



Workshop

WORKBOOK 101

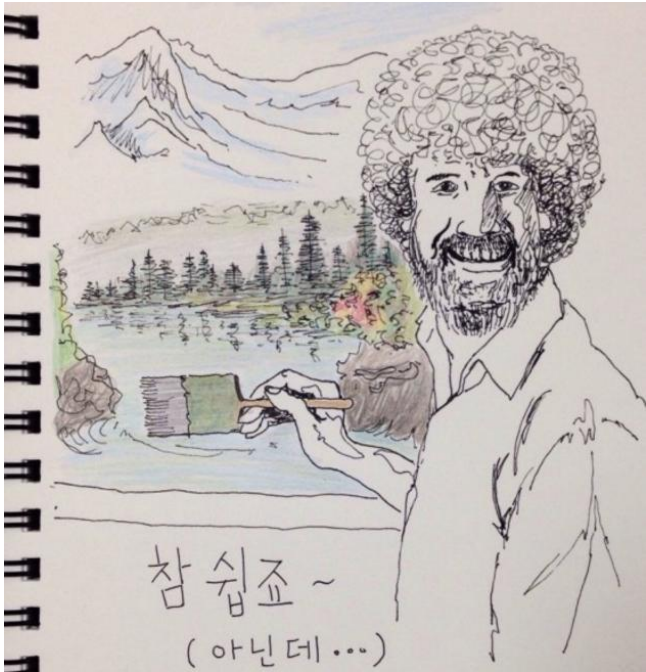
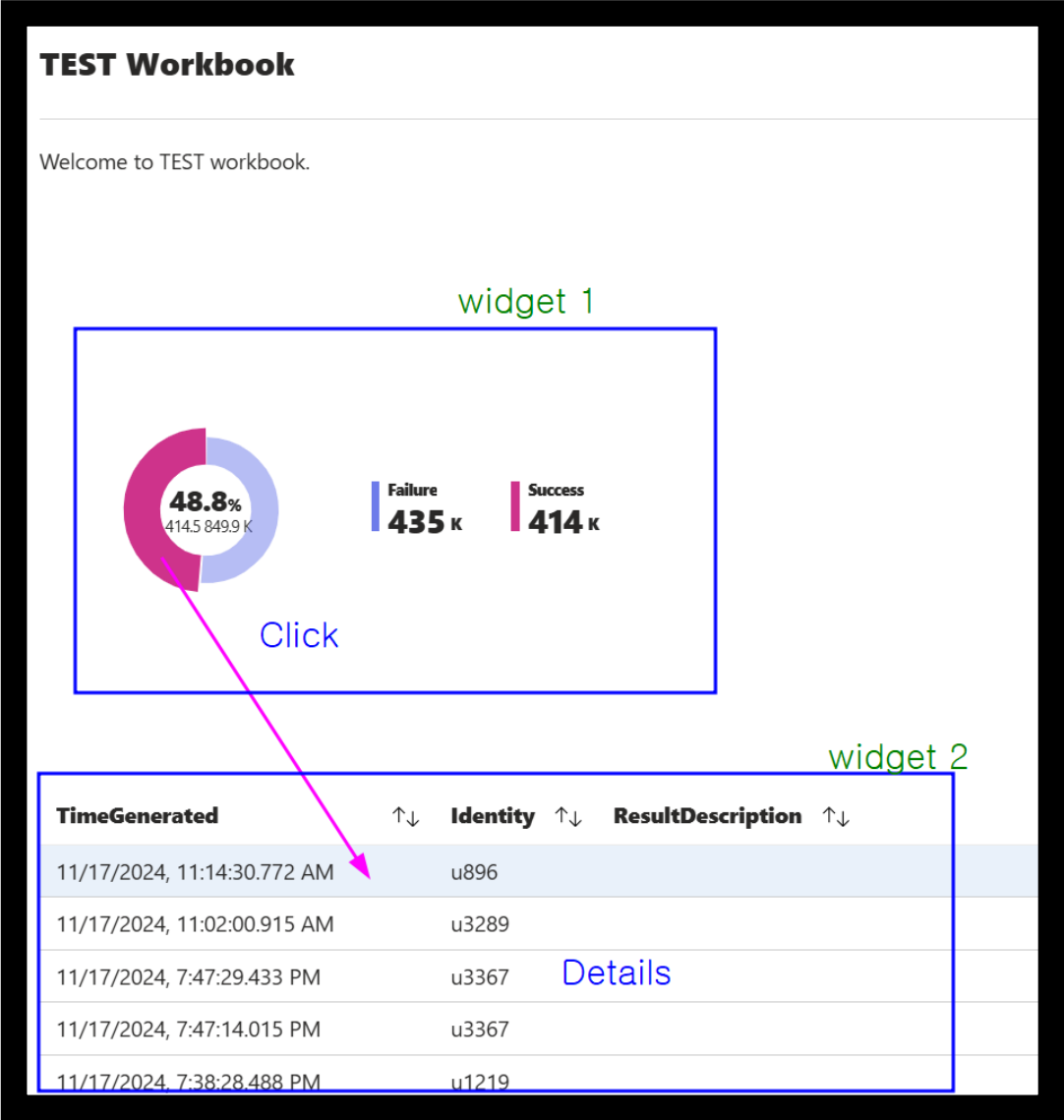


Owen lee
Sr. Cloud Solution Architect | Customer Success

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





workbook visualizations

Out of the Box Workbooks

Add New Workbook

Templates

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

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

Top 10 most common errors

14.4%

2.87%

1.42%

1.22%

1.16%

1.02%

915

620

364

526

Activity and time

14.4%

459

359

14.4%

Time

14.4%

459

359

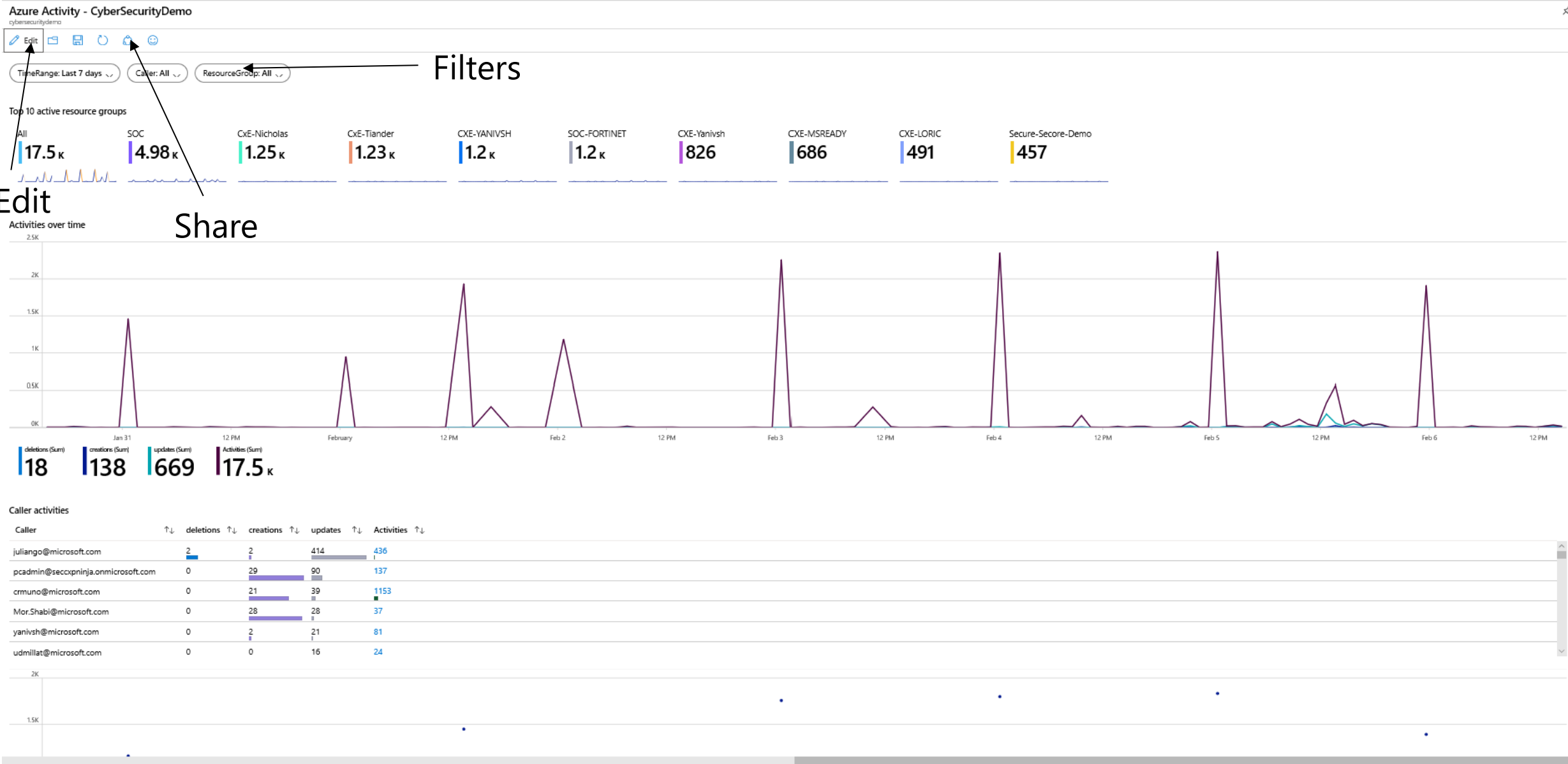
14.4%

View saved workbook

View template

Delete

Workbooks in edit



Workbooks in edit

Home > Azure Sentinel - Workbooks > New workbook

New workbook

cybersecuritydemo

Done Editing

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.

