

Workshop
WORKBOOK
101



Owen lee

Sr. Cloud Solution Architect | Customer Success

Agenda

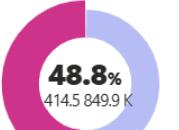
- Out of the box workbooks
- Custom workbooks
- Visualization types
- Parameters
- Advanced - Time brushing
- Advanced - Dynamic content in workbooks
- Advanced – Personalization
- Advanced - Tabs
- Sharing workbooks

Hands-on Lab - Simple Dynamic Dashboard

TEST Workbook

Welcome to TEST workbook.

widget 1



48.8%
Failure
435 k

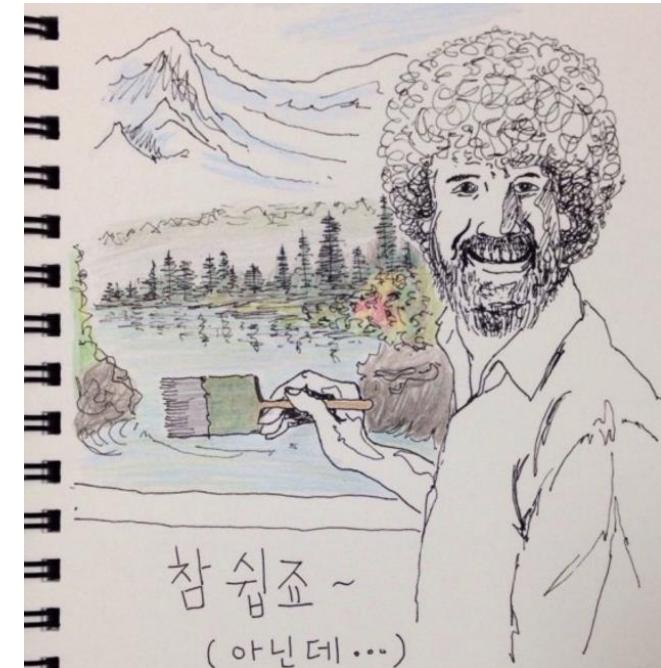
Success
414 k

Click

widget 2

| TimeGenerated | Identity | ResultDescription |
|-----------------------------|----------|-------------------------|
| 11/17/2024, 11:14:30.772 AM | u896 | |
| 11/17/2024, 11:02:00.915 AM | u3289 | |
| 11/17/2024, 7:47:29.433 PM | u3367 | Details |
| 11/17/2024, 7:47:14.015 PM | u3367 | |
| 11/17/2024, 7:38:28.488 PM | u1219 | |

A pink arrow points from the "Click" label in the top chart to the "Details" link in the table below.





workbook visualizations

Out of the Box Workbooks

Add New Workbook

The screenshot shows the Azure Sentinel - Workbooks interface. On the left, a sidebar lists various sections: General, Overview, Logs, News & guides, Threat management, Incidents, Workbooks (selected), Hunting, Notebooks, Configuration, Data connectors, Analytics, Playbooks, Community, and Settings. The main area displays 'Saved workbooks' (49) and 'Templates' (39). A callout labeled 'Templates' points to the 'Templates' section. A callout labeled 'Use workbook' points to a preview of the 'Azure Activity' template, which includes a description, required data types (AzureActivity), relevant data connectors (AzureActivity), and a preview chart.

Home > Azure Sentinel - Workbooks

Azure Sentinel - Workbooks
Selected workspace: 'CyberSecurityDemo'

Search (Ctrl+ /) Refresh + Add workbook

General

- Overview
- Logs
- News & guides
- Threat management
- Incidents
- Workbooks**
- Hunting
- Notebooks

Configuration

- Data connectors
- Analytics
- Playbooks
- Community
- Settings

49 Saved workbooks + 39 Templates 0 Updates

My workbooks Templates

Search workbooks

Azure Activity MICROSOFT

Gain extensive insight into your organization's Azure Activity by analyzing, and correlating all user operations and events. You can learn about all user operations, trends, and anomalous changes over time. This workbook gives you the ability to drill down into caller activities and summarize detected failure and warning events.

Required data types: ⓘ

✓ AzureActivity

Relevant data connectors: ⓘ

AzureActivity

Azure Activity MICROSOFT

Azure AD Audit logs MICROSOFT

Azure AD Sign-in logs MICROSOFT

Azure Firewall MICROSOFT

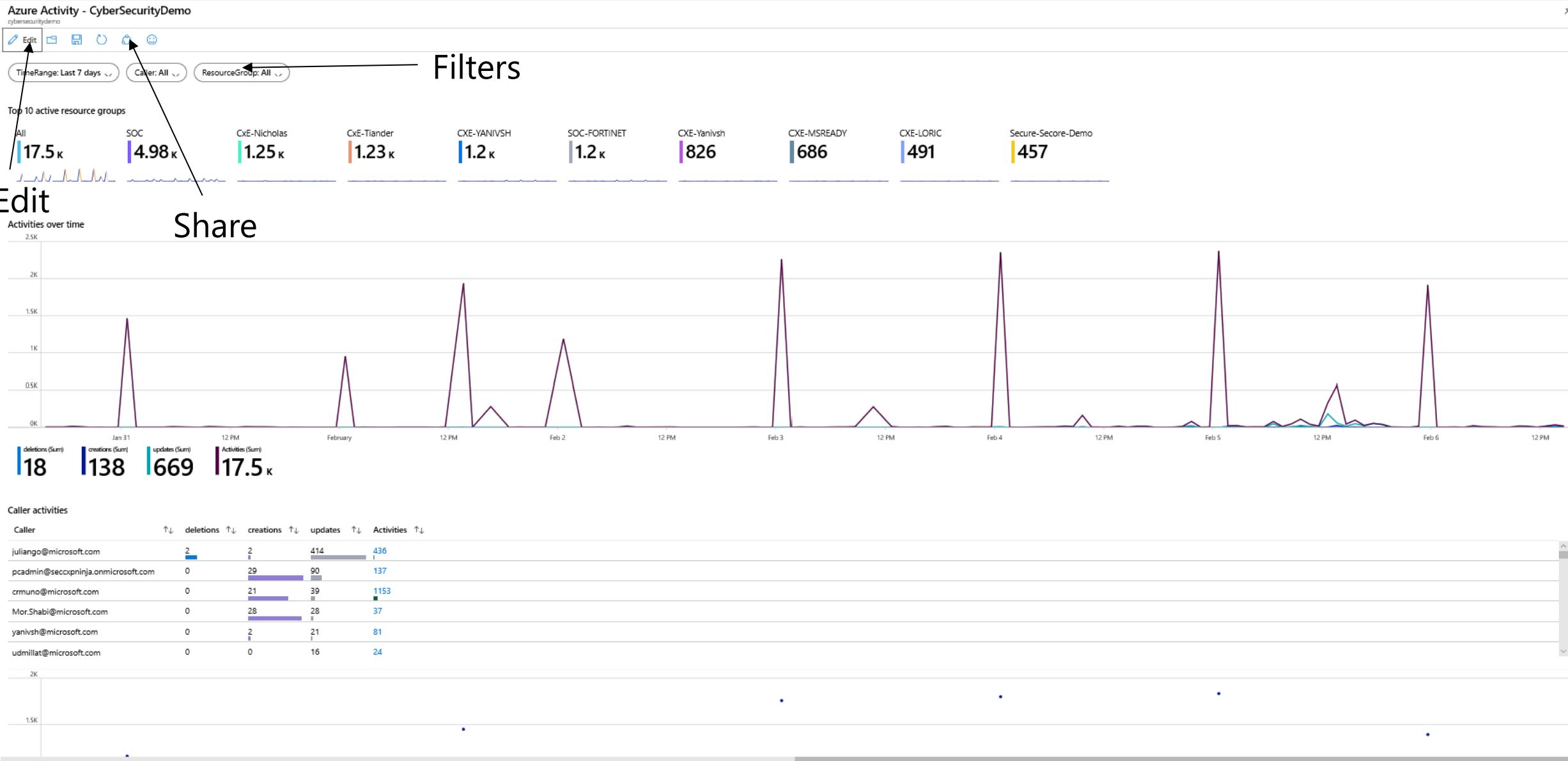
Azure Information Protection - Usage Report MICROSOFT

