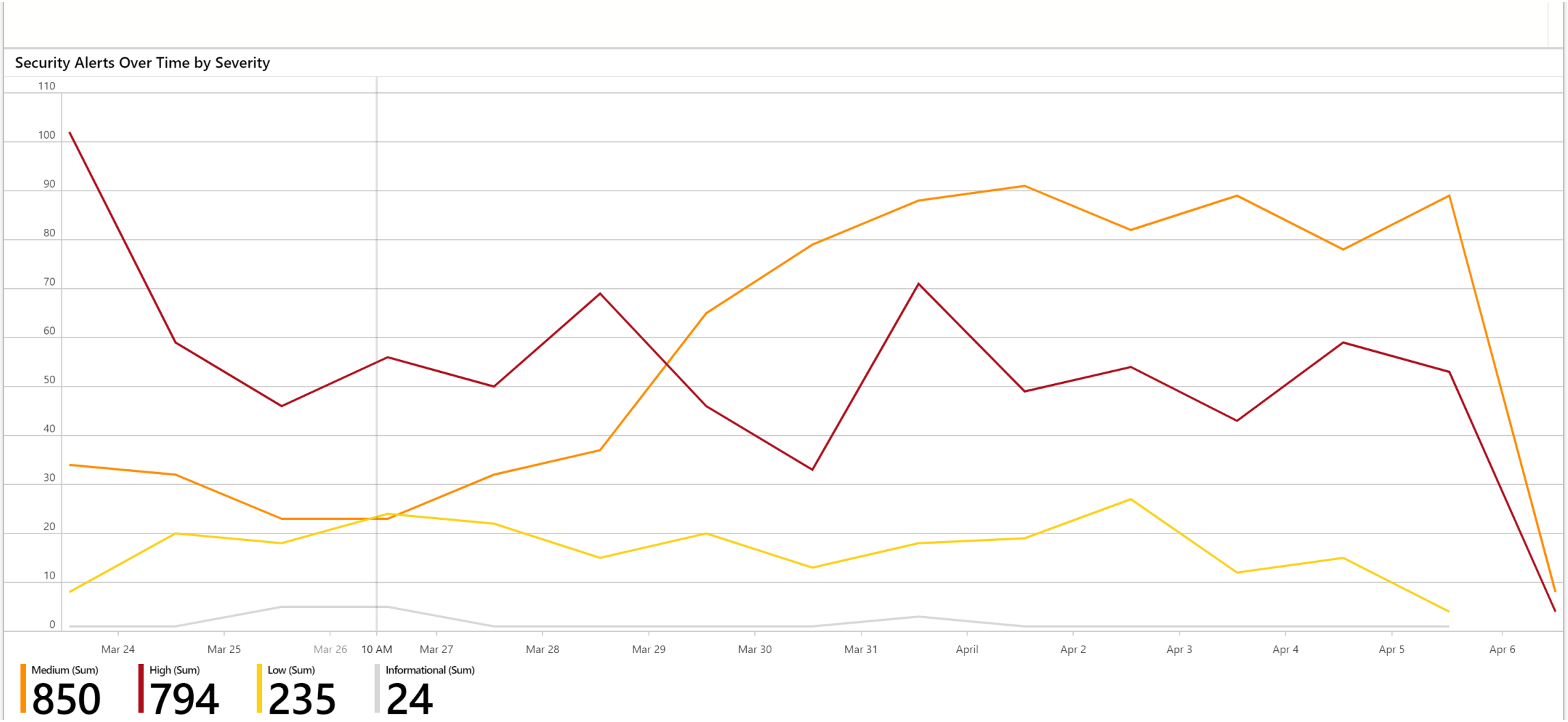
Custom Workbooks - Charts



Query behind the graphic

Choose the visualization (can be set in query or visualization drop-down)

Custom Workbooks – Time charts

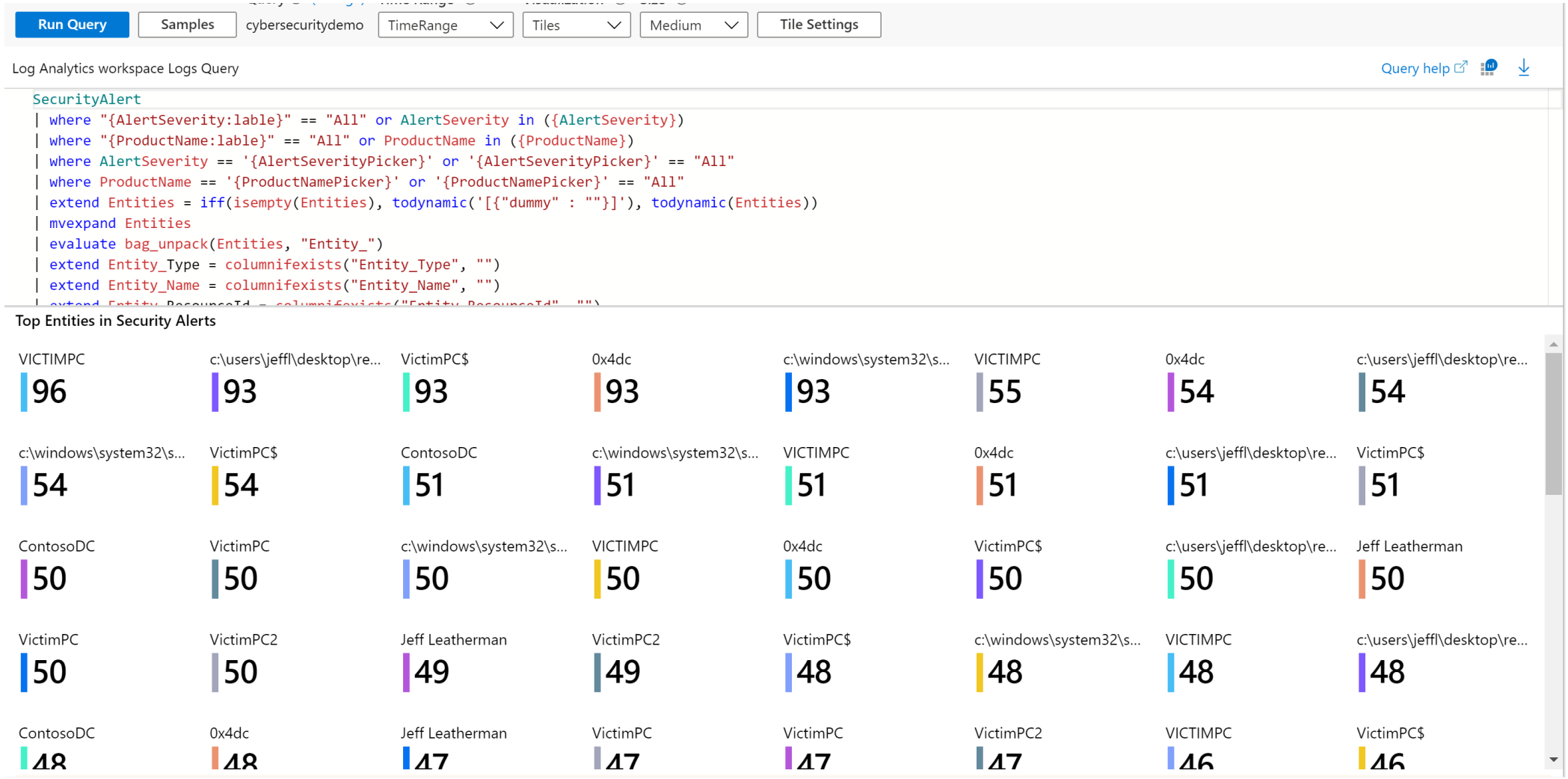


Custom Workbooks - Grids

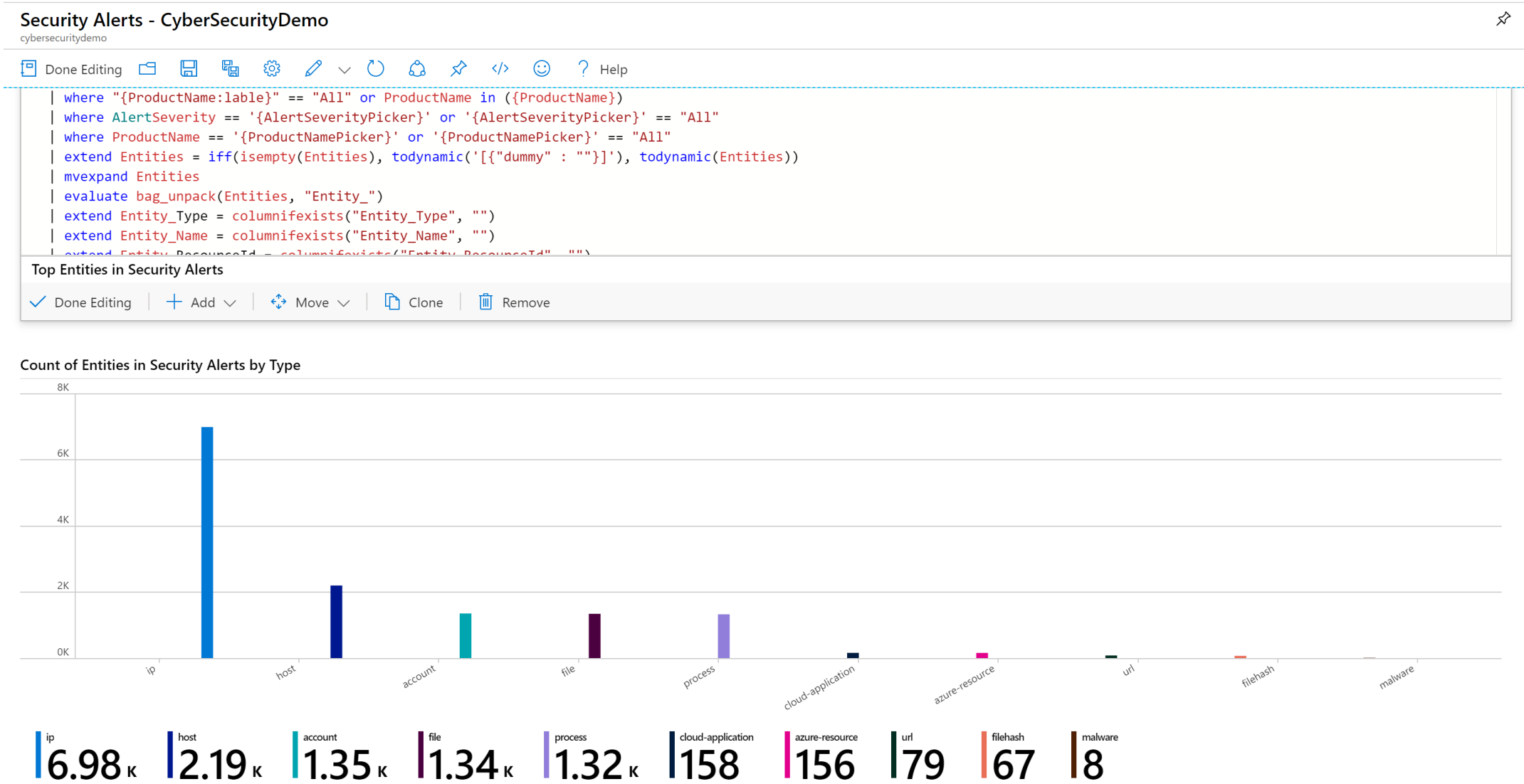
Top Entities in Security Alerts

Target	Entity_Type	count_
ContosoDC	host	123
Jeff Leatherman	account	121
VictimPC	host	121
VictimPC2	host	121
VICTIMPC	host	108
VictimPC$	account	106
0x4dc	process	106
c:\windows\system32\svchost.exe	file	106
c:\users\jeffl\desktop\readysess\2a. c2\svchost.exe	file	106
VictimPC$	account	62
0x4dc	process	62