2M

1M

0M

Perf

CommonSecurityLog

AuditLog_CL

SecurityEvent

WireData

Event

VMConnection

DnsEvents

AzureMetrics

VMBoundPort

Other

1.94 M

1.77 M

1.16 M

939 K

614 K

297 K

288 K

182 K

155 K

137 K

332 K

Run Query

Samples

Logs

Log Analytics

cybersecuritydemo

Set in query

Set by query

Medium

Log Analytics workspace Logs Query

Done Editing

Add text | Add query | Add metric | Add parameters | Add links/tabs | | | |

Visualization Options

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)

Add text | Add query | Add metric | Add parameters | Add links/tabs

Custom Workbooks

Add New Workbook

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

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

Top 10 most common errors

14.4%

2.87%

1.42%

1.22%

1.16%

1.02%

1.01%

1.01%

1.01%

1.01%

14.4%

459

359

14.4%

View saved workbook

View template

Delete

Use workbook

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  
---
```

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.

Give your workbook a name

Text formatted in markdown

Done Editing



Add



Move



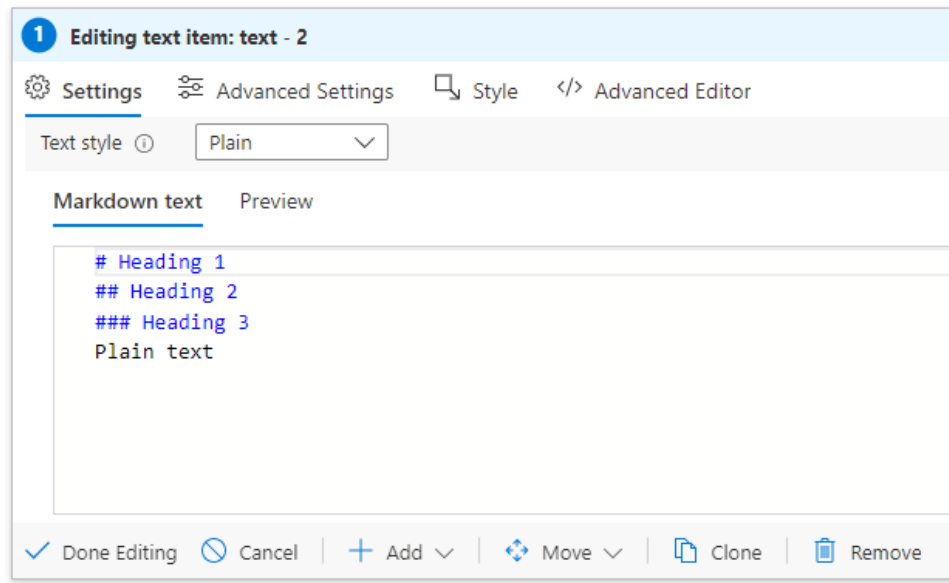
Clone



Remove

Custom Workbooks - Text

By typing this:



You'll get this:

Heading 1

Heading 2







Heading 3

Plain text

Custom Workbooks - Text