Azure Network Watcher MICROSOFT

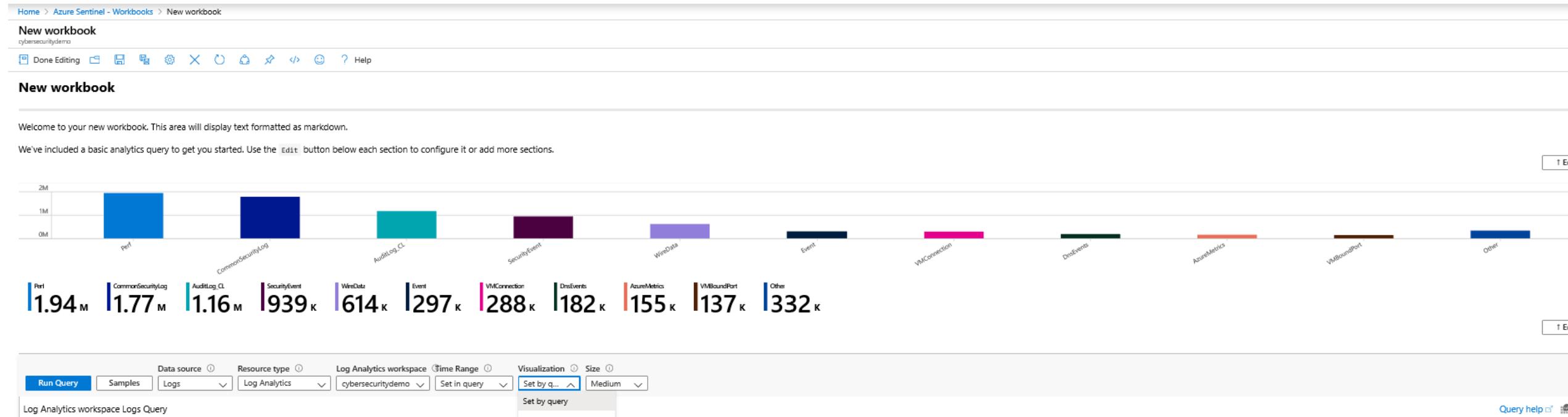
Barracuda Cloud FW

View saved workbook View template Delete

Workbooks in edit



Workbooks in edit



Visualization Options



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

Custom Workbooks

Add New Workbook

Home > Azure Sentinel - Workbooks

Azure Sentinel - Workbooks
Selected workspace: 'CyberSecurityDemo'

Refresh + Add workbook

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks **Selected**
- Hunting
- Notebooks

Configuration

- Data connectors
- Analytics
- Playbooks
- Community
- Settings

49 Saved workbooks + 39 Templates 0 Updates

My workbooks Templates

Search workbooks

- Azure Activity MICROSOFT
- Azure AD Audit logs MICROSOFT
- Azure AD Sign-in logs MICROSOFT
- Azure Firewall MICROSOFT
- Azure Information Protection - Usage Report MICROSOFT
- Azure Network Watcher MICROSOFT

Barracuda Cloud FW

Azure Activity MICROSOFT

Gain extensive insight into your organization's Azure Activity by analyzing, and correlating all user operations and events. You can learn about all user operations, trends, and anomalous changes over time. This workbook gives you the ability to drill down into caller activities and summarize detected failure and warning events.

Required data types: ⓘ

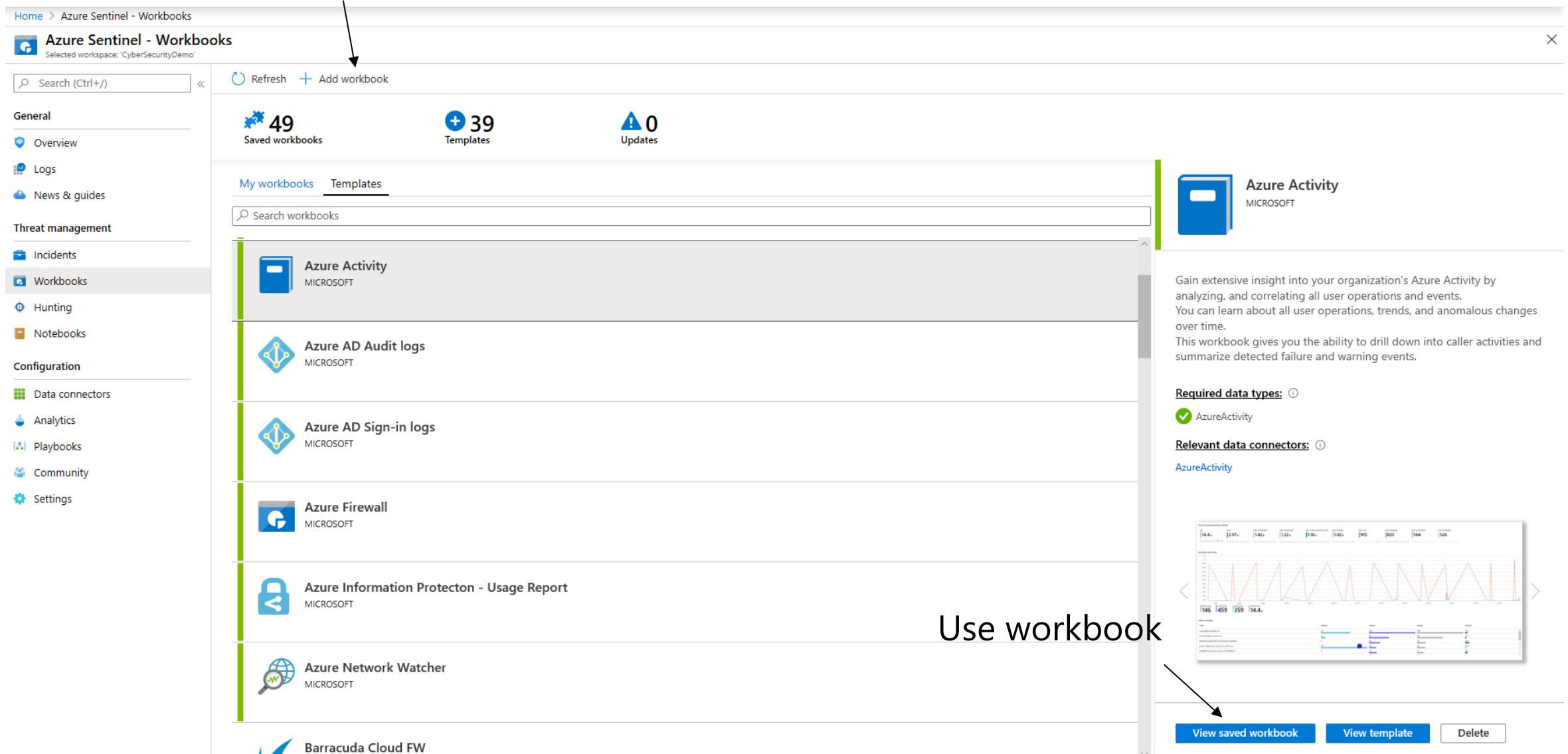
AzureActivity

Relevant data connectors: ⓘ

AzureActivity

Use workbook

View saved workbook View template Delete



Custom Workbooks - Text

New workbook

cybersecuritydemo

 Done Editing            ? Help

1 Editing text item: text - 2

Settings Advanced Settings Style

Markdown text to display

```
## My custom workbook
```

Give your workbook a name

Welcome to your new workbook. This area will display text formatted as markdown.