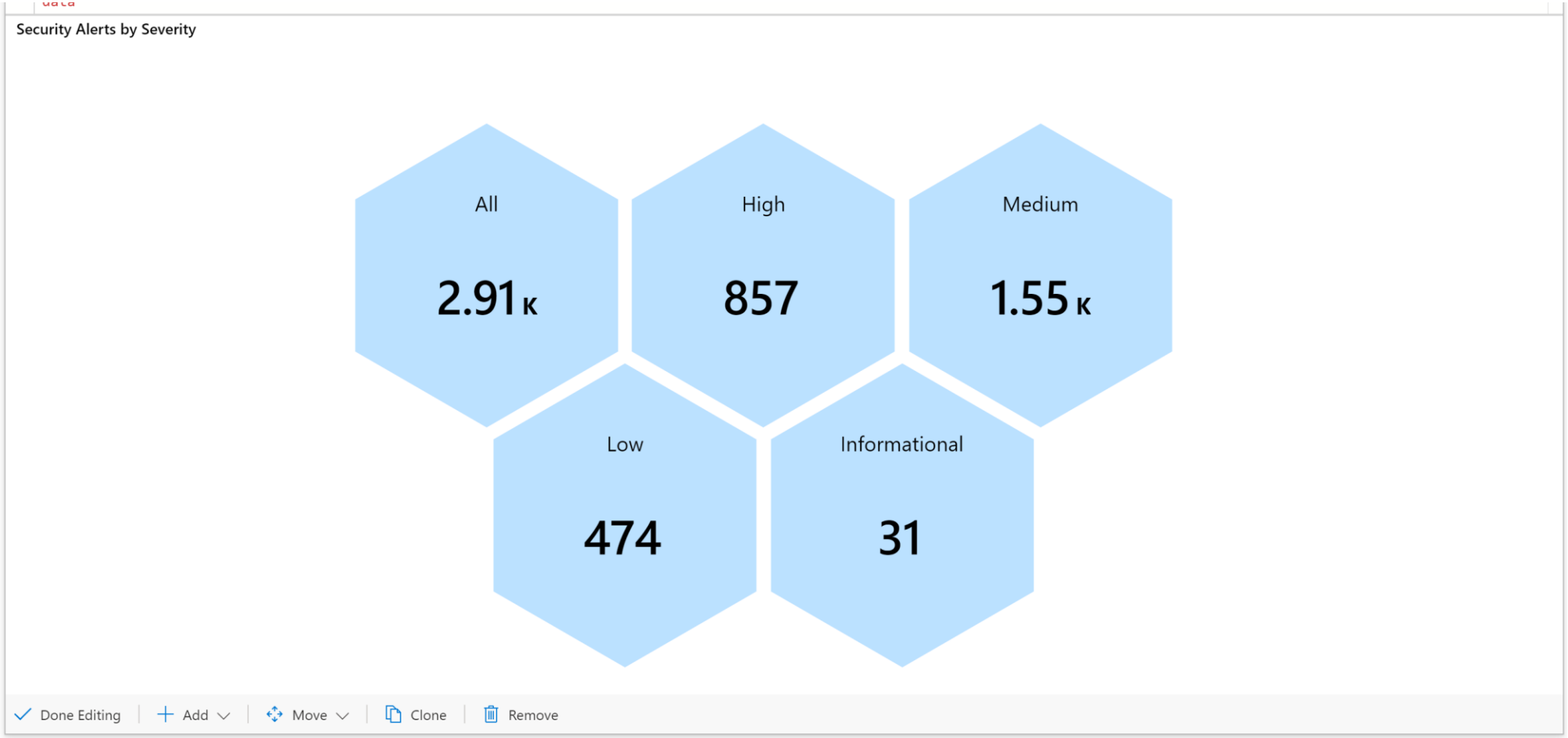
Custom Workbooks - Tiles



Custom Workbooks - Graphs

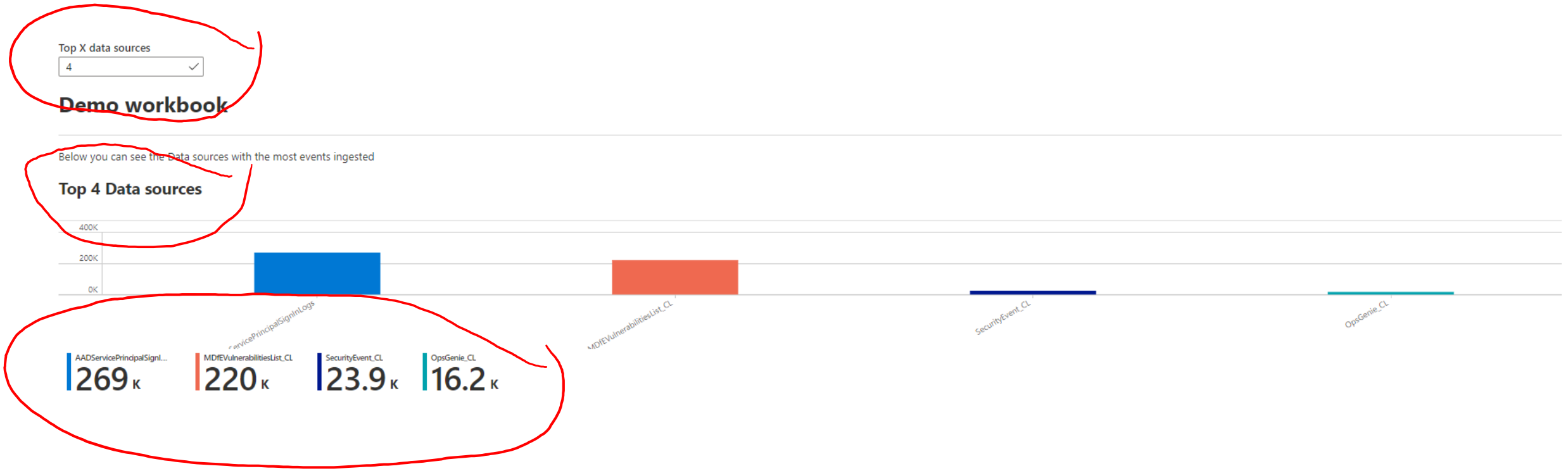


Custom Workbooks - Graph/Hives



Custom Workbooks - Parameters

Parameters allow workbook authors to collect input from the consumers and reference it in other parts of the workbook – usually to scope the result set or setting the right visual. It is a key capability that allows authors to build interactive reports and experiences. Parameters can be reused in visualization queries and text, making them interactive.



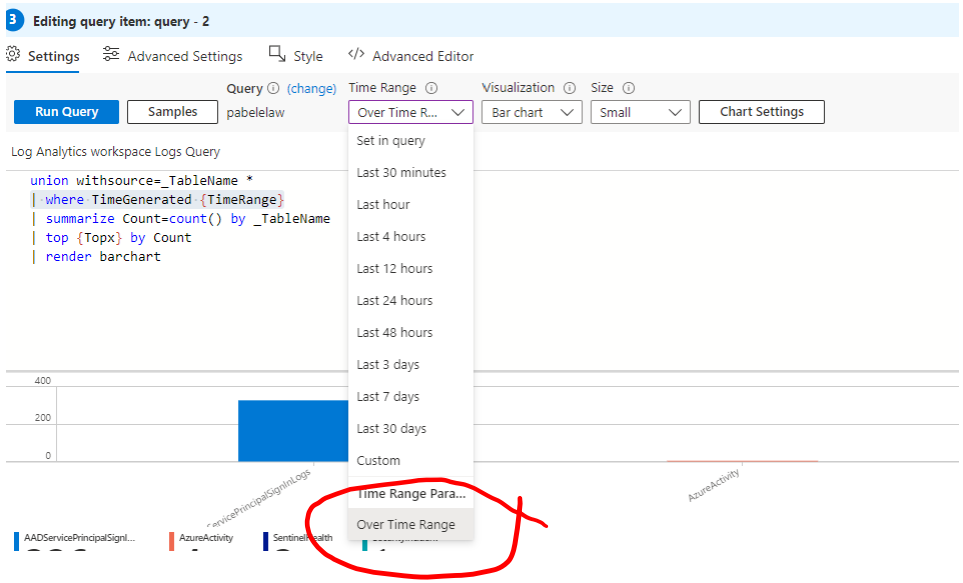
Custom Workbooks – Parameter types

Supported parameter types include:
- Time - allows a user to select from prepopulated time ranges or select a custom range
- Drop down - allows a user to select from a value or set of values
- Text - allows a user to enter arbitrary text
- Resource - allows a user to select one or more Azure resources
- Subscription - allows a user to select one or more Azure subscription resources
- Resource Type - allows a user to select one or more Azure resource type values
- Location - allows a user to select one or more Azure location values

Custom Workbooks – Time Parameter

Time parameters allow users to set the time context of analysis and is used by almost all reports. It is relatively simple to setup and use - allowing authors to specify the time ranges to show in the drop-down, including the option for custom time ranges.
Referencing Timerange is possible in:

- Via Time Range Scope picker of the Query control
- KQL Query (`| where TimeGenerated {TimeRange}`)
- Text (`Events in {TimeRange:label}`)



Custom Workbooks – Text Parameter

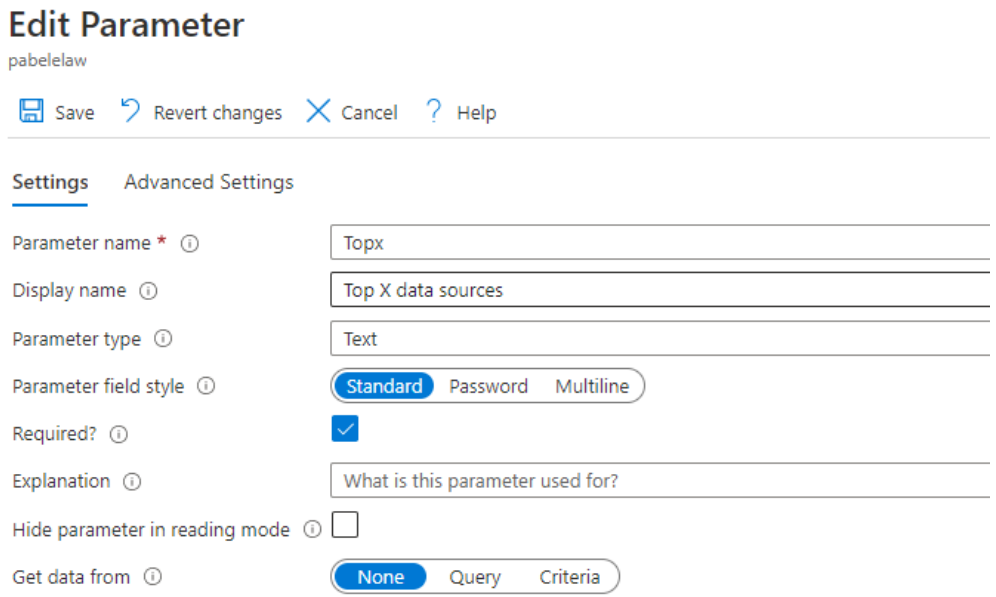
- Text parameters provide a simple way to collect text input from workbook users.
- They're used when it isn't practical to use a drop-down to collect the input (for example, an arbitrary threshold or generic filters). Workbooks allow authors to get the default value of the textbox from a query.
- This allows interesting scenarios like setting the default threshold based on the p95 of the metric.
- Regex based input validation is also possible, like accepting numbers only