Microsoft Azure (Preview)

Search resources, services, and docs (G+/)















sayoung@microsoft.com
MICROSOFT

Home > Azure Sentinel workspaces > Azure Sentinel | Workbooks >

New workbook

cybersecuritydemo

Done Editing



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

...

 The query returned no results.

+ Add

Add text

Add parameters

Add links/tabs

Add query

Add metric

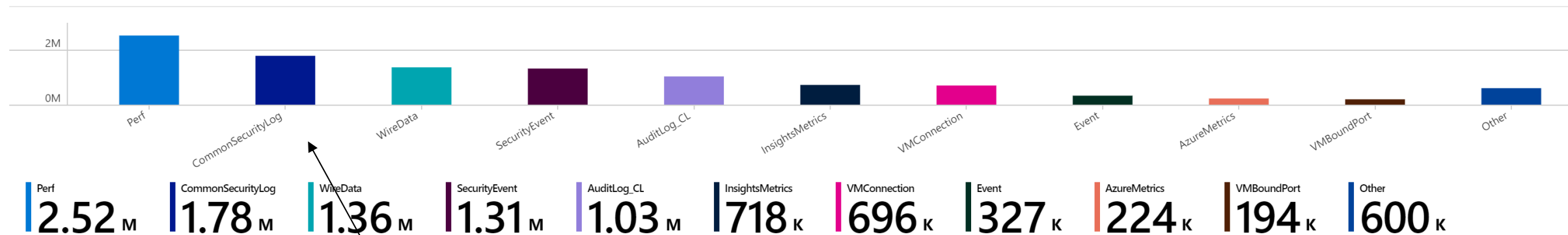
Add group (preview)

Add 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.

1 Edit



A basic event ingestion query gets you started

Custom Workbooks - Charts

2 Editing query item: query - 2

Settings Advanced Settings Style

Run Query Samples Query (change) Time Range (Set in query) Visualization (Pie chart) Size (Small) Chart Settings

Log Analytics workspace Logs Query

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

Log Analytics workspace Logs Query

10.8M

Other 2.76 M Perf 2.52 M CommonSecurityLog 1.78 M AuditLog_CL 1.03 M

Done Editing | Add | Move | Clone | Remove

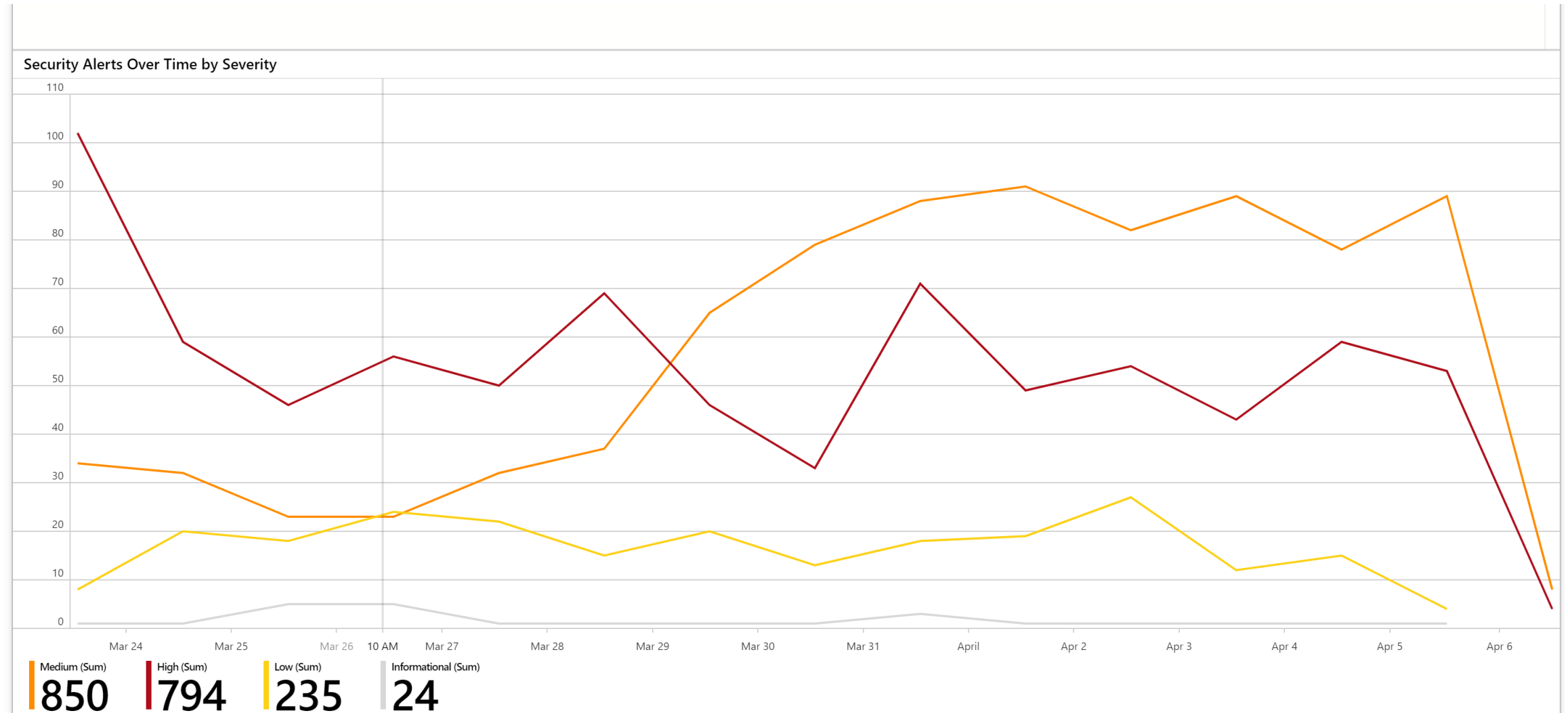
Visualization options:

- 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

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

Custom Workbooks – Time charts

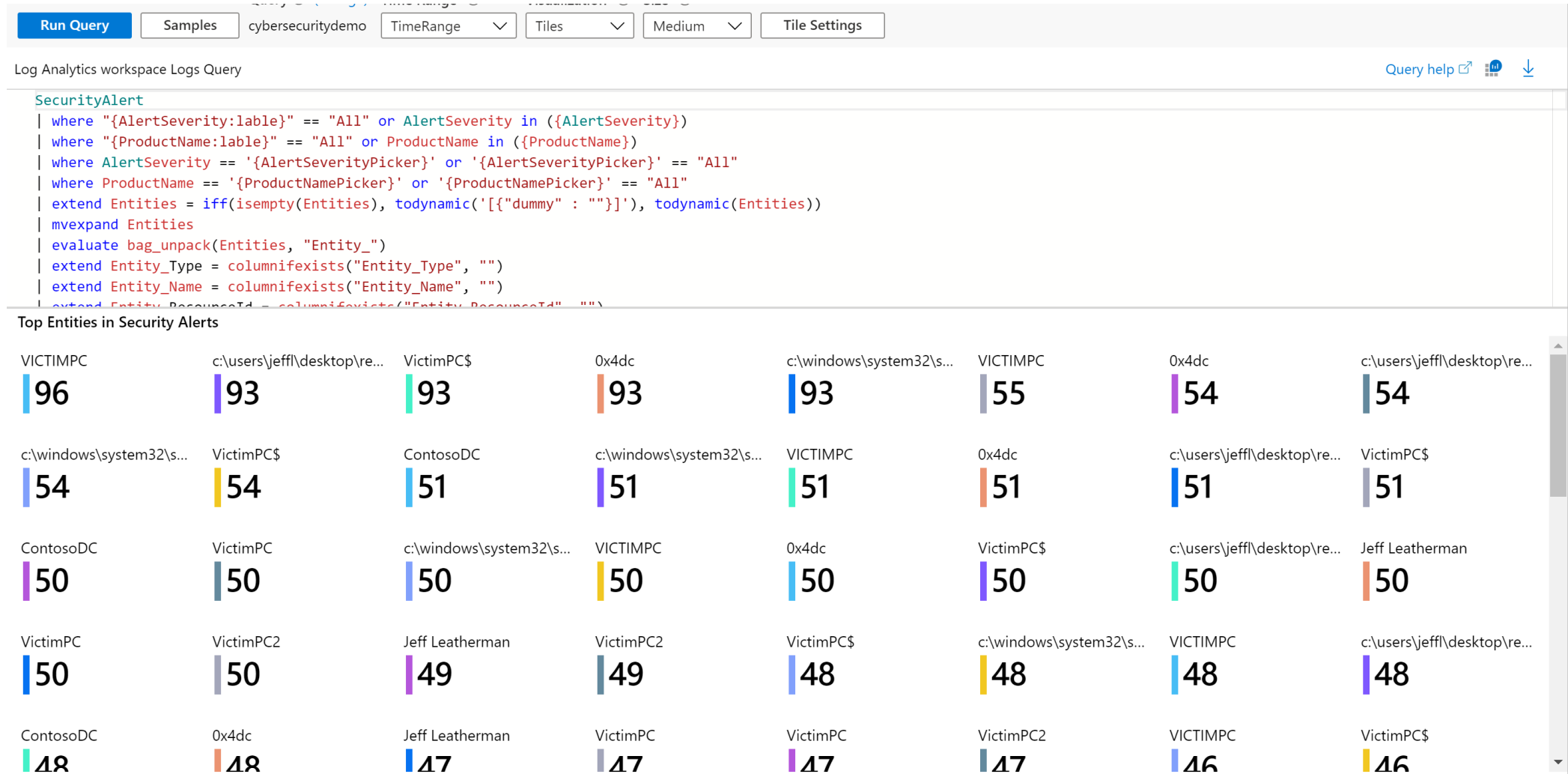


Custom Workbooks - Grids