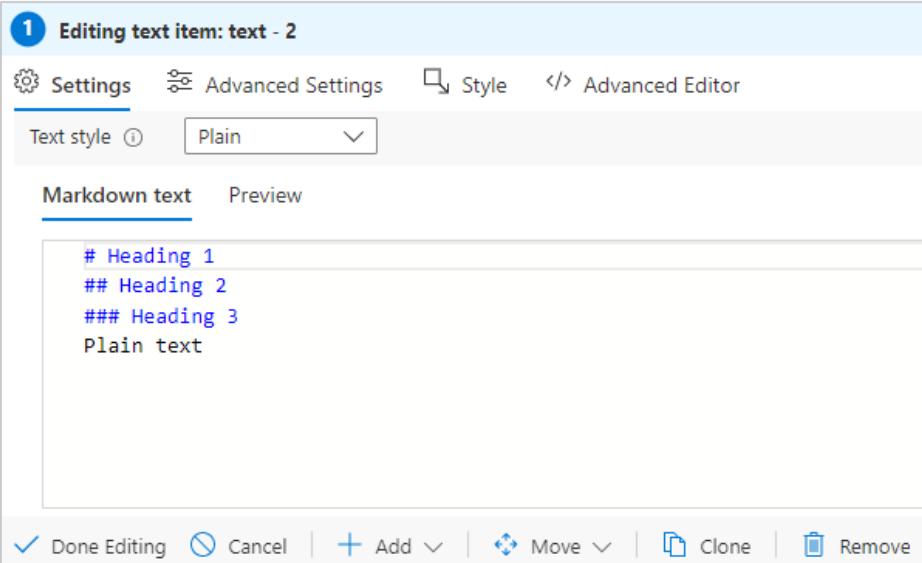
We've included a basic analytics query to get you started. Use the `Edit` button below each section to configure it or add more sections.

Text formatted in markdown

 Done Editing |  Add  |  Move  |  Clone |  Remove

Custom Workbooks - Text

By typing this:



The screenshot shows a software interface for editing text items. At the top, a blue header bar displays "1 Editing text item: text - 2". Below it is a toolbar with "Settings" (selected), "Advanced Settings", "Style", and "Advanced Editor". A dropdown menu "Text style" is set to "Plain". The main area is divided into "Markdown text" and "Preview" tabs, with "Markdown text" currently selected. It contains the following Markdown code:

```
# Heading 1
## Heading 2
### Heading 3
Plain text
```

At the bottom, there are buttons for "Done Editing" (with a checkmark), "Cancel", "Add", "Move", "Clone", and "Remove".

You'll get this:

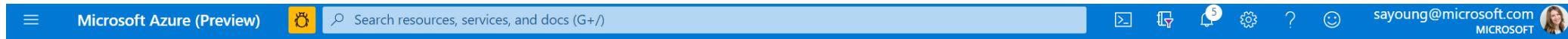
Heading 1

Heading 2

Heading 3

Plain text

Custom Workbooks - Text



Home > Azure Sentinel workspaces > Azure Sentinel | Workbooks >

New workbook X

cybersecuritydemo

Done Editing Save New Import Export Settings Edit Help

New workbook

Welcome to your new workbook. This area will display text formatted as markdown.

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.

↑ Edit | ...

i The query returned no results.

Add text

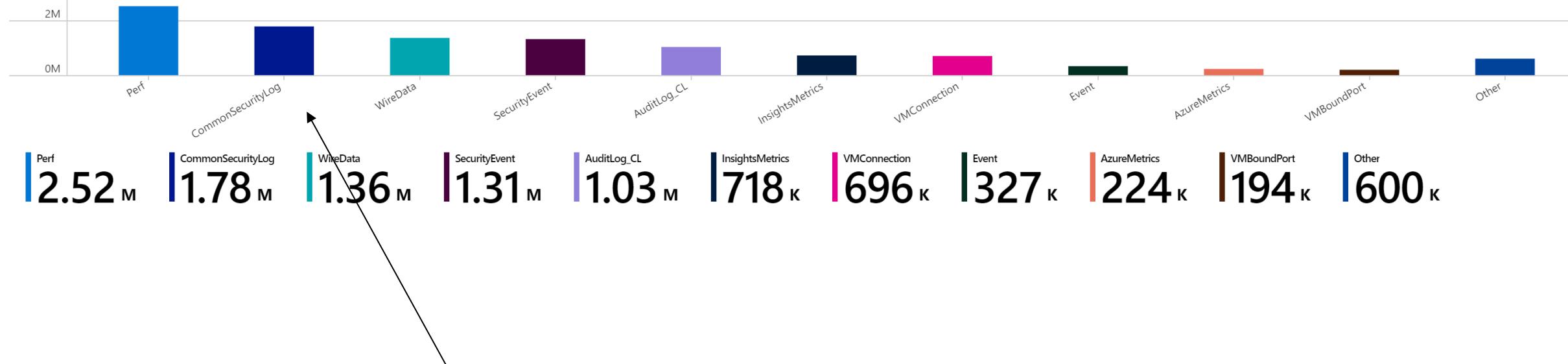
- + Add ▼
 - + Add text
 - </> Add parameters
 - ≡ Add links/tabs
 - grid Add query
 - chart Add metric
 - list Add group (preview)

↑ Edit | ...

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.

[↑ Edit](#)



A basic event ingestion query gets you started

Custom Workbooks - Charts

2 Editing query item: query - 2

Settings Advanced Settings Style

Query (change) Time Range Visualization Size

Run Query Samples cybersecuritydemo Set in query Pie chart Small Chart Settings

Log Analytics workspace Logs Query

```
union withsource=TableName *
| summarize Count=count() by TableName
| render barchart
```

Set by query

Grid

Area chart

Bar chart

Bar chart (Categorical)

Bar chart (Unstacked)

Line chart

Pie chart

Scatter chart

Time chart

Tiles

Graph (preview)

Map (preview)