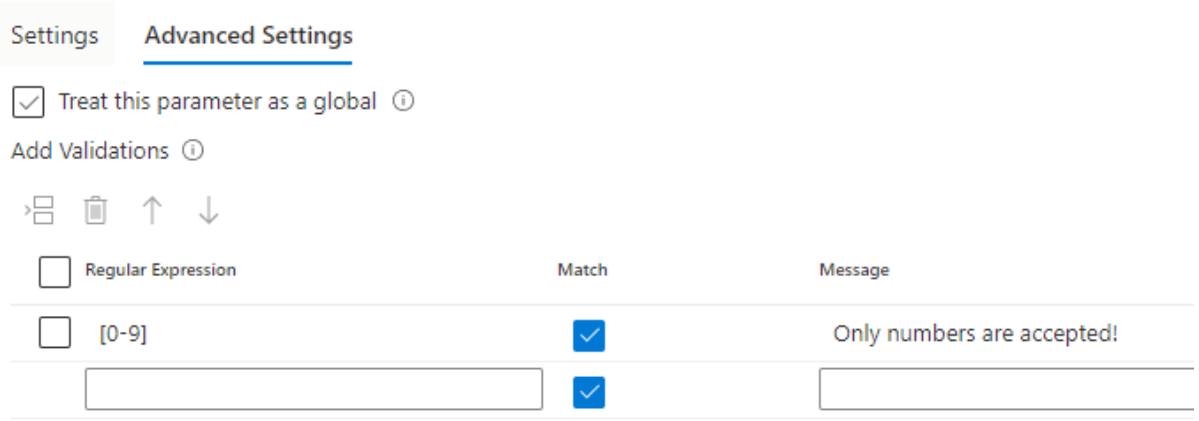
Can be used in Text:

```
## Top {Topx:label} Data sources
```

Or Query:

```
union withsource=_TableName *
| where TimeGenerated {TimeRange}
| summarize Count=count() by _TableName
| top {Topx} by Count
| render barchart
```





Custom Workbooks – Drop Down Parameter

Drop downs allow user to collect one or more input values from a known set

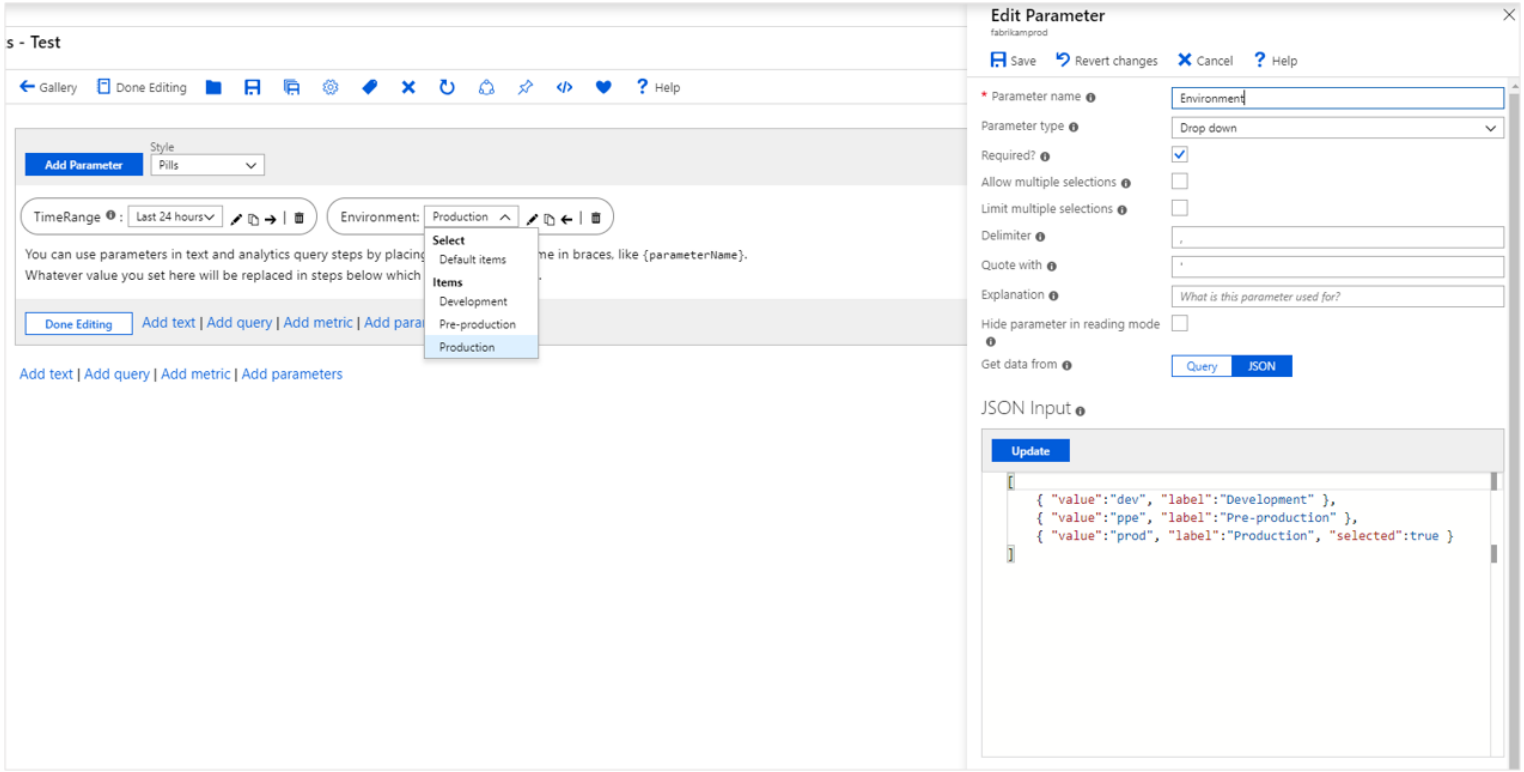
Povide a user-friendly way to collect arbitrary inputs from users.

Especially useful in enabling filtering in your interactive reports.

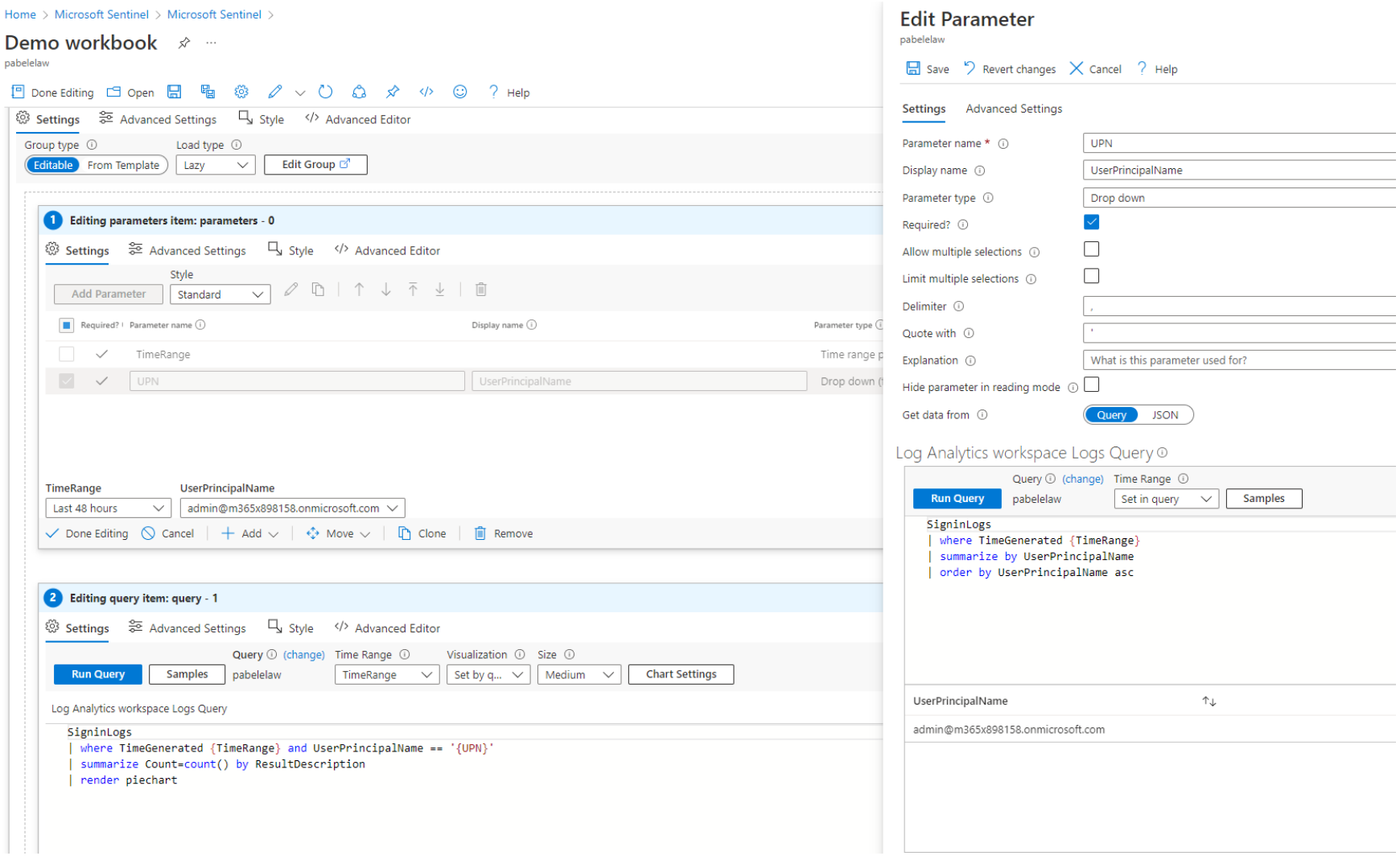
Drop-down can be specified by:

- providing a static JSON list in the parameter setting.
- dynamically via a KQL query.

Parameter settings also allow you to specify whether it is single or multi-select, and if it is multi-select, how the result set should be formatted (delimiter, quotation, etc.).