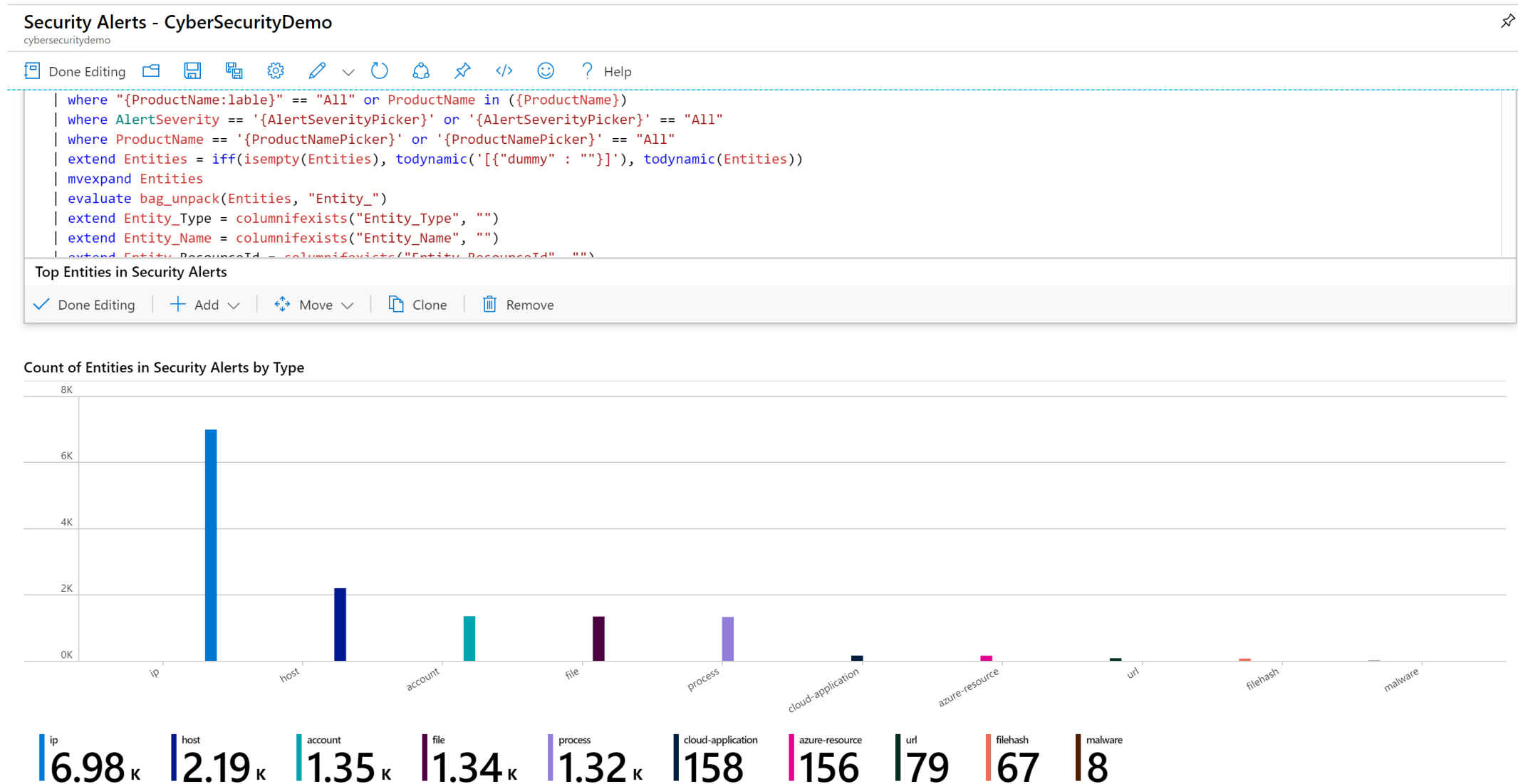
Top Entities in Security Alerts

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

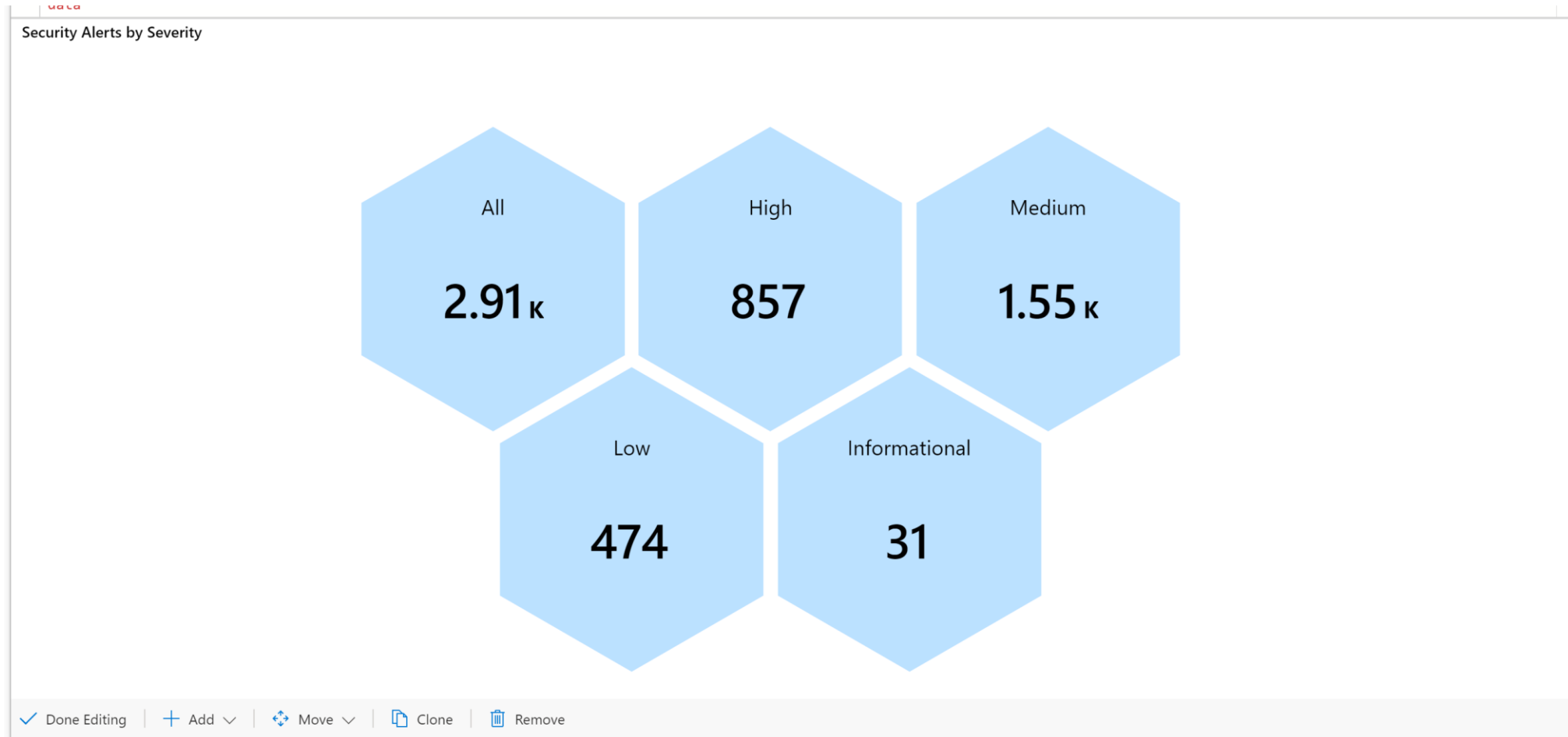
Custom Workbooks - Tiles



Custom Workbooks - Graphs

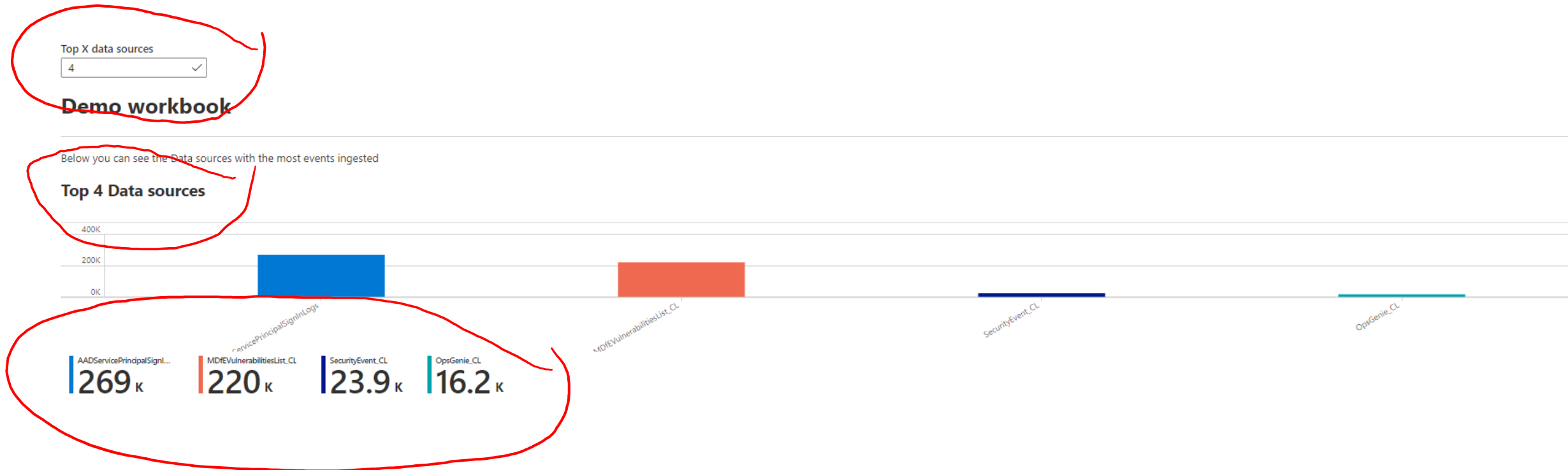


Custom Workbooks - Graph/Hives



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:

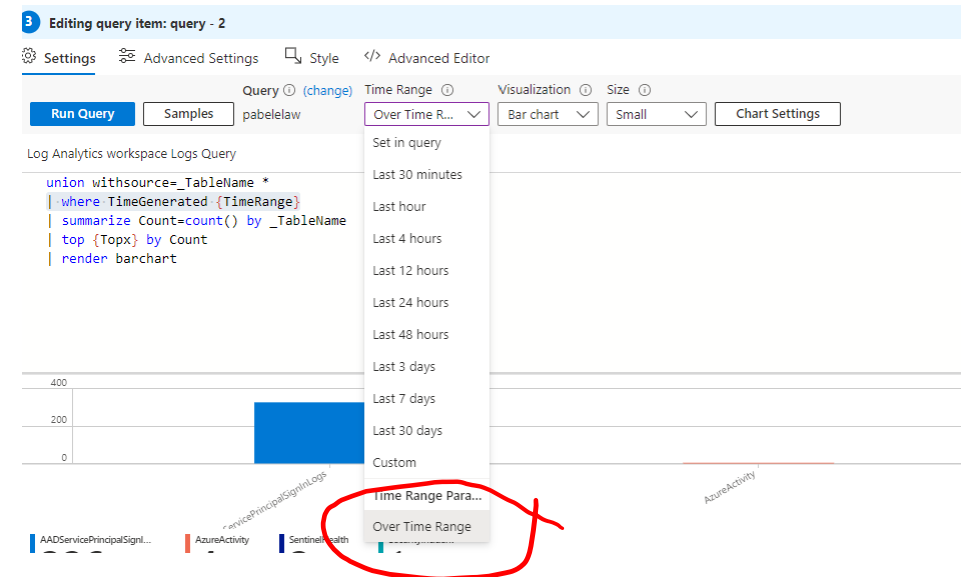
- Time - allows a user to select from prepopulated time ranges or select a custom range
- Drop down - allows a user to select from a value or set of values
- Text - allows a user to enter arbitrary text
- Resource - allows a user to select one or more Azure resources
- Subscription - allows a user to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

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?	<input checked="" type="checkbox"/>
Explanation	What is this parameter used for?
Hide parameter in reading mode	<input type="checkbox"/>
Get data from	None Query Criteria

Settings Advanced Settings

☒ Treat this parameter as a global

Add Validations

   		Match	Message
<input type="checkbox"/> Regular Expression			
<input type="checkbox"/> [0-9]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Only numbers are accepted!
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Custom Workbooks – Drop Down Parameter