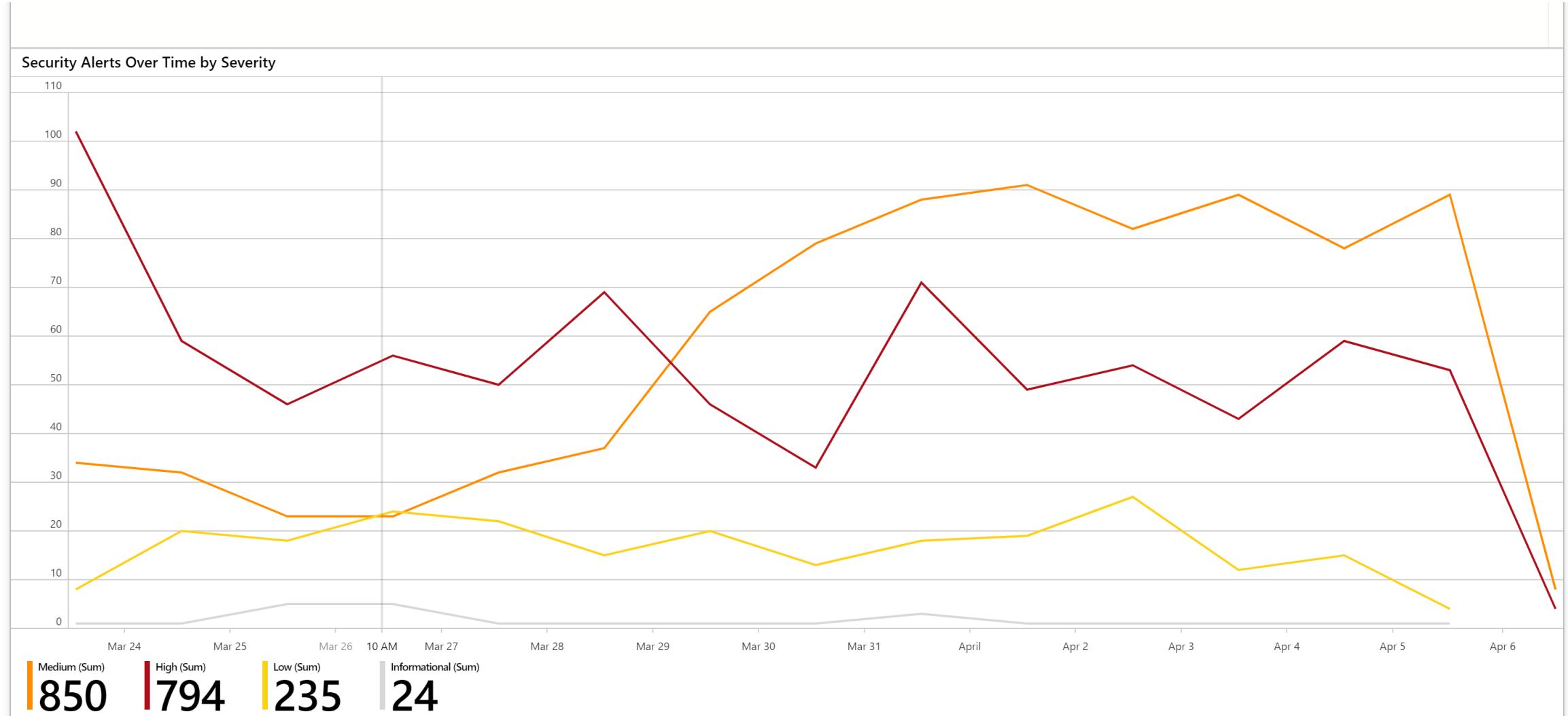
Query behind the graphic

| Category | Count |
|-------------------|--------|
| Other | 2.76 M |
| Perf | 2.52 M |
| CommonSecurityLog | 1.78 M |
| AuditLog_CL | 1.03 M |

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

Done Editing | Add | Move | Clone | Remove

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

Run Query Samples cybersecuritydemo TimeRange Tiles Medium Tile Settings

Log Analytics workspace Logs Query

Query help ↗ ⓘ ⏴

```
SecurityAlert
| where "{AlertSeverity:lable}" == "All" or AlertSeverity in ({AlertSeverity})
| where "{ProductName:lable}" == "All" or ProductName in ({ProductName})
| where AlertSeverity == '{AlertSeverityPicker}' or '{AlertSeverityPicker}' == "All"
| where ProductName == '{ProductNamePicker}' or '{ProductNamePicker}' == "All"
| extend Entities = iff(isempty(Entities), todynamic('["dummy": ""]', todynamic(Entities)))
| mvexpand Entities
| evaluate bag_unpack(Entities, "Entity_")
| extend Entity_Type = columnifexists("Entity_Type", "")
| extend Entity_Name = columnifexists("Entity_Name", "")
| extend Entity_ResourceId = columnifexists("Entity_ResourceId", "")\
```

Top Entities in Security Alerts

| VICTIMPC | c:\users\jeffl\desktop\re... | VictimPC\$ | 0x4dc | c:\windows\system32\s... | VICTIMPC | 0x4dc | c:\users\jeffl\desktop\re... |
|----------|------------------------------|--------------------------|----------|--------------------------|------------|-----------|------------------------------|
| 96 | 93 | 93 | 93 | 93 | 55 | 54 | 54 |
| 54 | 54 | ContosoDC | 51 | c:\windows\system32\s... | 51 | 0x4dc | c:\users\jeffl\desktop\re... |
| 50 | 50 | c:\windows\system32\s... | VICTIMPC | 0x4dc | VictimPC\$ | 51 | VictimPC\$ |
| 50 | 50 | VictimPC2 | 49 | 50 | 50 | 50 | Jeff Leatherman |
| 48 | 50 | Jeff Leatherman | 49 | 49 | 48 | 48 | c:\users\jeffl\desktop\re... |
| 48 | 0x4dc | VictimPC2 | 47 | VictimPC | 47 | VictimPC2 | VICTIMPC |
| 48 | 48 | Jeff Leatherman | 47 | VictimPC | 47 | 47 | 46 |
| 48 | 48 | VictimPC2 | 47 | VictimPC | 47 | 46 | VictimPC\$ |

Custom Workbooks - Graphs

Security Alerts - CyberSecurityDemo

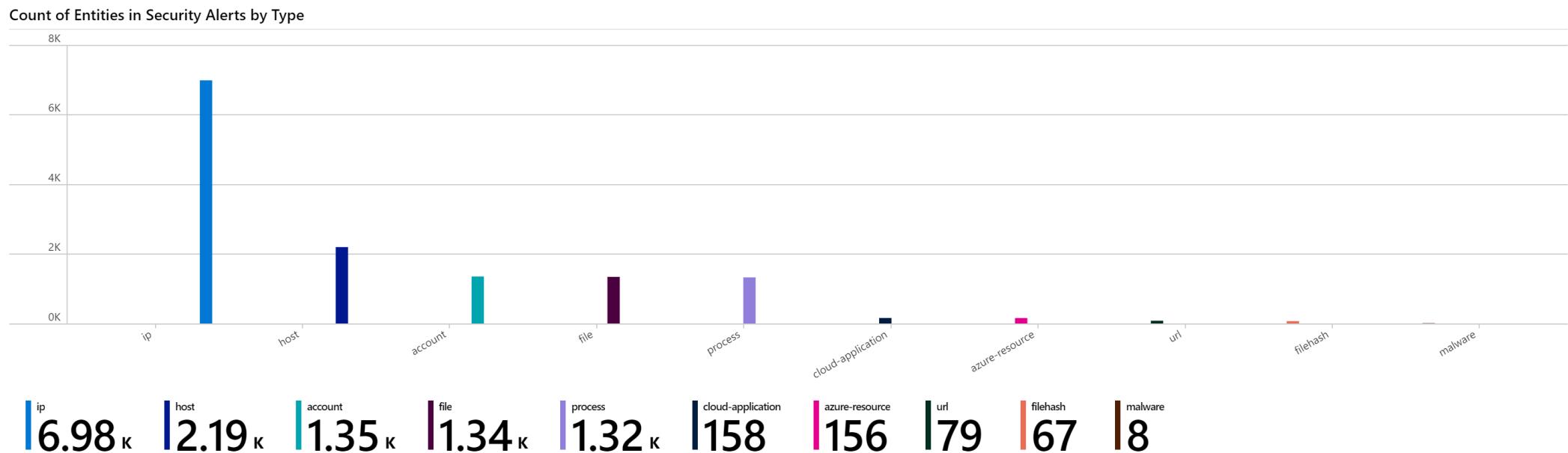
cybersecuritydemo

Done Editing ? Help

```
| where "{ProductName:label}" == "All" or ProductName in ({ProductName})
| where AlertSeverity == '{AlertSeverityPicker}' or '{AlertSeverityPicker}' == "All"
| where ProductName == '{ProductNamePicker}' or '{ProductNamePicker}' == "All"
| extend Entities = ifempty(Entities), todynamic('[{"dummy" : ""}]'), todynamic(Entities))
| mvexpand Entities
| evaluate bag_unpack(Entities, "Entity_")
| extend Entity_Type = columnifexists("Entity_Type", "")
| extend Entity_Name = columnifexists("Entity_Name", "")
| extend Entity_DocumentId = columnifexists("Entity_DocumentId", "")
```