Custom Workbooks – Drop Down Query Parameter

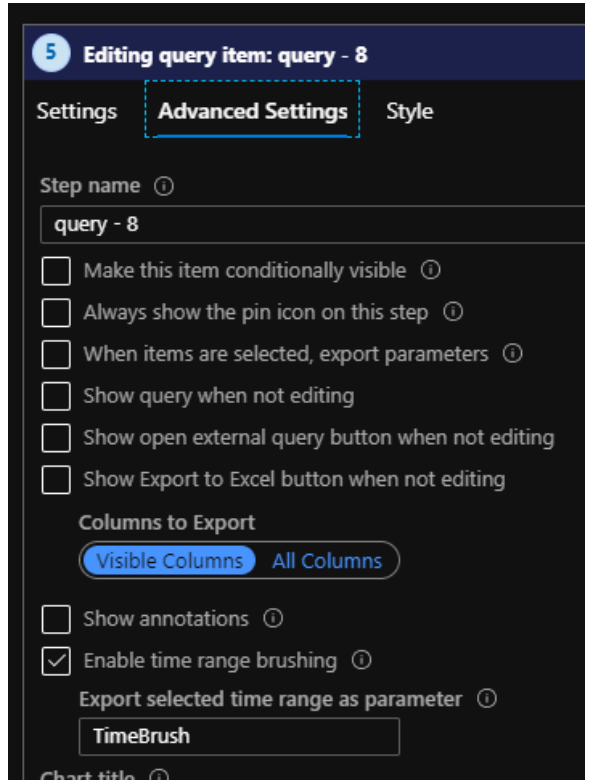


Advanced - Time Brushing for Sentinel workbooks

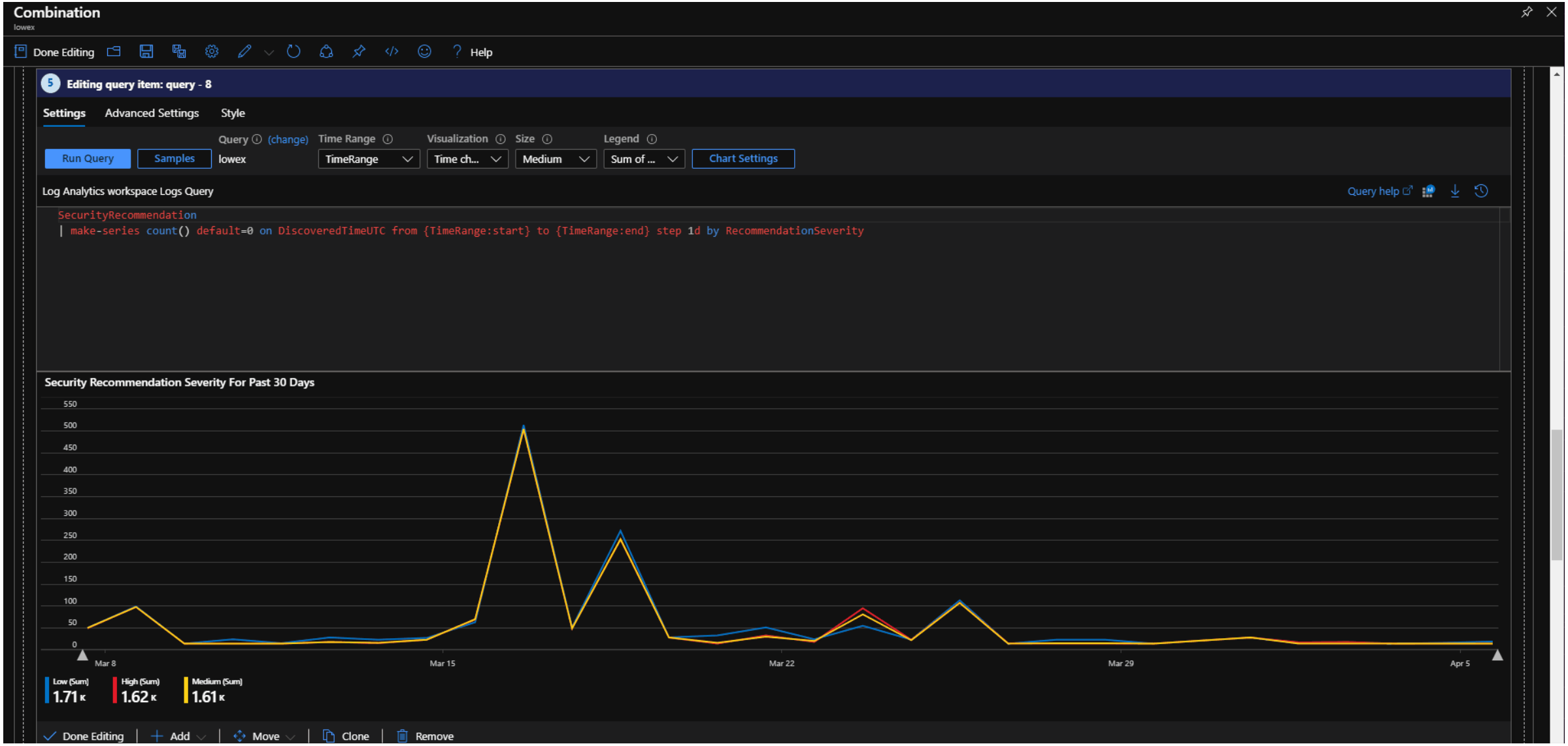
- Time brushing is the method of using a time chart to display the data and allowing the selection of time ranges within the displayed data.

- This is done by turning on the feature for time brushing within the time chart and creating a variable for the value of the time range

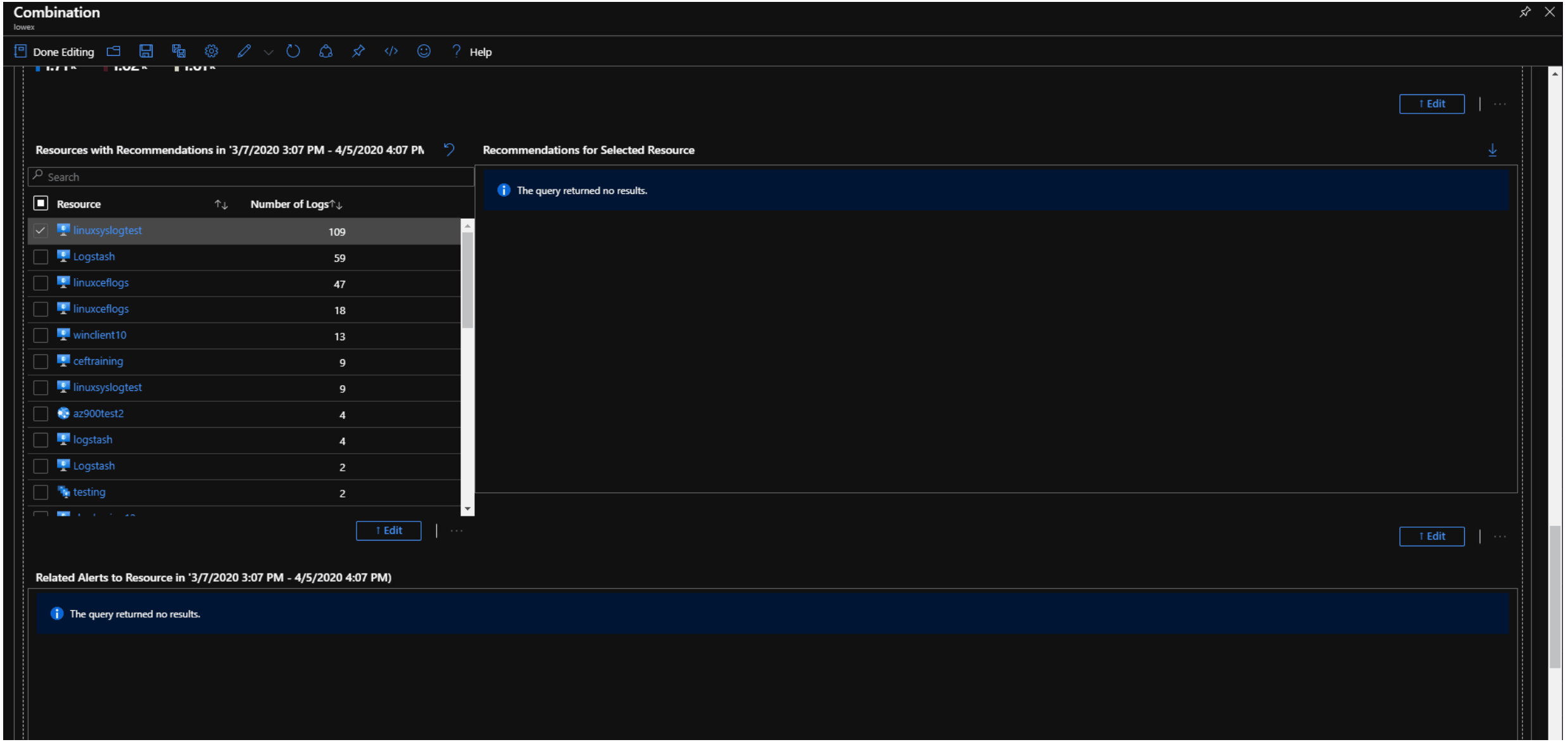
- Once the variable is created, any tile beneath the time chart will inherit the variable as a time option. Once selected, the data shown for them will be between the start and end dates of the range chosen by the user