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

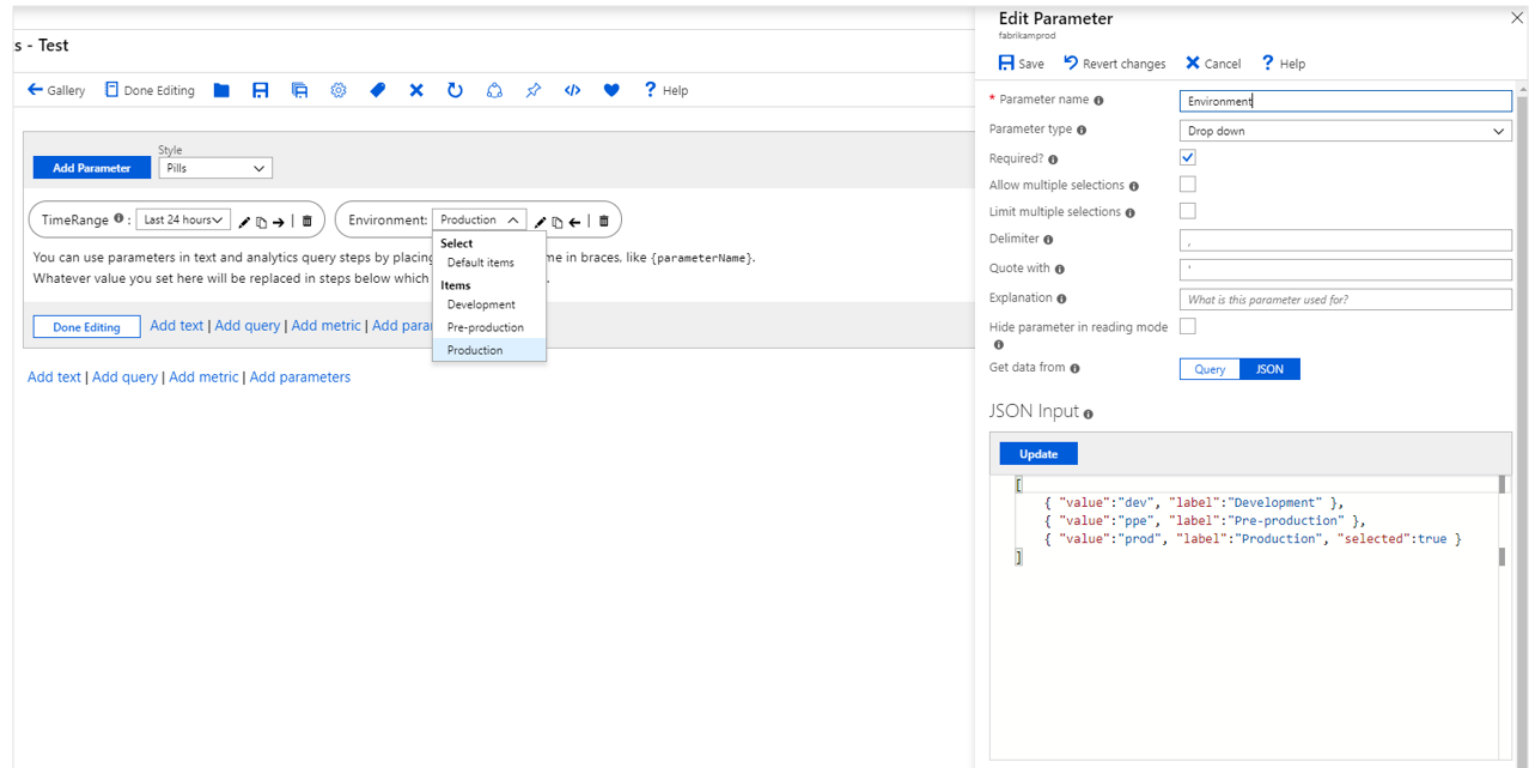
Provide a user-friendly way to collect arbitrary inputs from users.

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.).



Custom Workbooks – Drop Down Query Parameter

Home > Microsoft Sentinel > Microsoft Sentinel >

Demo workbook

pabelelaw

Done Editing Open Save Copy Settings Edit View Refresh Add Delete Code View Help

Settings Advanced Settings Style </> Advanced Editor

Group type Editable From Template Load type Lazy Edit Group

1 Editing parameters item: parameters - 0

Settings Advanced Settings Style </> Advanced Editor

Add Parameter Style Standard

Required?	Parameter name	Display name	Parameter type
<input type="checkbox"/>	TimeRange		Time range p
<input checked="" type="checkbox"/>	UPN	UserPrincipalName	Drop down t

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?	<input checked="" type="checkbox"/>
Allow multiple selections	<input type="checkbox"/>
Limit multiple selections	<input type="checkbox"/>
Delimiter	,
Quote with	'
Explanation	What is this parameter used for?
Hide parameter in reading mode	<input type="checkbox"/>
Get data from	Query JSON

Log Analytics workspace Logs Query

Run Query Query (change) Time Range Samples

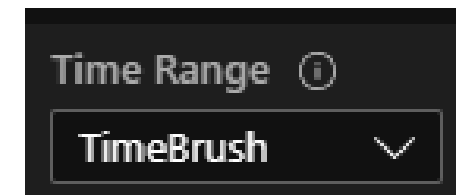