Top Entities in Security Alerts

✓ Done Editing | + Add | Move | Clone | Remove

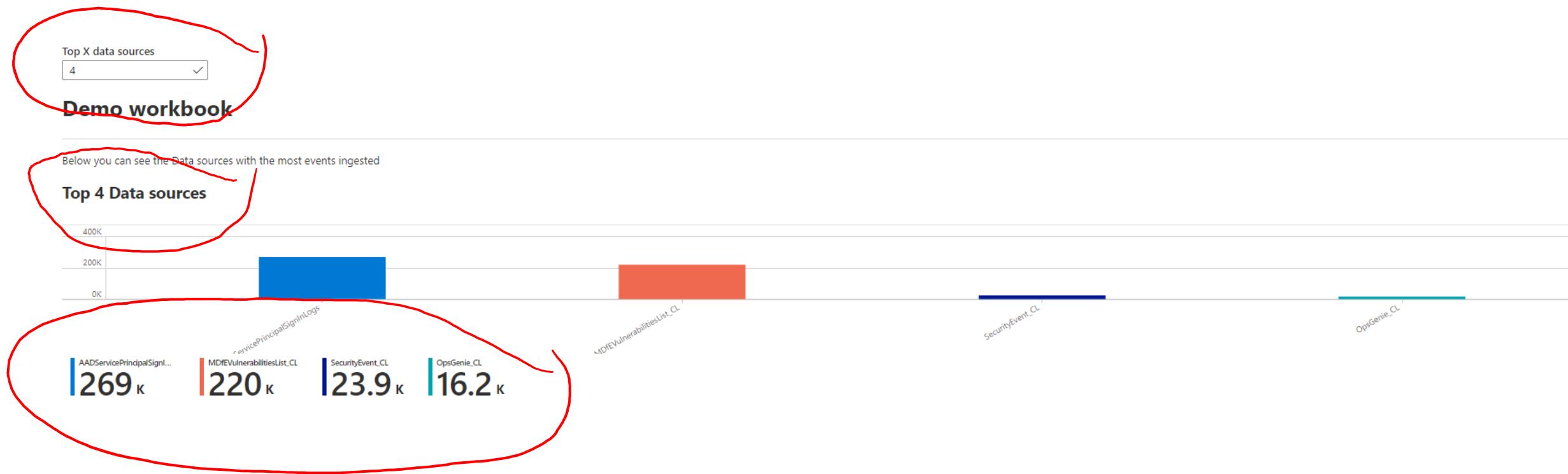


Custom Workbooks - Graph/Hives



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:

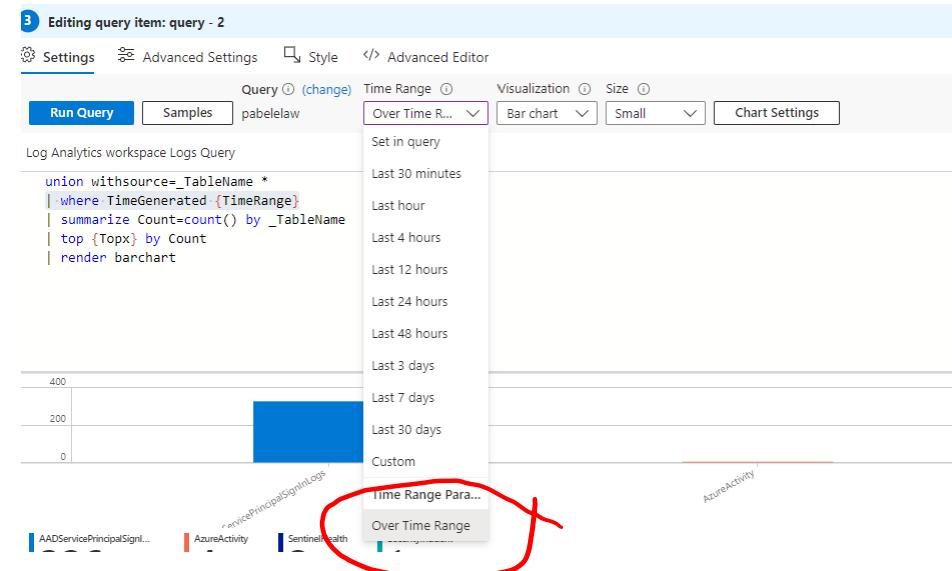
- Time - allows a user to select from prepopulated time ranges or select a custom range
- Drop down - allows a user to select from a value or set of values
- Text - allows a user to enter arbitrary text
- Resource - allows a user to select one or more Azure resources
- Subscription - allows a user to 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 dropdown 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
```

Edit Parameter

pabelelaw

Save Revert changes Cancel Help

Settings Advanced Settings

Parameter name *

Topx

Display name

Top X data sources

Parameter type

Text

Parameter field style

Standard Password Multiline

Required?



Explanation

What is this parameter used for?

Hide parameter in reading mode



Get data from

None Query Criteria

Settings Advanced Settings

Treat this parameter as a global

Add Validations

Regular Expression

Match

Message

[0-9]



Only numbers are accepted!



Custom Workbooks – Drop Down Parameter

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

Provide 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.).

The screenshot shows the Data Studio interface with a modal dialog titled "Edit Parameter". The parameter is named "Environment" and is defined as a "Drop down" type. It is marked as required. The "Default items" dropdown menu is open, showing options: "Select", "Default items", "Items", "Development", "Pre-production", and "Production". The "Production" option is currently selected. On the right side of the dialog, there are fields for "Allow multiple selections", "Limit multiple selections", "Delimiter", "Quote with", "Explanation", and "Hide parameter in reading mode". Below the dialog, the main workspace shows a "TimeRange" set to "Last 24 hours" and a "Environment" step with the "Production" item selected. The "JSON Input" section at the bottom contains the following JSON code:

```
{ "value": "dev", "label": "Development" },  
{ "value": "ppe", "label": "Pre-production" },  
{ "value": "prod", "label": "Production", "selected": true }
```

Custom Workbooks – Drop Down Query Parameter

Home > Microsoft Sentinel > Microsoft Sentinel >

Demo workbook

pabelelaw

Done Editing Open Advanced Settings Style Advanced Editor

Group type: Editable Load type: Lazy Edit Group

1 Editing parameters item: parameters - 0

Settings Advanced Settings Style Advanced Editor

Add Parameter Standard | TimeRange UPN UserPrincipalName Drop down

Required? Parameter name: UPN Display name: UserPrincipalName Parameter type: Drop down

TimeRange Time range parameter

TimeRange UPN UserPrincipalName Drop down

TimeRange UserPrincipalName

Last 48 hours admin@m365x898158.onmicrosoft.com

Done Editing Cancel Add Move Clone Remove

2 Editing query item: query - 1

Settings Advanced Settings Style Advanced Editor

Run Query Samples Query (change) Time Range Visualization Size Chart Settings

Log Analytics workspace Logs Query

SignInLogs
| where TimeGenerated <= TimeRange and UserPrincipalName == '{UPN}'
| summarize Count=count() by ResultDescription
| render piechart

Edit Parameter

pabelelaw

Save Revert changes Cancel Help

Settings Advanced Settings

Parameter name: UPN Display name: UserPrincipalName Parameter type: Drop down Required? Allow multiple selections Limit multiple selections Delimiter: , Quote with: ' Explanation: What is this parameter used for? Hide parameter in reading mode

Get data from: Query JSON

Log Analytics workspace Logs Query

Query (change) Time Range

Run Query pabelelaw Set in query Samples

SignInLogs
| where TimeGenerated <= TimeRange
| summarize Count=count() by UserPrincipalName
| order by UserPrincipalName asc

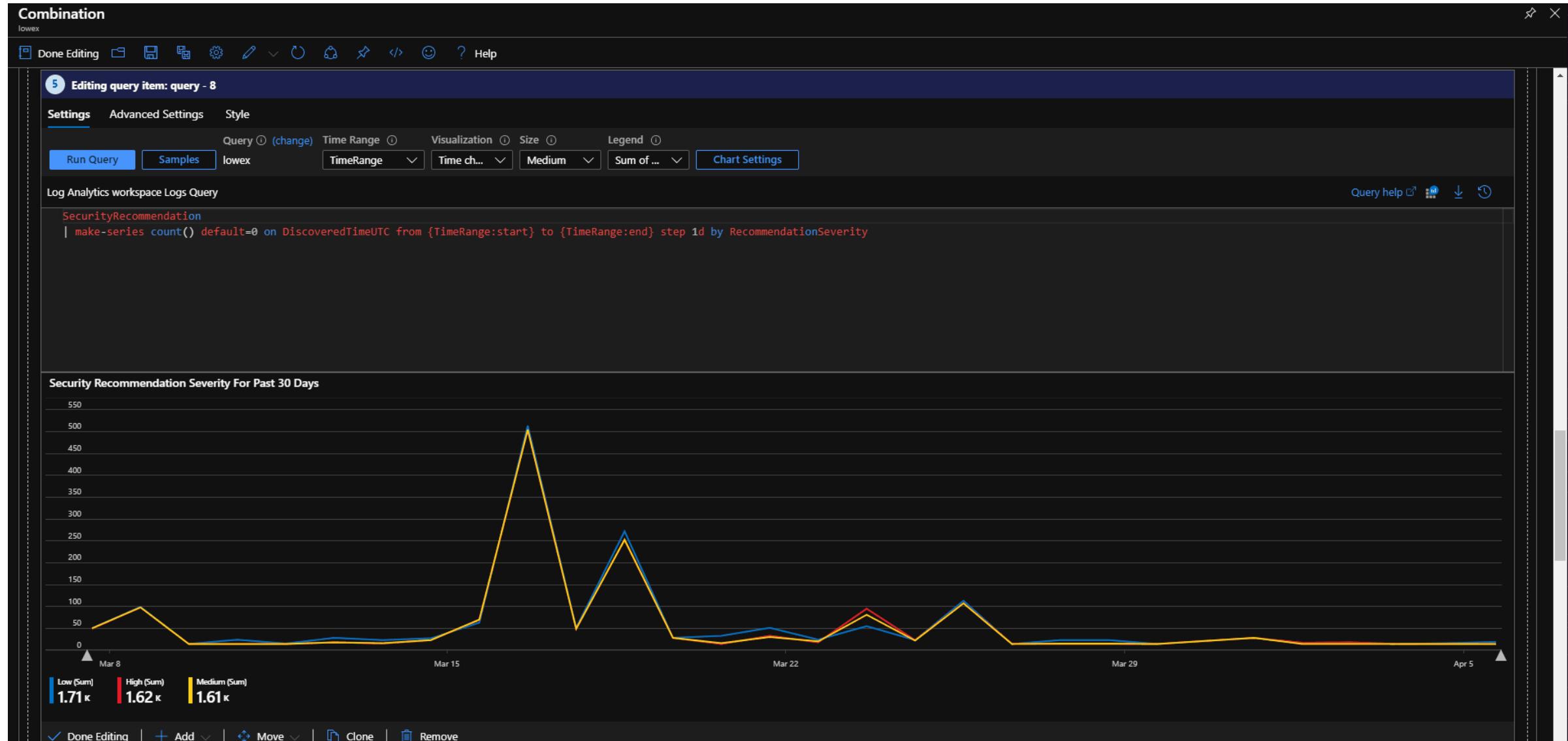
UserPrincipalName ↑
admin@m365x898158.onmicrosoft.com

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

The screenshot shows the 'Editing query item: query - 8' interface. The 'Advanced Settings' tab is selected. Under 'Step name', 'query - 8' is listed. In the 'Advanced Settings' section, there are several checkboxes: 'Make this item conditionally visible', 'Always show the pin icon on this step', 'When items are selected, export parameters', 'Show query when not editing', 'Show open external query button when not editing', and 'Show Export to Excel button when not editing'. A 'Columns to Export' section has 'Visible Columns' selected. Under 'Time Range', 'Enable time range brushing' is checked. A 'Time Brush' dropdown menu is open, showing 'TimeBrush' as the selected option. A 'Time Range' dropdown menu at the bottom also shows 'TimeBrush'.

Parameter Setup



Setting the Time Range

Combination
lowex

Done Editing Help

Resources with Recommendations in '3/7/2020 3:07 PM - 4/5/2020 4:07 PM' ↻ Recommendations for Selected Resource

Search

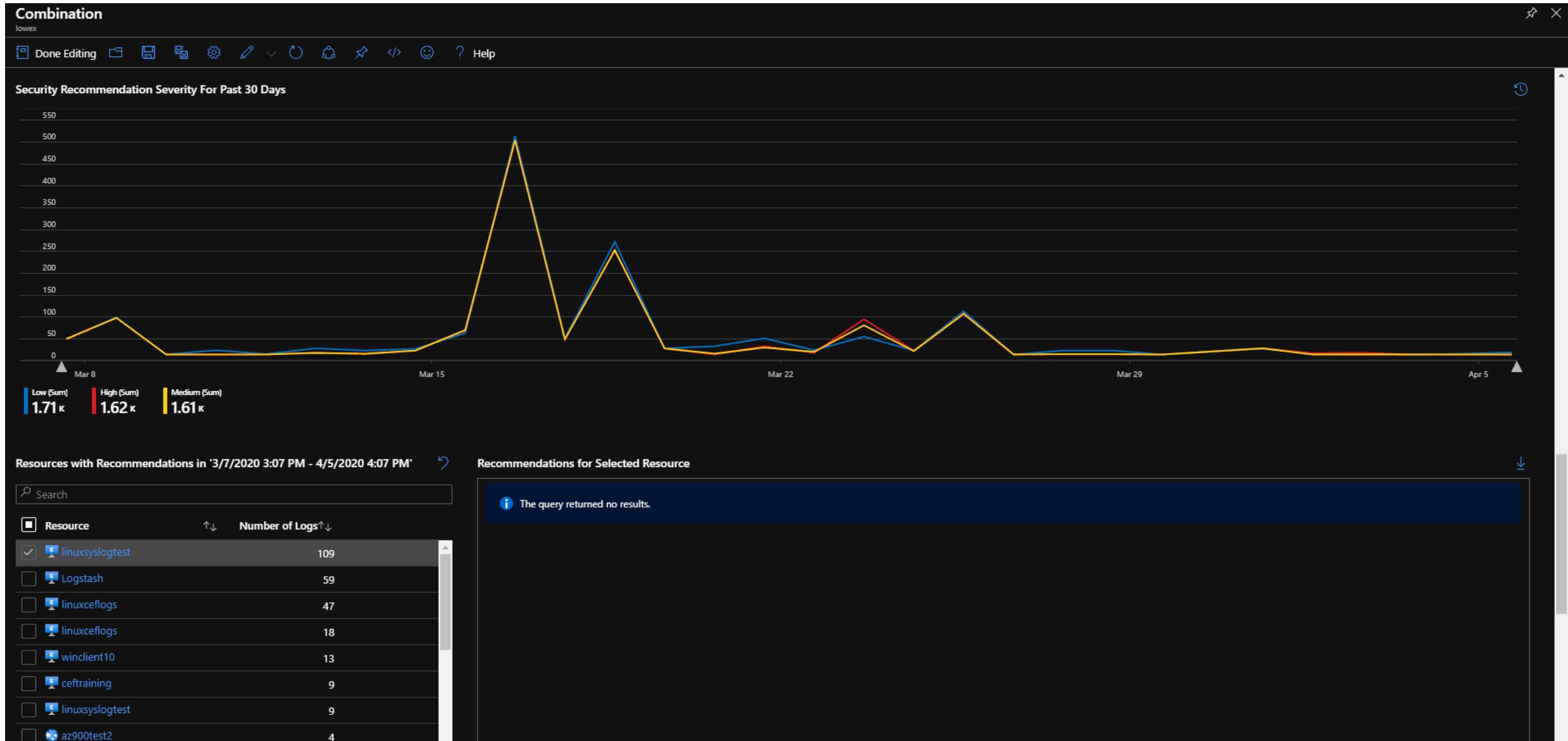
| Resource | Number of Logs |
|-----------------|----------------|
| linuxsyslogtest | 109 |
| Logstash | 59 |
| linuxceflogs | 47 |
| linuxceflogs | 18 |
| winclient10 | 13 |
| ceptraining | 9 |
| linuxsyslogtest | 9 |
| az900test2 | 4 |
| logstash | 4 |
| Logstash | 2 |
| testing | 2 |

The query returned no results.

Related Alerts to Resource in '3/7/2020 3:07 PM - 4/5/2020 4:07 PM'

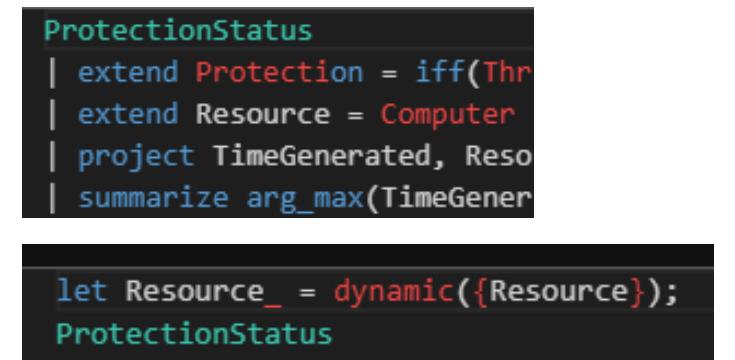
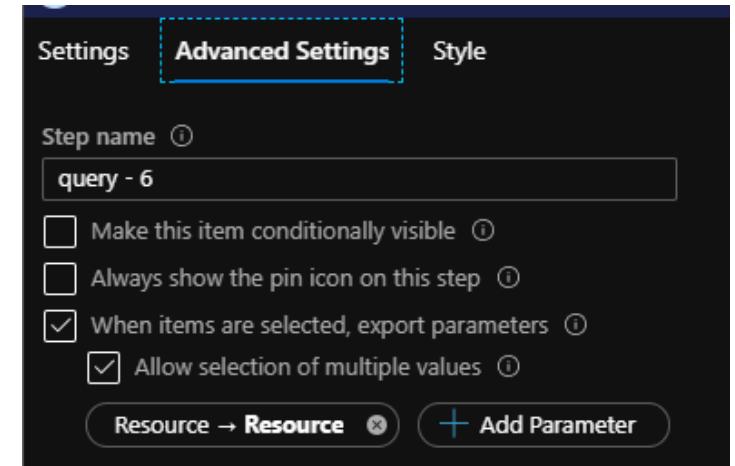
The query returned no results.

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:
 - 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

Combination
lowex

Done Editing Add Move Clone Remove

Settings Advanced Settings Style

Query (change) Time Range Visualization Size

Run Query Samples lowex TimeBrush Set by q... Medium Column Settings

Log Analytics workspace Logs Query

SecurityRecommendation
| where RecommendationState contains 'unhealthy'
| extend Resource = AssessedResourceId
| summarize count() by Resource, RecommendationState
| project-away RecommendationState
| sort by count_ desc

Resources with Recommendations in '3/7/2020 3:07 PM - 4/5/2020 4:07 PM'

Search

| Resource | Number of Logs |
|-----------------|----------------|
| linuxsyslogtest | 109 |
| Logstash | 59 |
| linuxceflogs | 47 |
| linuxceflogs | 18 |
| winclient10 | 13 |
| cefraining | 9 |
| linuxsyslogtest | 9 |
| az900test2 | 4 |
| logstash | 4 |
| mattlevenhub | 2 |
| logstashexport | 2 |