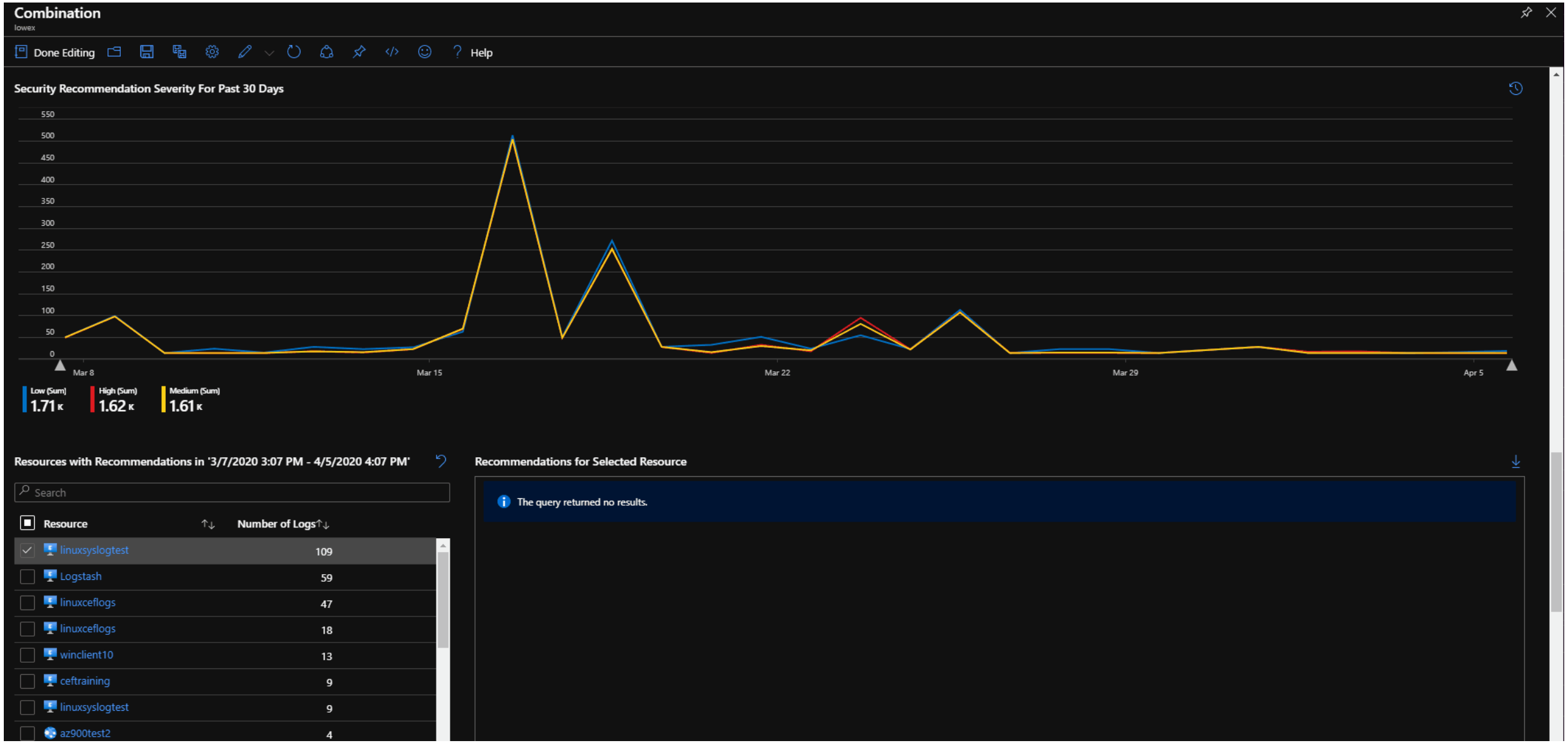
Parameter Setup



Setting the Time Range

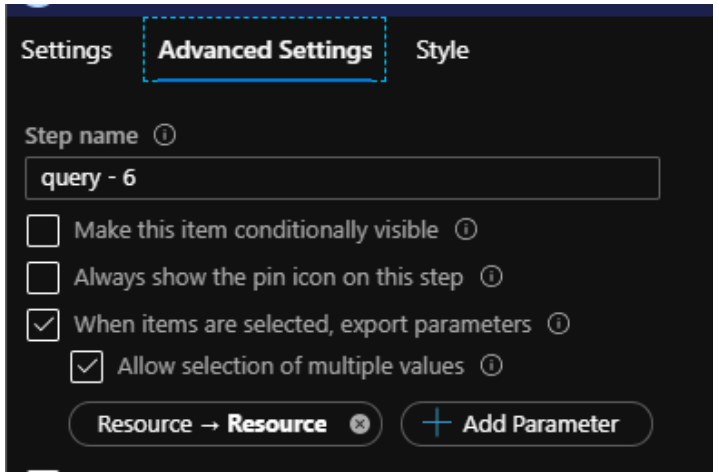


Time Brushing in Action



Dynamic content in Sentinel workbooks

- Dynamic content is the ability for tiles to inherit information from another tile when a row is selected.
- This is done by enabling the option to export a parameter when a row is chosen within the settings of a tile.
- Within the tile that is performing the export, the parameter to be exported will need to be set.
- Within the tiles that you want the data to be exported to, a call to the parameter that you are exporting is needed:

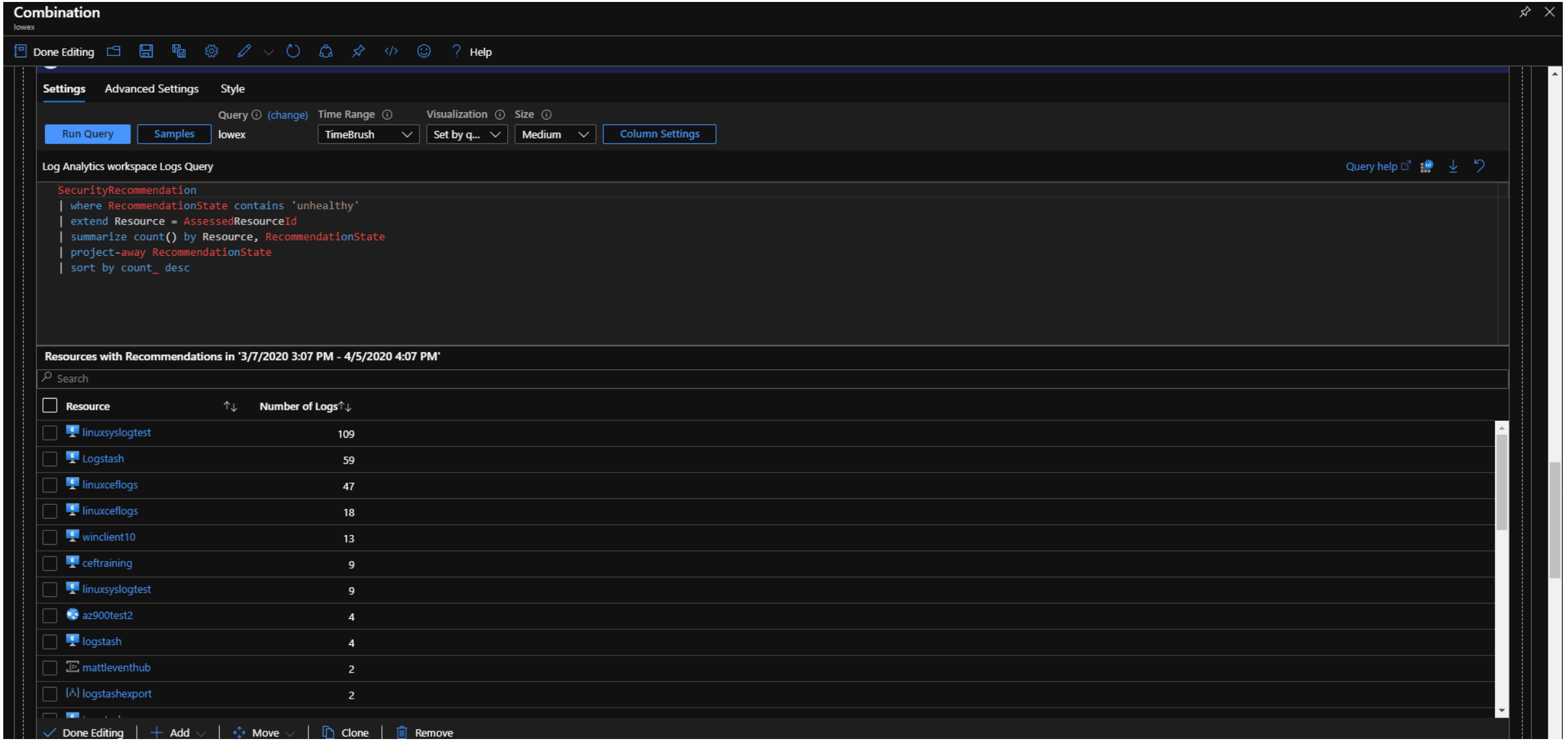



```
ProtectionStatus
| extend Protection = iff(Thr
| extend Resource = Computer
| project TimeGenerated, Reso
| summarize arg_max(TimeGener
```

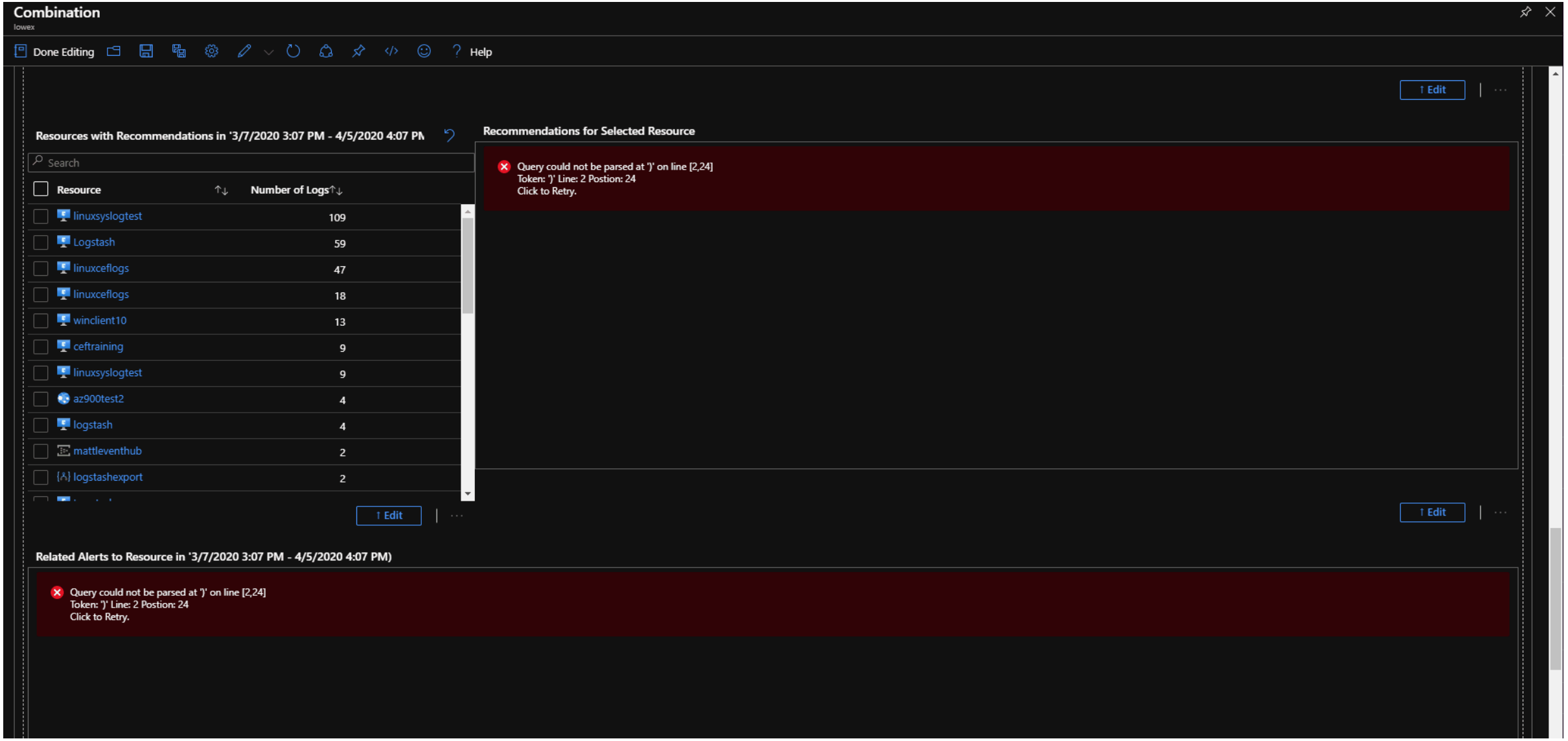
```
let Resource_ = dynamic({Resource});
ProtectionStatus
```

  - Picture 2 shows the setting of the value for Resource, which is supposed to be inherited by the tiles that call it
  - Picture 3 shows a new variable, Resource_, being established to take on the value of Resource whenever something is clicked on