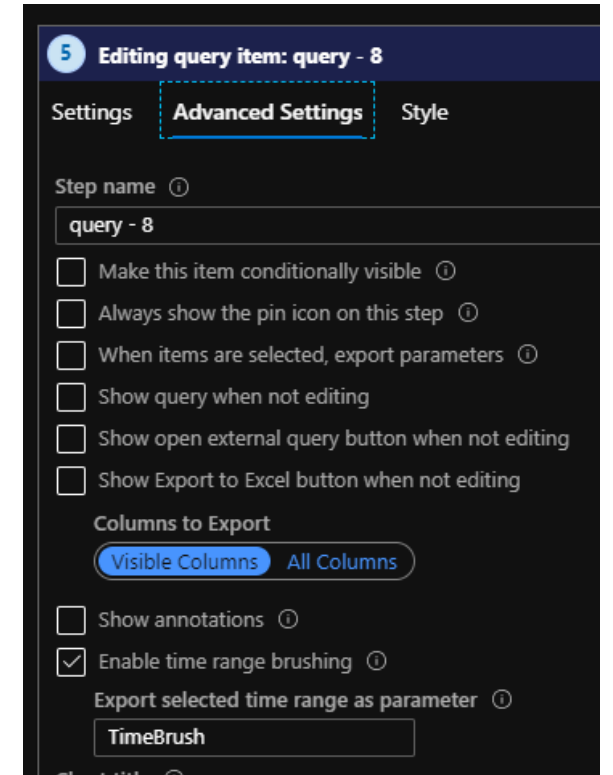
```
SignInLogs
| where TimeGenerated {TimeRange}
| summarize by UserPrincipalName
| order by UserPrincipalName asc
```

UserPrincipalName ↑↓

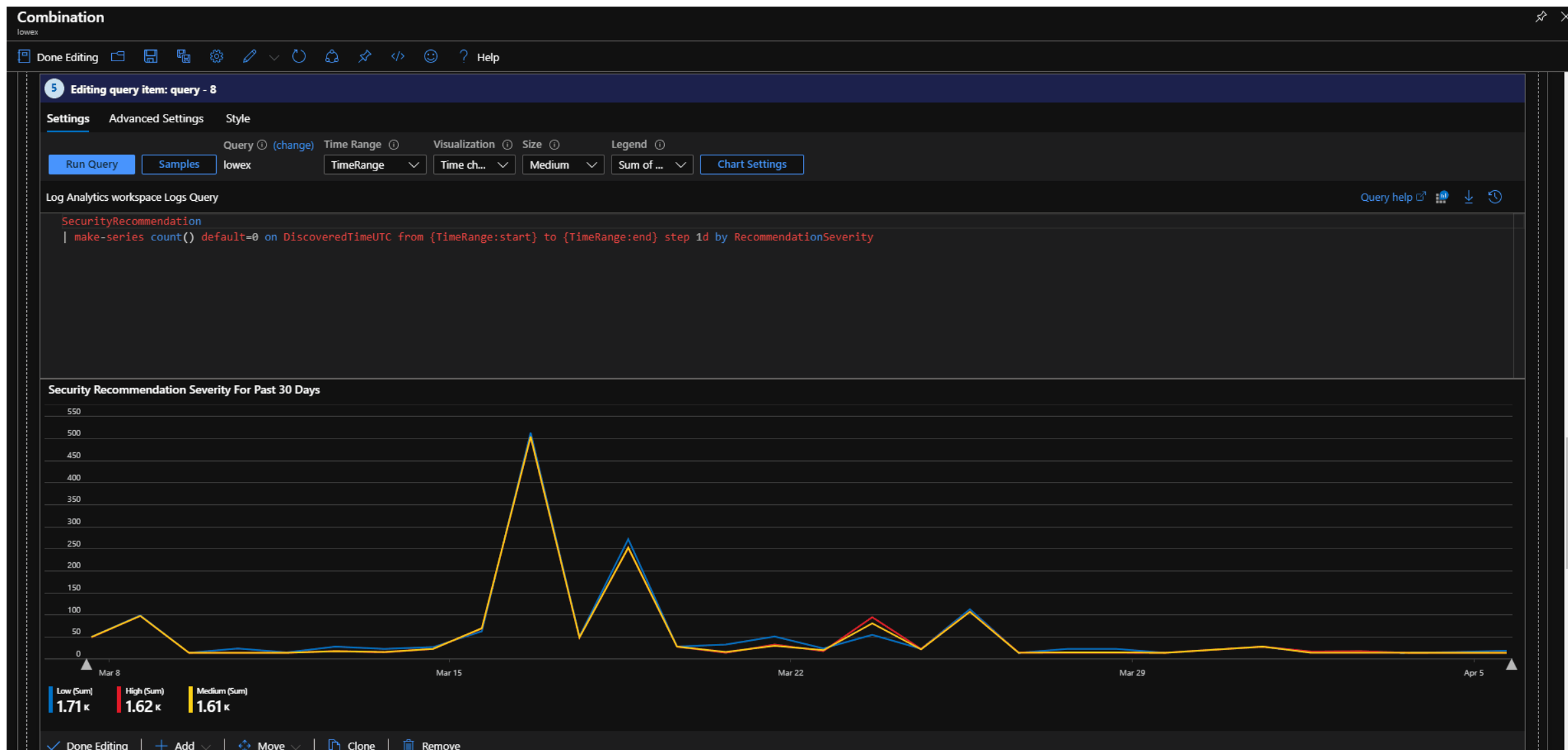
admin@m365x898158.onmicrosoft.com

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



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
<input checked="" type="checkbox"/> linuxsyslogtest	109
<input type="checkbox"/> Logstash	59
<input type="checkbox"/> linuxceflogs	47
<input type="checkbox"/> linuxceflogs	18
<input type="checkbox"/> winclient10	13
<input type="checkbox"/> ceftraining	9
<input type="checkbox"/> linuxsyslogtest	9
<input type="checkbox"/> az900test2	4
<input type="checkbox"/> logstash	4
<input type="checkbox"/> Logstash	2
<input type="checkbox"/> testing	2

↑ Edit

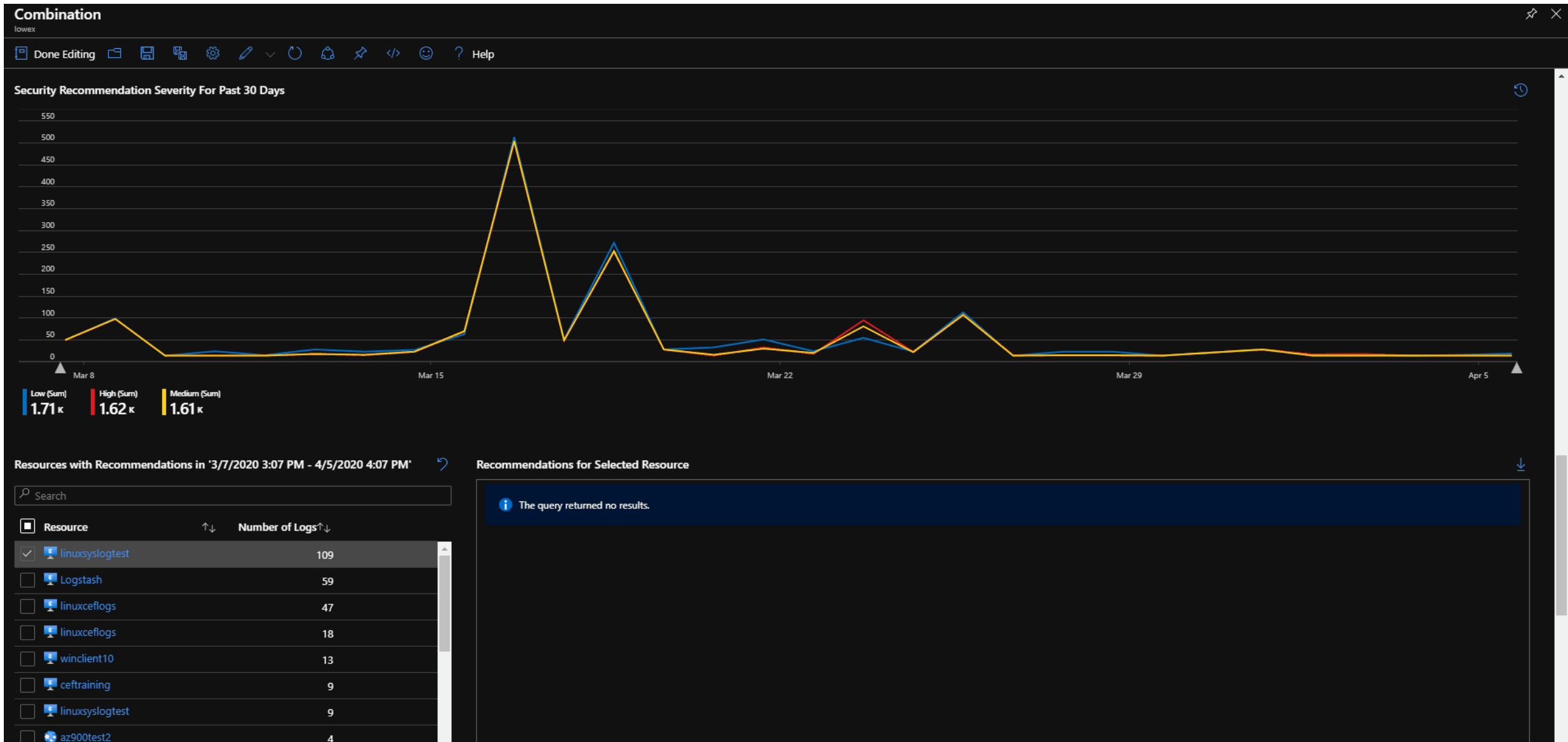
⋮

ⓘ The query returned no results.

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

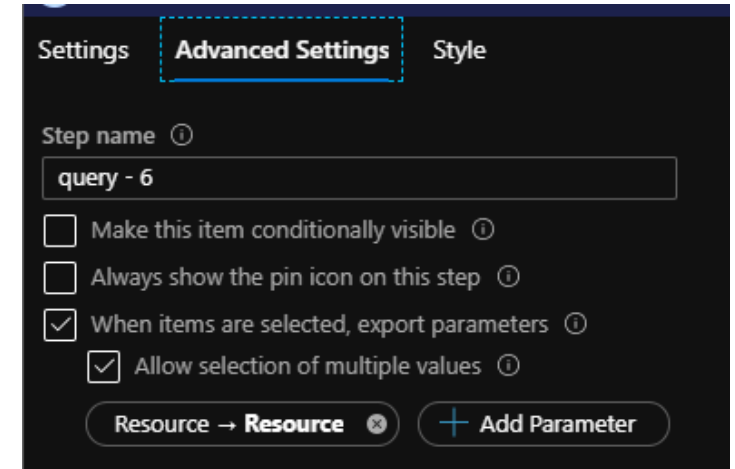
ⓘ The query returned no results.

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



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

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


Parameter Setup

Combination

lowex

Done Editing | [Icons]

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 Query help ⓘ [Icons]