Done Editing Add Move Clone Remove

Calling the Parameter

Combination
lowex

Done Editing | ... | ↑ Edit

Resources with Recommendations in '3/7/2020 3:07 PM - 4/5/2020 4:07 PM' ↻

Search

| Resource | Number of Logs |
|--------------------|----------------|
| linuxsyslogtest | 109 |
| Logstash | 59 |
| linuxceflogs | 47 |
| linuxceflogs | 18 |
| winclient10 | 13 |
| ceftraining | 9 |
| linuxsyslogtest | 9 |
| az900test2 | 4 |
| logstash | 4 |
| mattleventhub | 2 |
| {A} logstashexport | 2 |

↑ Edit | ... | ↑ Edit

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 '3/7/2020 3:07 PM - 4/5/2020 4:07 PM'

✖ Query could not be parsed at ')' on line [2,24]
Token: ')' Line: 2 Postion: 24
Click to Retry.

Demo

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 |
| ... 250 more | |

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 once 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.

Demo workbook

pabelelaw

Done Editing Open Grid Style Advanced Editor 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 | App |
|------------------------|-----------------------------------|------------|--|-----|
| 4/26/2022, 7:16:51 PM | alexw@m365x898158.onmicrosoft.com | ✓ 0 | | Azu |
| 4/26/2022, 11:34:07 AM | alexw@m365x898158.onmicrosoft.com | ! 50055 | Invalid password, entered expired password. | Azu |
| 4/26/2022, 11:34:22 AM | alexw@m365x898158.onmicrosoft.com | ! 50140 | This error occurred due to 'Keep me signed in' interrupt ... | Azu |
| 4/26/2022, 11:34:26 AM | alexw@m365x898158.onmicrosoft.com | ✓ 0 | | Azu |
| 4/26/2022, 11:45:30 AM | alexw@m365x898158.onmicrosoft.com | ✓ 0 | | Azu |
| 4/26/2022, 11:48:30 AM | alexw@m365x898158.onmicrosoft.com | ✓ 0 | | Azu |

Done Editing

+ Add

Edit column settings

Add **Remove** **Restore defaults**

Settings**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

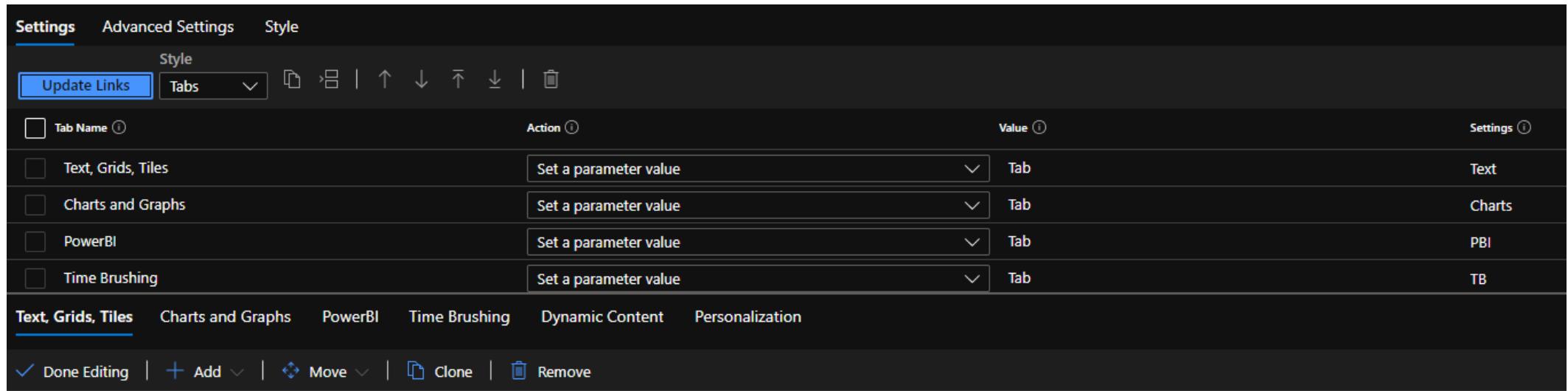
 Not a tree Parent/Child Group By

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

The image displays two screenshots of a software interface for managing tabs in a custom workbook.

Screenshot 1: Editing links item: links - 1

This screenshot shows the configuration of a "links" item. It includes settings for "Style" (Tabs) and "Tab size" (Normal). The "Update Links" button is highlighted. The main area lists four items under "Action":

| Action | Value | Settings |
|-----------------------|-------|----------|
| Set a parameter value | Tab | Text |
| Set a parameter value | Tab | Charts |
| Set a parameter value | Tab | TB |
| Set a parameter value | Tab | DC |

Below the table are tabs for "Text, Grids, Tiles", "Charts and Graphs", "Time Brushing", "Dynamic Content", and "Personalization".

Screenshot 2: Editing group item: TGT

This screenshot shows the configuration of a "TGT" group item. It includes settings for "Advanced Settings" and "Style". The "Step name" is set to "TGT". The "Make this item conditionally visible" checkbox is checked. A condition is defined: "Tab equals Text" AND "(Parameter name) equals not set". The "Group title" is set to "Group title".

At the bottom of both screenshots are standard editing controls: "Done Editing", "Cancel", "Add", "Move", "Clone", and "Remove".

Demo

Edit

Text, Grids, Tiles Charts and Graphs PowerBI Time Brushing Dynamic Content Personalization

This is an example of text being put in a workbook.

Time Parameter: Last 24 hours ▾

| 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, 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 |

| | | | | | | | | | |
|--------------------------------|---------------------------|------------------------------------|--------------------------|-----------------------------------|------------------------------------|------------------------------|--------------------------------------|---------------------------|---------------------------|
| WireData 24 | AzureMetrics 24 | Heartbeat 23 | Perf 23 | ConfigurationData 23 | ServiceMapComputer_CL 23 | InsightsMetrics 23 | ConfigurationChange 23 | VMConnection 23 | VMProcess 23 |
| NetworkMonitoring 23 | VMComputer 23 | ProtectionStatus 23 | VMBoundPort 23 | ServiceMapProcess_CL 23 | Event 21 | AzureActivity 19 | AzureNetworkAnalytics... 8 | Update 7 | UpdateSummary 7 |
| AzureDiagnostics 6 | SecurityAlert 6 | SecurityRecommendation 2 | Operation 1 | WindowsFirewall 1 | | | | | |

Sharing workbooks