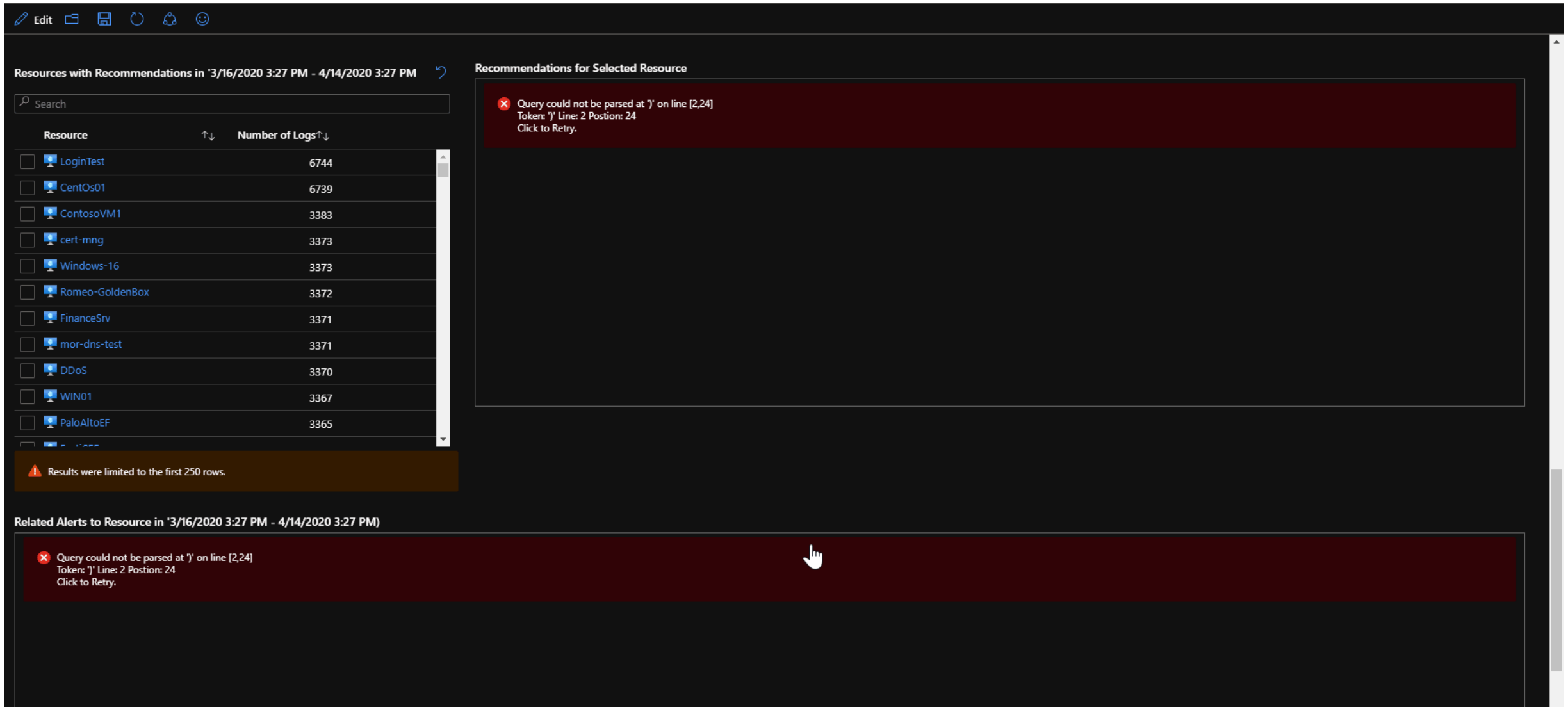
Parameter Setup



Calling the Parameter

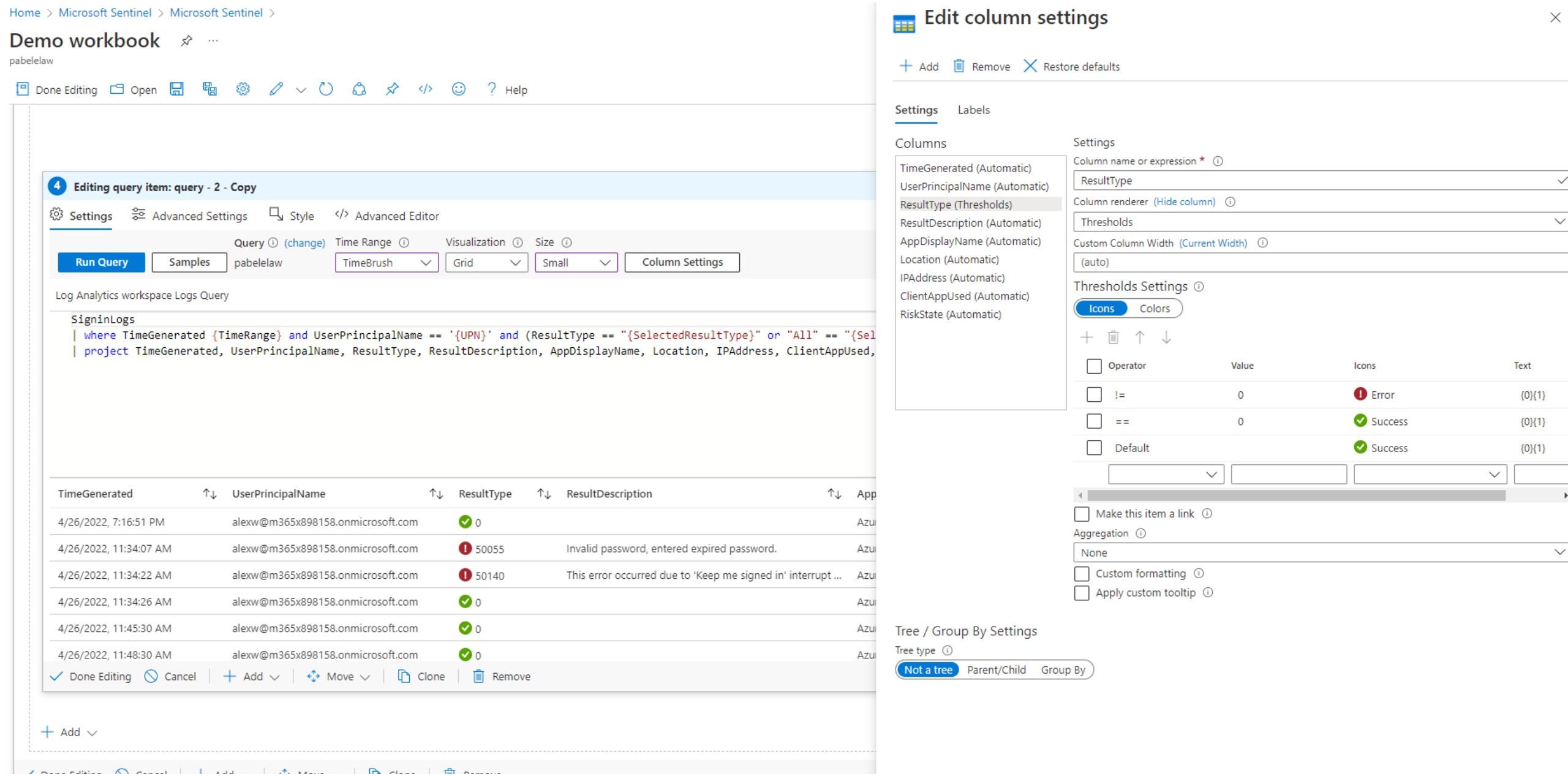


Demo


Edit
Resources with Recommendations in '3/16/2020 3:27 PM - 4/14/2020 3:27 PM
Search
Resource
Number of Logs
LoginTest 6744
CentOs01 6739
ContosoVM1 3383
cert-mng 3373
Windows-16 3373
Romeo-GoldenBox 3372
FinanceSrv 3371
mor-dns-test 3371
DDoS 3370
WIN01 3367
PaloAltoEF 3365
Results were limited to the first 250 rows.
Recommendations for Selected Resource
Query could not be parsed at ')' on line [2,24]
Token: ')' Line: 2 Postion: 24
Click to Retry.
Related Alerts to Resource in '3/16/2020 3:27 PM - 4/14/2020 3:27 PM)
Query could not be parsed at ')' on line [2,24]
Token: ')' Line: 2 Postion: 24
Click to Retry.

Personalization in Sentinel workbooks

- Personalization allows users to change titles, select color schemes, and make other changes in order to make tiles stand out.
- These changes can be made by going to the "column settings" option one a tile has been made.
- Go to use when showing severity, high vs low counts, and making more friendly column headers.
- Allows you to set colors, color schemes, make items into links, change labels, etc.

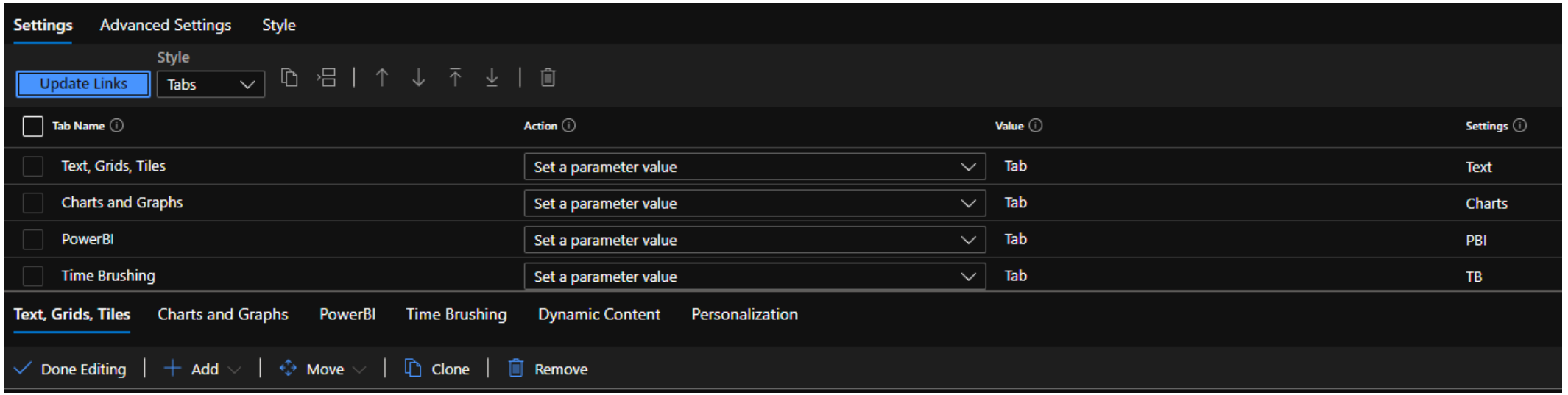

Home > Microsoft Sentinel > Microsoft Sentinel >
Demo workbook
pabelelaw
Done Editing
Open
Help
4 Editing query item: query - 2 - Copy
Settings
Advanced Settings
Style
Advanced Editor
Query (change)
Time Range
Visualization
Size
Run Query
Samples
pabelelaw
TimeBrush
Grid
Small
Column Settings
Log Analytics workspace Logs Query
SigninLogs
| where TimeGenerated {TimeRange} and UserPrincipalName == '{UPN}' and (ResultType == "{SelectedResultType}" or "All" == "{Sel
| project TimeGenerated, UserPrincipalName, ResultType, ResultDescription, AppDisplayName, Location, IPAddress, ClientAppUsed,
TimeGenerated
UserPrincipalName
ResultType
ResultDescription
4/26/2022, 7:16:51 PM
alexw@m365x898158.onmicrosoft.com
0
4/26/2022, 11:34:07 AM
alexw@m365x898158.onmicrosoft.com
50055
Invalid password, entered expired password.
4/26/2022, 11:34:22 AM
alexw@m365x898158.onmicrosoft.com
50140
This error occurred due to 'Keep me signed in' interrupt ...
4/26/2022, 11:34:26 AM
alexw@m365x898158.onmicrosoft.com
0
4/26/2022, 11:45:30 AM
alexw@m365x898158.onmicrosoft.com
0
4/26/2022, 11:48:30 AM
alexw@m365x898158.onmicrosoft.com
0
Done Editing
Cancel
Add
Move
Clone
Remove
Add
Edit column settings
Add
Remove
Restore defaults
Settings
Labels
Columns
TimeGenerated (Automatic)
UserPrincipalName (Automatic)
ResultType (Thresholds)
ResultDescription (Automatic)
AppDisplayName (Automatic)
Location (Automatic)
IPAddress (Automatic)
ClientAppUsed (Automatic)
RiskState (Automatic)
Settings
Column name or expression *
ResultType
Column renderer (Hide column)
Thresholds
Custom Column Width (Current Width)
(auto)
Thresholds Settings
Icons
Colors
Operator
Value
Icons
Text
!=
0
Error
{0}{1}
==
0
Success
{0}{1}
Default
Success
{0}{1}
Make this item a link
Aggregation
None
Custom formatting
Apply custom tooltip
Tree / Group By Settings
Tree type
Not a tree
Parent/Child
Group By