```
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

<input type="checkbox"/> Resource	↑↓ Number of Logs↑↓
<input type="checkbox"/> linuxsyslogtest	109
<input type="checkbox"/> Logstash	59
<input type="checkbox"/> linuxceflogs	47
<input type="checkbox"/> linuxceflogs	18
<input type="checkbox"/> winclient10	13
<input type="checkbox"/> ceftraining	9
<input type="checkbox"/> linuxsyslogtest	9
<input type="checkbox"/> az900test2	4
<input type="checkbox"/> logstash	4
<input type="checkbox"/> mattleventhuhub	2
<input type="checkbox"/> {^} logstashexport	2

[Icons] Done Editing | + Add | Move | Clone | Remove

Calling the Parameter

Combination

lowex

Done Editing | [Icons] ? Help

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
wincient10	13
cefraining	9
linuxsyslogtest	9
az900test2	4
logstash	4
mattleventhub	2
{A} logstashexport	2

Recommendations for Selected Resource

Error message box about query parsing error.

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

Error message box about query parsing error.

Demo

Edit

Resources with Recommendations in '3/16/2020 3:27 PM - 4/14/2020 3:27 PM'

Search

Resource	Number of Logs
<input type="checkbox"/> LoginTest	6744
<input type="checkbox"/> CentOS01	6739
<input type="checkbox"/> ContosoVM1	3383
<input type="checkbox"/> cert-mng	3373
<input type="checkbox"/> Windows-16	3373
<input type="checkbox"/> Romeo-GoldenBox	3372
<input type="checkbox"/> FinanceSrv	3371
<input type="checkbox"/> mor-dns-test	3371
<input type="checkbox"/> DDoS	3370
<input type="checkbox"/> WIN01	3367
<input type="checkbox"/> 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 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

4 Editing query item: query - 2 - Copy

Settings Advanced Settings Style Advanced Editor

Run Query

Samples

Query (change)Time RangeTimeBrushVisualizationGridSizeSmallColumn 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 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

+ - ↑ ↓

<input type="checkbox"/> Operator	Value	Icons	Text
<input type="checkbox"/> !=	0	Error	{0}{1}
<input type="checkbox"/> ==	0	Success	{0}{1}
<input type="checkbox"/> 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.

SettingsAdvanced SettingsStyle

Style

Update Links

Tabs

<input type="checkbox"/> Tab Name ⓘ	Action ⓘ	Value ⓘ	Settings ⓘ
<input type="checkbox"/> Text, Grids, Tiles	Set a parameter value	Tab	Text
<input type="checkbox"/> Charts and Graphs	Set a parameter value	Tab	Charts
<input type="checkbox"/> PowerBI	Set a parameter value	Tab	PBI
<input type="checkbox"/> Time Brushing	Set a parameter value	Tab	TB

Text, Grids, Tiles

Charts and Graphs

PowerBI

Time Brushing

Dynamic Content

Personalization

✓ Done Editing

+ Add

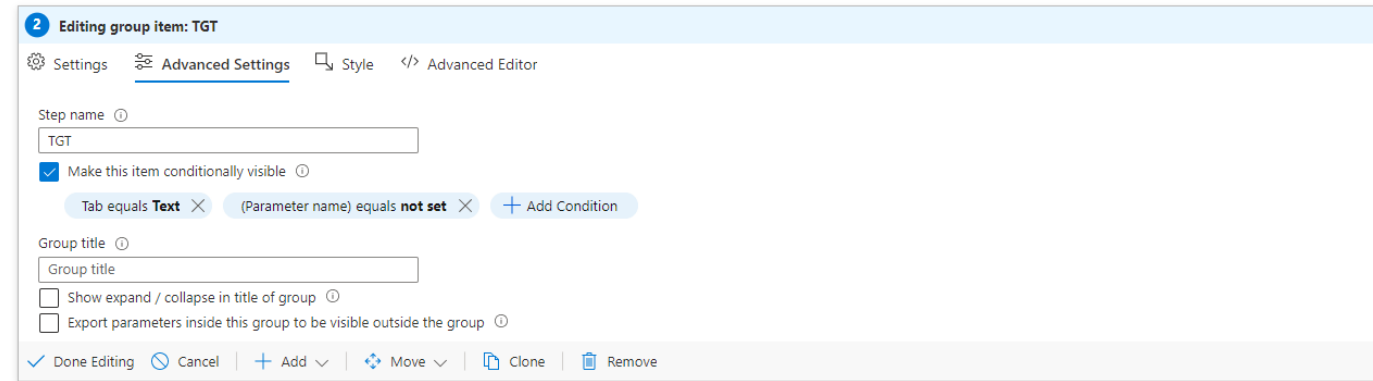
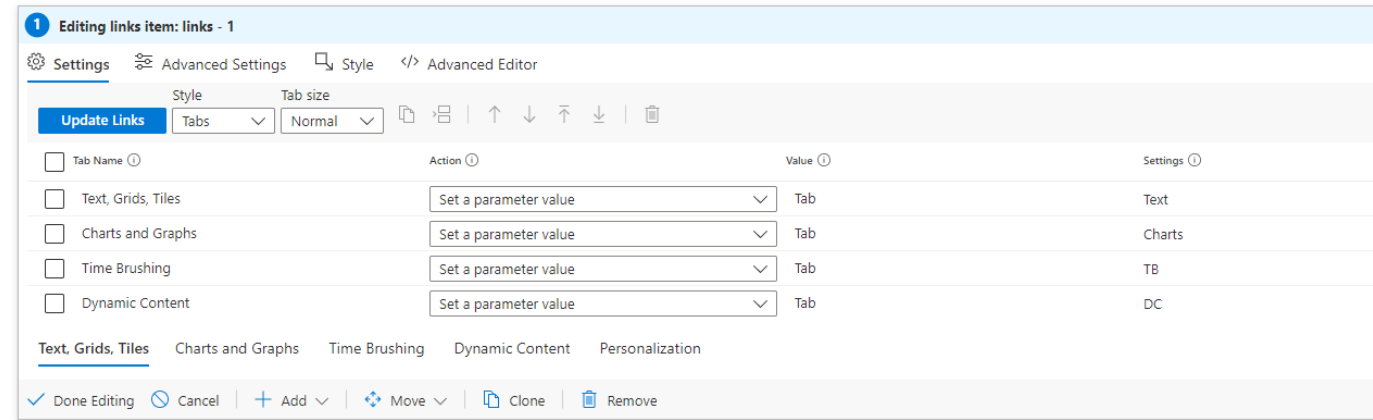
↻ Move