The screenshot shows the Azure Sentinel Workbooks interface. At the top, there's a navigation bar with 'Home > Azure Sentinel | Workbooks > AWS Network Activities - CyberSecurityDemo'. Below it, the title 'AWS Network Activities - CyberSecurityDemo' and the identifier 'cybersecuritydemo' are displayed. A toolbar with icons for 'Edit', 'Share', 'Copy', 'Refresh', 'Import', and 'Export' is visible. The main area is titled 'AWS network activities' and includes a 'TimeRange: Last 14 days' dropdown. A section labeled 'Top 10 active regions - click to filter' is shown. On the right, a modal window titled 'Share Report' is open, showing the report title 'AWS Network Activities - CyberSecurityDemo' Workbooks report'. It contains a heading 'Share a link to this report' and a note that recipients need access to the Azure resource. It includes a 'Link to share' field with the URL <https://go.microsoft.com/fwlink/?linkid=874159&res> and a 'Share link via email' button.

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

Where to from here?

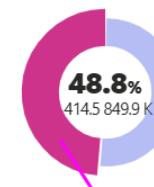
- Monitor workbooks documentation - <https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview>
- How to use Azure Monitor Workbooks to map Sentinel data -
<https://techcommunity.microsoft.com/t5/azure-sentinel/how-to-use-azure-monitor-workbooks-to-map-sentinel-data/ba-p/971818>
- 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>

Hands on Lab !

TEST Workbook

Welcome to TEST workbook.

widget 1



48.8%
414.5 849.9 K

Failure 435 k Success 414 k

Click

widget 2

| TimeGenerated | Identity | ResultDescription |
|-----------------------------|----------|-------------------|
| 11/17/2024, 11:14:30.772 AM | u896 | |
| 11/17/2024, 11:02:00.915 AM | u3289 | |
| 11/17/2024, 7:47:29.433 PM | u3367 | Details |
| 11/17/2024, 7:47:14.015 PM | u3367 | |
| 11/17/2024, 7:38:28.488 PM | u1219 | |

CSA Dashboard x

sentinel-law - Microsoft Azure x

https://portal.azure.com/#@MngEnvMCAP103564.onmicrosoft.com/resource/subscriptions/af9d3219-0de2-484a-9a14-9d8a824fc692/resourceGroups/Sentinel... ...

Microsoft Azure Search resources, services, and docs (G+)

Home > Log Analytics workspaces > sentinel-law

sentinel-law | Workbooks | Windows Event ...

Log Analytics workspace

Workbooks Done Editing ...

DefaultSubscription_Int... Subscription Workspace Time Range Show Help Yes No

af9d3219-0de2-484a-9... ME-MngEnvMCAP103564-jaele-1 sentinel-law Last 60 days

↑ 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
OK
count_(Sum)
4.9 M

Aug 27 Sep 3 Sep 10

Event Filter ...

| | Event..↑↓ | Count ↑↓ |
|--------------------------|-----------|------------------|
| <input type="checkbox"/> | 4658 | 1,261,051 |
| <input type="checkbox"/> | 5156 | 972,285 |
| <input type="checkbox"/> | 5158 | 757,941 |
| <input type="checkbox"/> | 4690 | 645,195 |
| <input type="checkbox"/> | 4656 | 605,570 |
| <input type="checkbox"/> | 5152 | 254,260 |

Device Filter ...

| | Source_Device | Count ↑↓ |
|--------------------------|---------------|------------------|
| <input type="checkbox"/> | dc01.ms.local | 4,873,521 |
| <input type="checkbox"/> | Az-VM-Win11 | 26,166 |

Account Filter ...

| | UserName | Count ↑↓ |
|--------------------------|----------|------------------|
| <input type="checkbox"/> | N/A | 4,889,516 |
| <input type="checkbox"/> | S-1-5-18 | 7,702 |
| <input type="checkbox"/> | S-1-5-19 | 1,507 |
| <input type="checkbox"/> | S-1-5-20 | 962 |

Log Filter ...

| | LogSource | Count ↑↓ |
|--------------------------|--------------------------|------------------|
| <input type="checkbox"/> | Security-Microsoft-Wi... | 4,889,646 |
| <input type="checkbox"/> | Microsoft-Windows-A... | 10,179 |
| <input type="checkbox"/> | Security-Microsoft-Wi... | 3 |

Error Filter ...

| | Description | Count ↑↓ |
|--------------------------|--------------------------------|------------------|
| <input type="checkbox"/> | The handle to an object wa... | 1,261,051 |
| <input type="checkbox"/> | The Windows Filtering Plat... | 972,285 |
| <input type="checkbox"/> | The Windows Filtering Plat... | 757,941 |
| <input type="checkbox"/> | An attempt was made to d... | 645,195 |
| <input type="checkbox"/> | A handle to an object was r... | 616,967 |
| <input type="checkbox"/> | The Windows Filtering Plat... | 254,260 |

Select an event, device, or account to begin