Result

TimeGenerated	UserPrincipalName	ResultType	ResultDescription	AppDisplayName	Location	IPAddress	ClientAppUsed	RiskState
4/26/2022, 7:16:51 PM	alexw@m365x898158.onmicrosoft.com	0		Azure Portal	HU	176.63.6.177	Browser	none
4/26/2022, 11:34:07 AM	alexw@m365x898158.onmicrosoft.com	50055	Invalid password, entered expired password.	Azure Portal	HU	176.63.6.177	Browser	none
4/26/2022, 11:34:22 AM	alexw@m365x898158.onmicrosoft.com	50140	This error occurred due to 'Keep me signed in' interrupt ...	Azure Portal	HU	176.63.6.177	Browser	none
4/26/2022, 11:34:26 AM	alexw@m365x898158.onmicrosoft.com	0		Azure Portal	HU	176.63.6.177	Browser	none
4/26/2022, 11:45:30 AM	alexw@m365x898158.onmicrosoft.com	0		Azure Portal	HU	176.63.6.177	Browser	none
4/26/2022, 11:48:30 AM	alexw@m365x898158.onmicrosoft.com	0		Azure Portal	HU	176.63.6.177	Browser	none

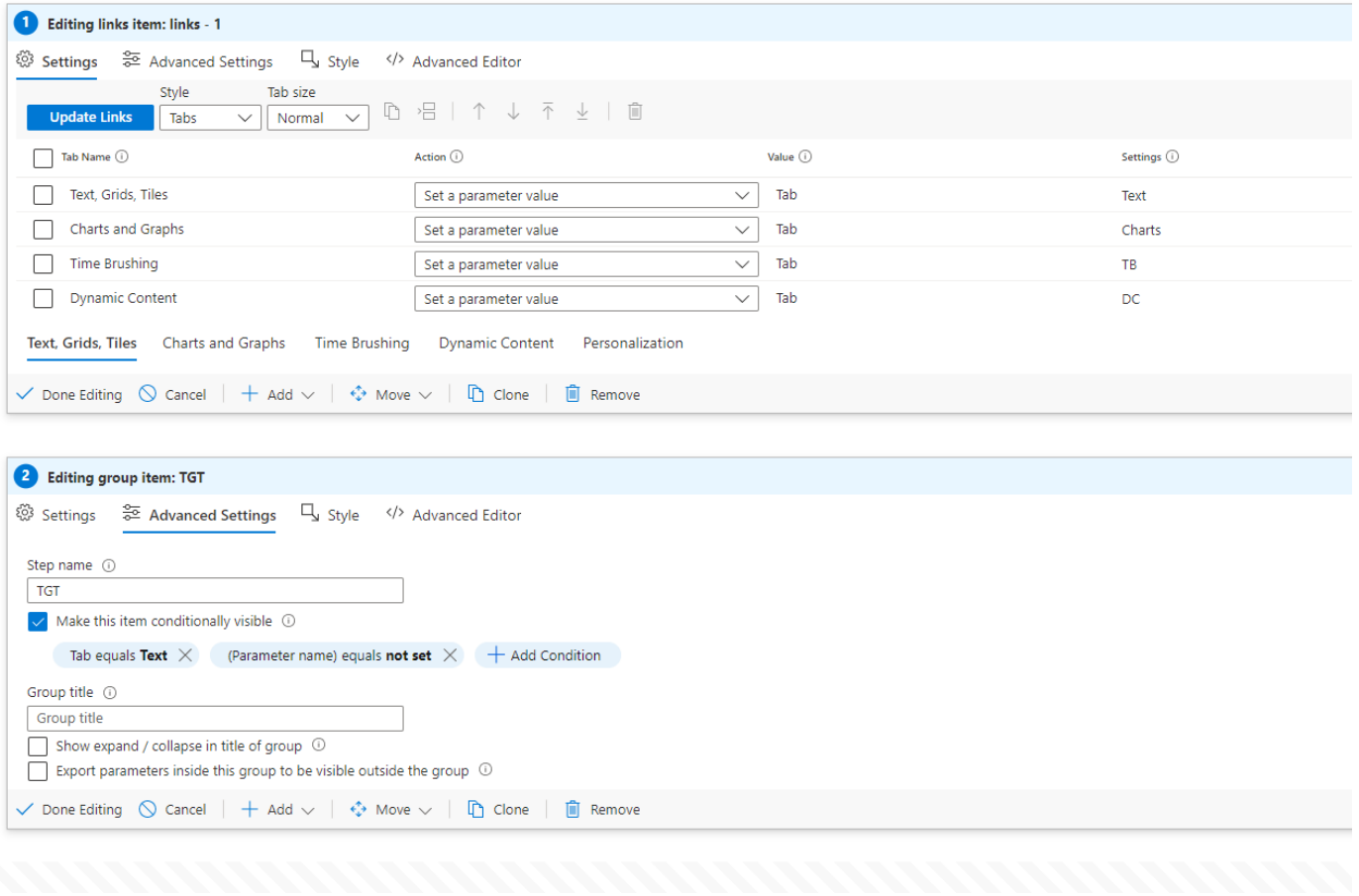
Tabs

- Tabs allow you to organize and classify parts of a workbook into a more orderly fashion.
- When used in combination with groups, this can be a powerful combination.
- Set by adding tabs and setting values to identify when a tab is chosen.

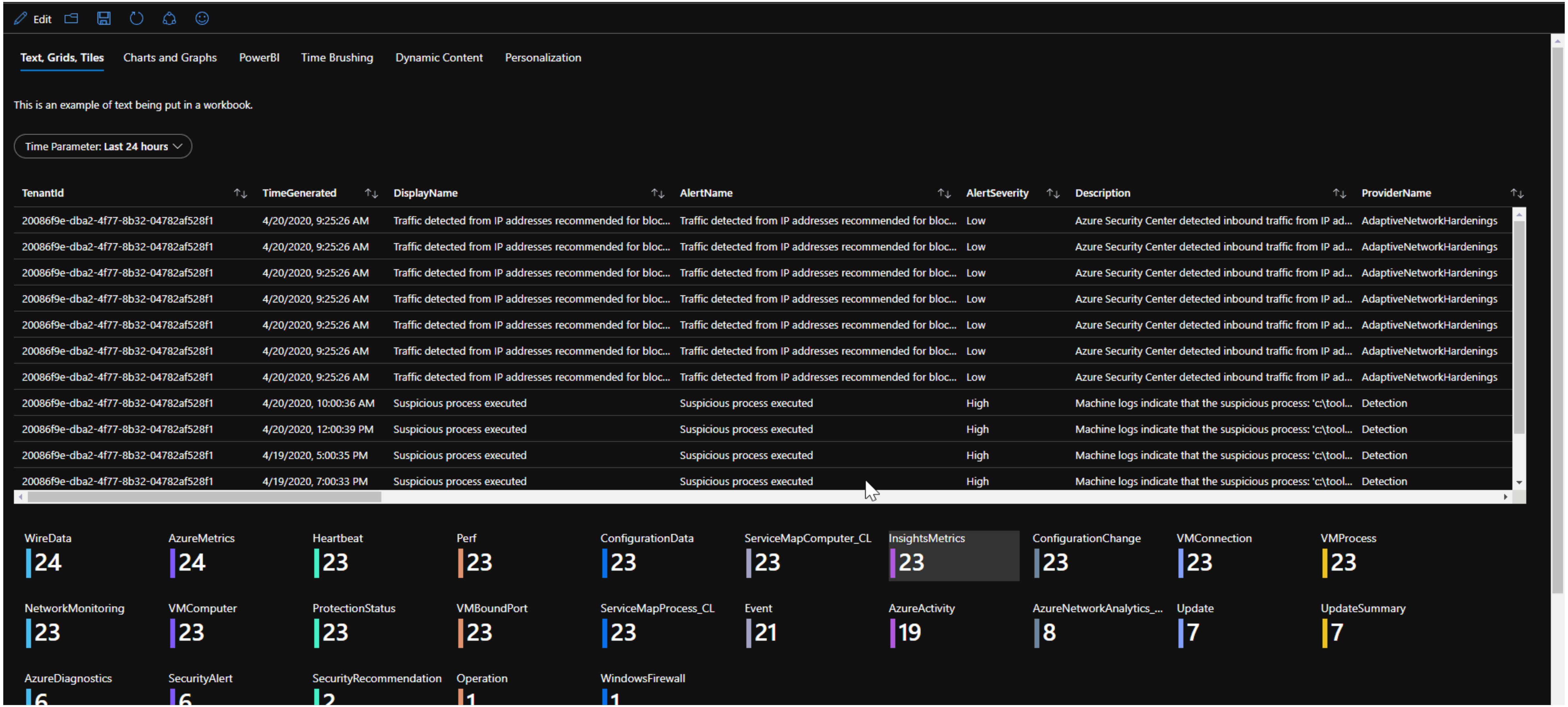


Custom Workbooks - Controlling tabs

- Add link items which set parameter values
- Add Group items with conditional visibility

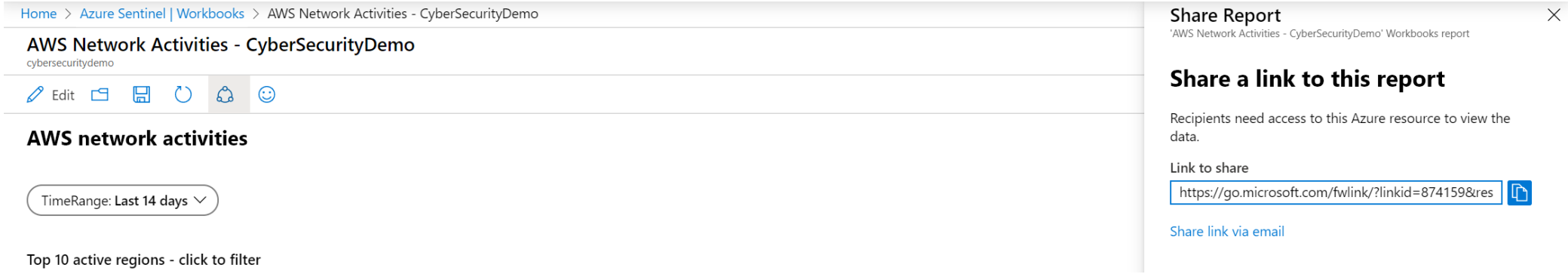


Demo



TenantId	TimeGenerated	DisplayName	AlertName	AlertSeverity	Description	ProviderName
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 9:25:26 AM	Traffic detected from IP addresses recommended for bloc...	Traffic detected from IP addresses recommended for bloc...	Low	Azure Security Center detected inbound traffic from IP ad...	AdaptiveNetworkHardenings
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 9:25:26 AM	Traffic detected from IP addresses recommended for bloc...	Traffic detected from IP addresses recommended for bloc...	Low	Azure Security Center detected inbound traffic from IP ad...	AdaptiveNetworkHardenings
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 9:25:26 AM	Traffic detected from IP addresses recommended for bloc...	Traffic detected from IP addresses recommended for bloc...	Low	Azure Security Center detected inbound traffic from IP ad...	AdaptiveNetworkHardenings
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 9:25:26 AM	Traffic detected from IP addresses recommended for bloc...	Traffic detected from IP addresses recommended for bloc...	Low	Azure Security Center detected inbound traffic from IP ad...	AdaptiveNetworkHardenings
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 9:25:26 AM	Traffic detected from IP addresses recommended for bloc...	Traffic detected from IP addresses recommended for bloc...	Low	Azure Security Center detected inbound traffic from IP ad...	AdaptiveNetworkHardenings
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 9:25:26 AM	Traffic detected from IP addresses recommended for bloc...	Traffic detected from IP addresses recommended for bloc...	Low	Azure Security Center detected inbound traffic from IP ad...	AdaptiveNetworkHardenings
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 9:25:26 AM	Traffic detected from IP addresses recommended for bloc...	Traffic detected from IP addresses recommended for bloc...	Low	Azure Security Center detected inbound traffic from IP ad...	AdaptiveNetworkHardenings
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 10:00:36 AM	Suspicious process executed	Suspicious process executed	High	Machine logs indicate that the suspicious process: 'c:\tool...	Detection
20086f9e-dba2-4f77-8b32-04782af528f1	4/20/2020, 12:00:39 PM	Suspicious process executed	Suspicious process executed	High	Machine logs indicate that the suspicious process: 'c:\tool...	Detection
20086f9e-dba2-4f77-8b32-04782af528f1	4/19/2020, 5:00:35 PM	Suspicious process executed	Suspicious process executed	High	Machine logs indicate that the suspicious process: 'c:\tool...	Detection
20086f9e-dba2-4f77-8b32-04782af528f1	4/19/2020, 7:00:33 PM	Suspicious process executed	Suspicious process executed	High	Machine logs indicate that the suspicious process: 'c:\tool...	Detection

Sharing workbooks



- To share access to workbooks, recipients need to have access to the Azure resource.
- (Workbook Reader or Sentinel Reader)

Where to from here?