📄 Clone

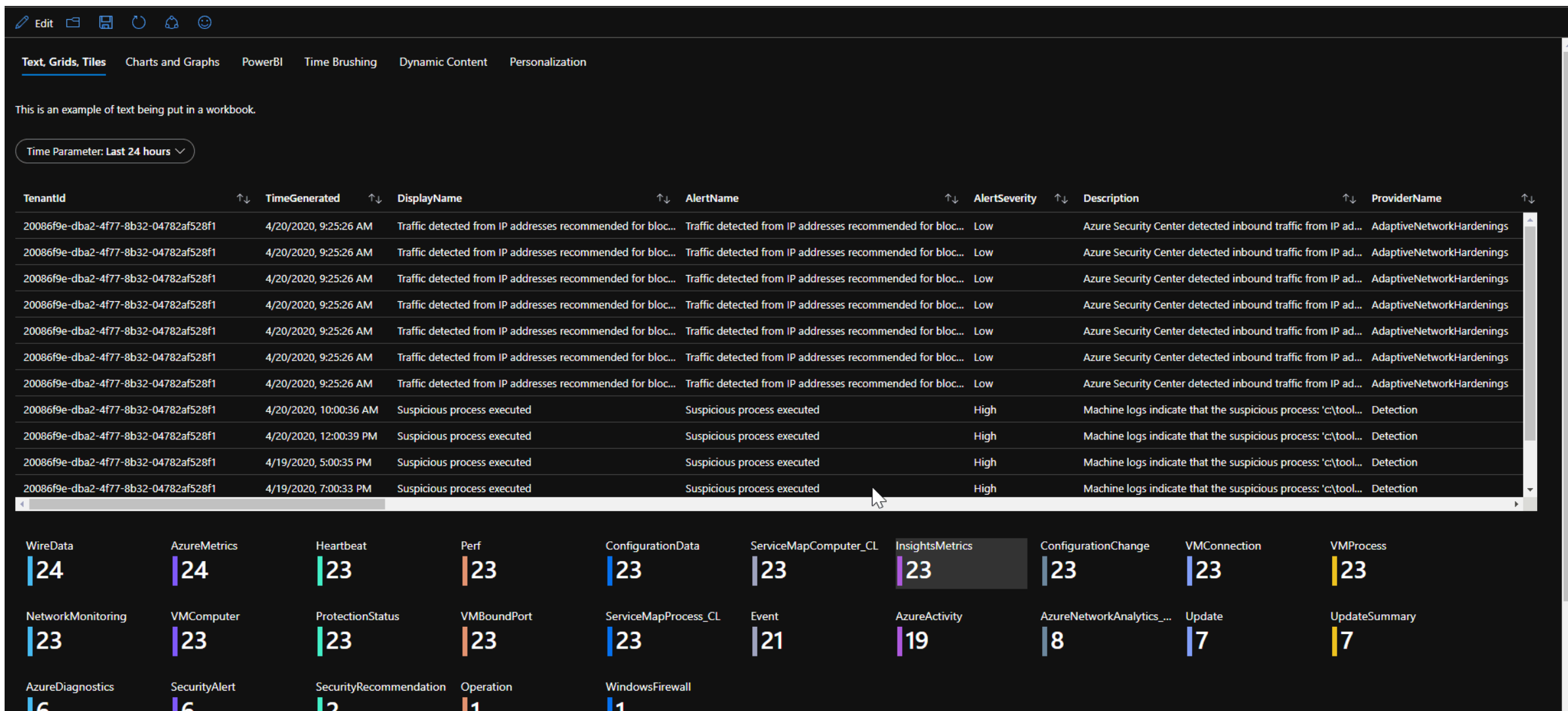
🗑 Remove

Custom Workbooks - Controlling tabs

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



Demo



Sharing workbooks

The screenshot shows the 'Share Report' sidebar in the Azure Sentinel console. The breadcrumb path is 'Home > Azure Sentinel | Workbooks > AWS Network Activities - CyberSecurityDemo'. The main content area displays the workbook title 'AWS Network Activities - CyberSecurityDemo' with a sub-label 'cybersecuritydemo'. Below this is a toolbar with icons for Edit, Save, Refresh, Share, and Feedback. The section title 'AWS network activities' is followed by a 'TimeRange: Last 14 days' dropdown menu and a note 'Top 10 active regions - click to filter'. The 'Share Report' sidebar on the right has a close button (X) and a title 'Share Report' with a subtitle 'AWS Network Activities - CyberSecurityDemo Workbooks report'. It contains a section 'Share a link to this report' with a note: 'Recipients need access to this Azure resource to view the data.' Below this is a 'Link to share' section with a text input field containing the URL 'https://go.microsoft.com/fwlink/?linkid=874159&res' and a copy icon. At the bottom of the sidebar is a link 'Share link via email'.

Home > Azure Sentinel | Workbooks > AWS Network Activities - CyberSecurityDemo

AWS Network Activities - CyberSecurityDemo
cybersecuritydemo

Edit Save Refresh Share Feedback

AWS network activities

TimeRange: Last 14 days ▾

Top 10 active regions - click to filter

Share Report X
'AWS Network Activities - CyberSecurityDemo' Workbooks report

Share a link to this report

Recipients need access to this Azure resource to view the data.

Link to share

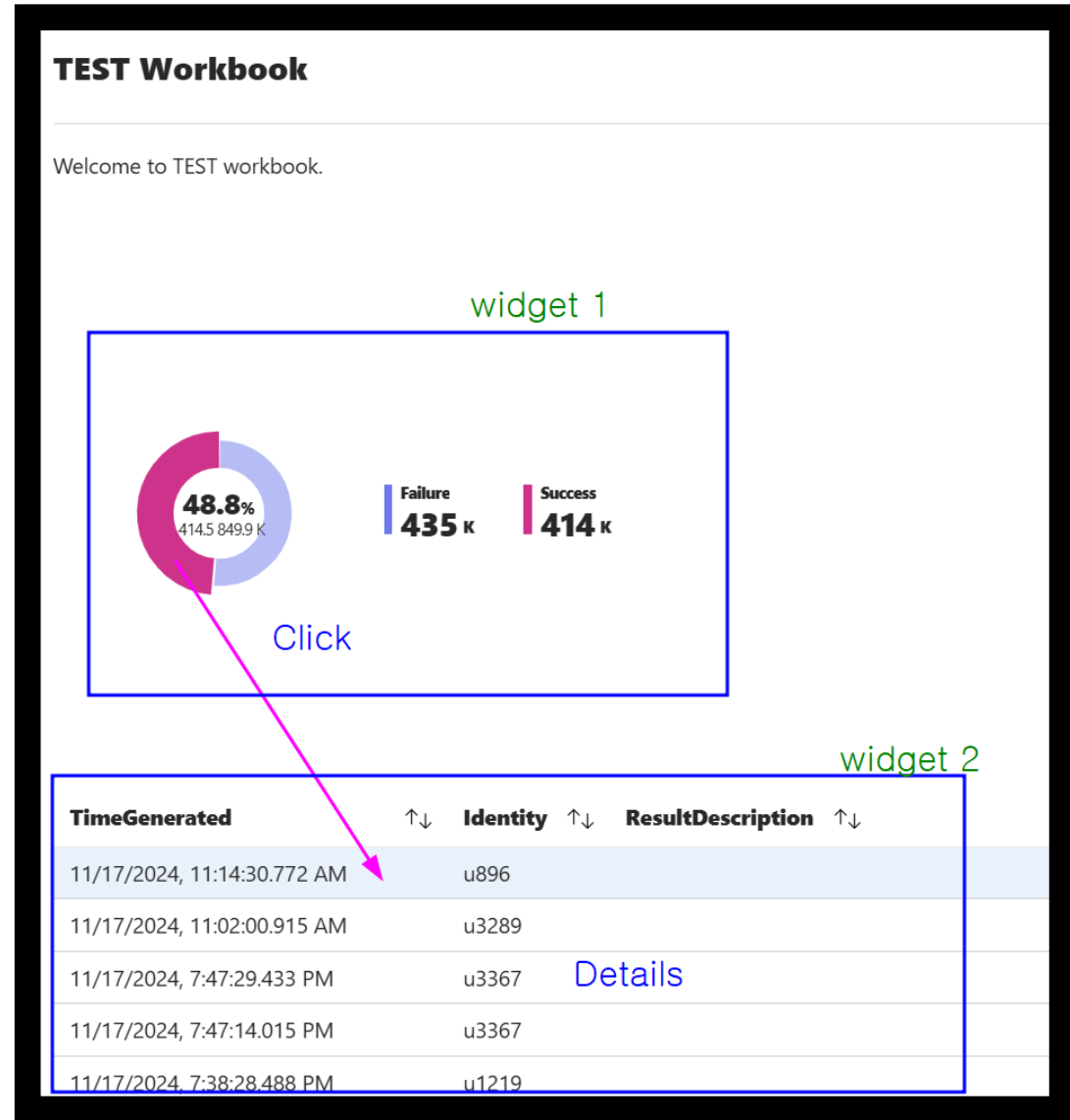
[Share link via email](#)

- 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 !



Microsoft Azure

Search resources, services, and docs (G+)

jaele@mngenvmcap103...
CONTOSO (MNGENVMCAP103...

Home > Log Analytics workspaces > sentinel-law

sentinel-law | Workbooks | Windows Event

Log Analytics workspace

Workbooks Done Editing

DefaultSubscription_Int... af9d3219-0de2-484a-9... Subscription ME-MngEnvMCAP103564-jaele-1 Workspace sentinel-law Time Range Last 60 days Show Help Yes No

1 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

count_ (Sum) 4.9 M

Aug 27 Sep 3 Sep 10

Event Filter

Device Filter

Account Filter

Log Filter

Error Filter

Select an event, device, or account to begin

Event Filter

Search

<input type="checkbox"/>	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

Search

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

Account Filter

Search

<input type="checkbox"/>	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

Search

<input type="checkbox"/>	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

Search

<input type="checkbox"/>	Description	↑↓	Count ↑↓
<input type="checkbox"/>	The handle to an object wa...		1,261,051
<input type="checkbox"/>	The Windows Filtering Platf...		972,285
<input type="checkbox"/>	The Windows Filtering Platf...		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 Platf...		254,260

Select an event, device, or account to begin