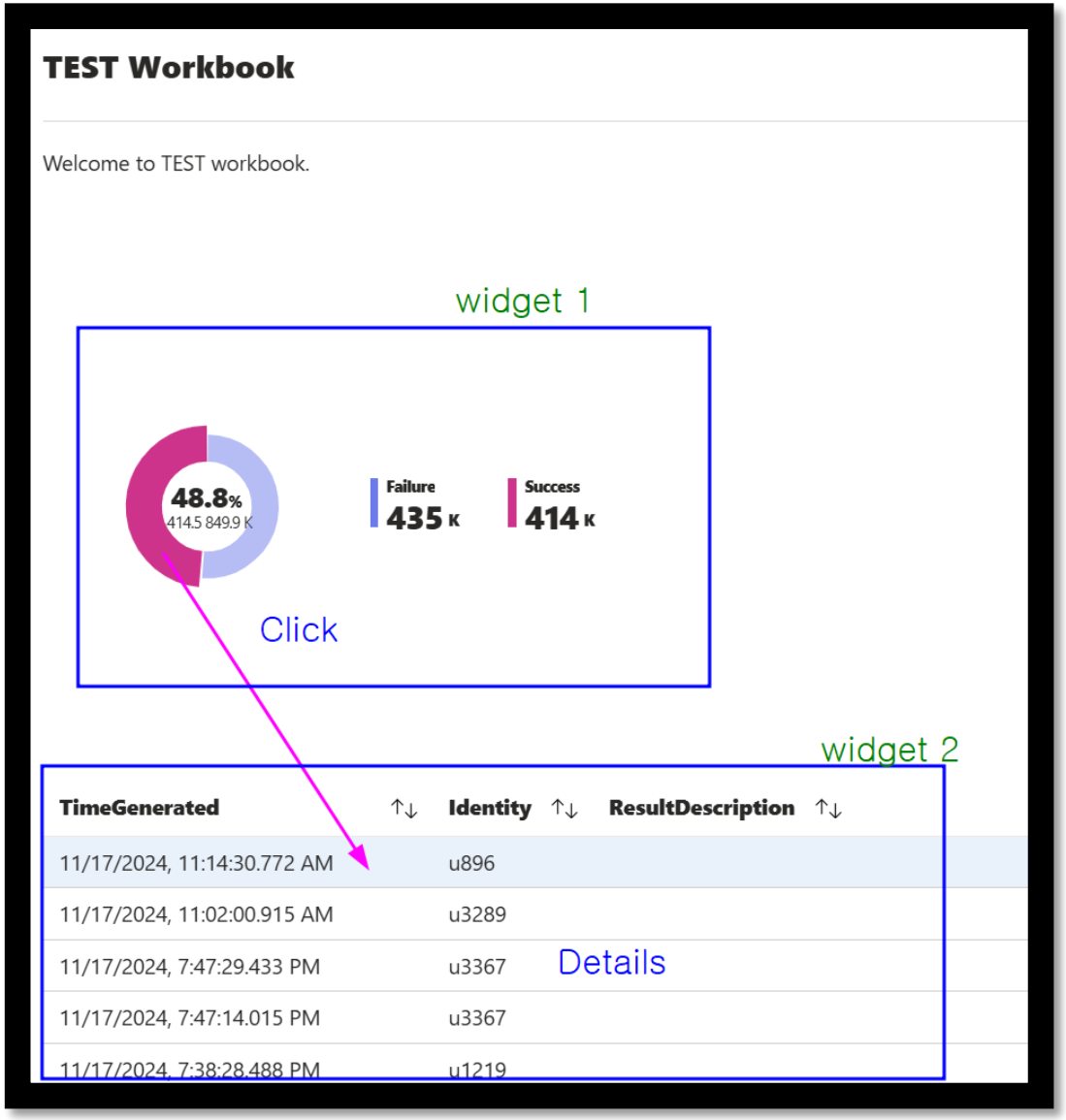
- Monitor workbooks documentation - https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview
- How to use Azure Monitor Workbooks to map Sentinel data - https://techcommunity.microsoft.com/t5/azure-sentinel/how-to-use-azure-monitor-workbooks-to-map-sentinel-data/ba-p/971818
- Visualization demo workbook used in this presentation - https://github.com/Azure/Azure-Sentinel/blob/master/Workbooks/VisualizationDemo.json

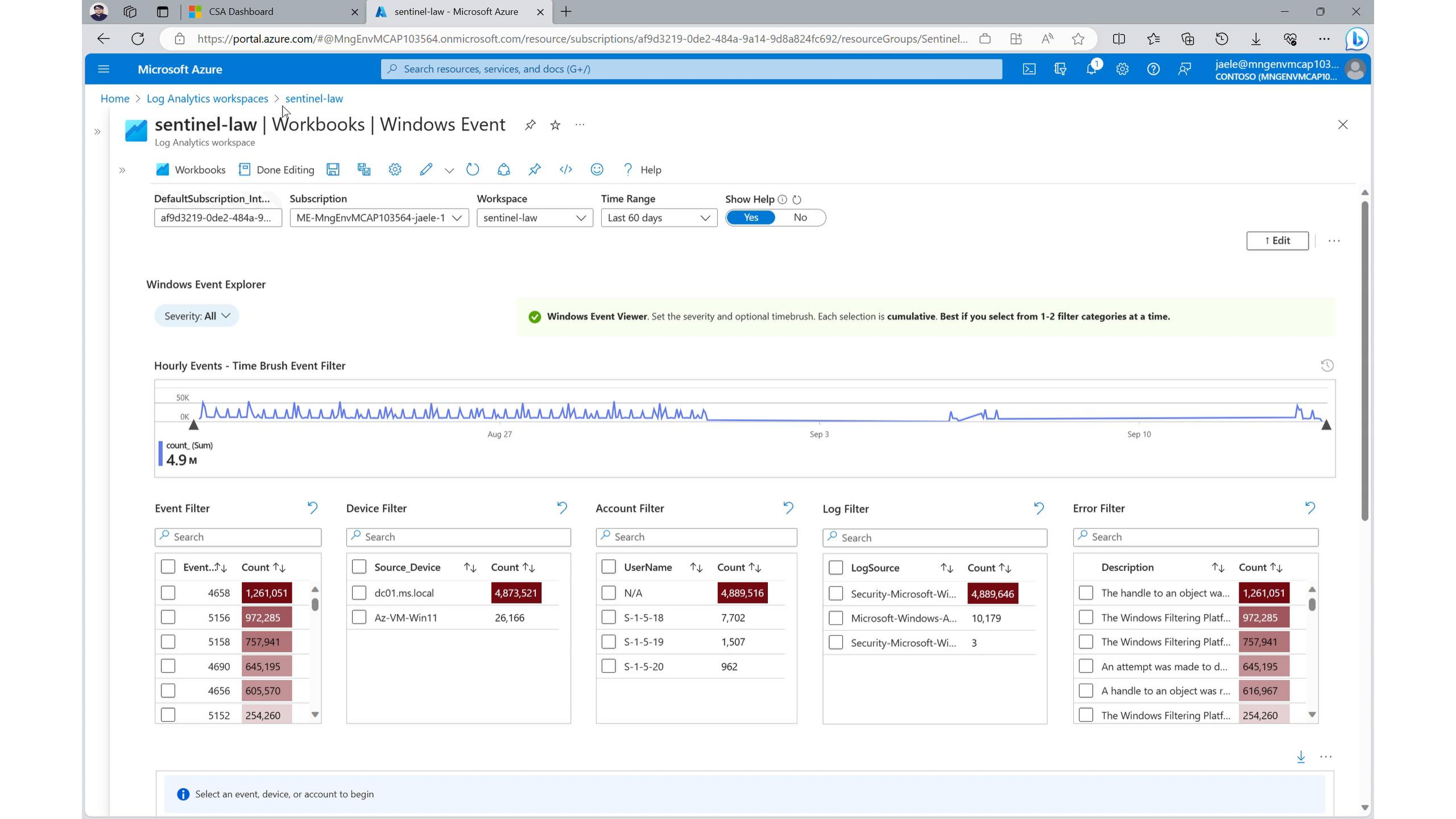
- and

- https://techcommunity.microsoft.com/blog/microsoftsentinelblog/microsoft-sentinel-workbooks-101-with-sample-workbook/1409216

Microsoft

Hands on Lab !




CSA Dashboard
sentinel-law - Microsoft Azure
https://portal.azure.com/#@MngEnvMCAP103564.onmicrosoft.com/resource/subscriptions/af9d3219-0de2-484a-9a14-9d8a824fc692/resourceGroups/Sentinel...
Microsoft Azure
Search resources, services, and docs (G+/)
jaele@mngenvmcap103...
CONTOSO (MNGENVMCAP10...
Home > Log Analytics workspaces > sentinel-law
sentinel-law | Workbooks | Windows Event
Log Analytics workspace
Workbooks
Done Editing
Help
DefaultSubscription_Int...
af9d3219-0de2-484a-9...
Subscription
ME-MngEnvMCAP103564-jaele-1
Workspace
sentinel-law
Time Range
Last 60 days
Show Help
Yes
No
Edit
Windows Event Explorer
Severity: All
Windows Event Viewer. Set the severity and optional timebrush. Each selection is cumulative. Best if you select from 1-2 filter categories at a time.
Hourly Events - Time Brush Event Filter
50K
0K
Aug 27
Sep 3
Sep 10
count_ (Sum)
4.9 M
Event Filter
Search
Event..
Count
4658 1,261,051
5156 972,285
5158 757,941
4690 645,195
4656 605,570
5152 254,260
Device Filter
Search
Source_Device
Count
dc01.ms.local 4,873,521
Az-VM-Win11 26,166
Account Filter
Search
UserName
Count
N/A 4,889,516
S-1-5-18 7,702
S-1-5-19 1,507
S-1-5-20 962
Log Filter
Search
LogSource
Count
Security-Microsoft-Wi... 4,889,646
Microsoft-Windows-A... 10,179
Security-Microsoft-Wi... 3
Error Filter
Search
Description
Count
The handle to an object wa... 1,261,051
The Windows Filtering Platf... 972,285
The Windows Filtering Platf... 757,941
An attempt was made to d... 645,195
A handle to an object was r... 616,967
The Windows Filtering Platf... 254,260
Select an event, device, or account to begin