

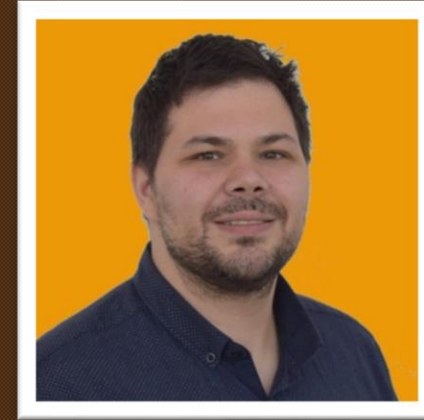
KQL Café | August 2024

Your | hosts

Alex Verboon



Gianni Castaldi



<https://twitter.com/alexverboon>

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

<https://github.com/alexverboon>

<https://www.verboon.info/>

https://twitter.com/castello_johnny

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

<https://github.com/KustoKing>

<https://www.kustoking.com/>



KQL | Cafe

Show | Agenda

Welcome

What is new/updates for KQL

Our guest: Truvis Thornton

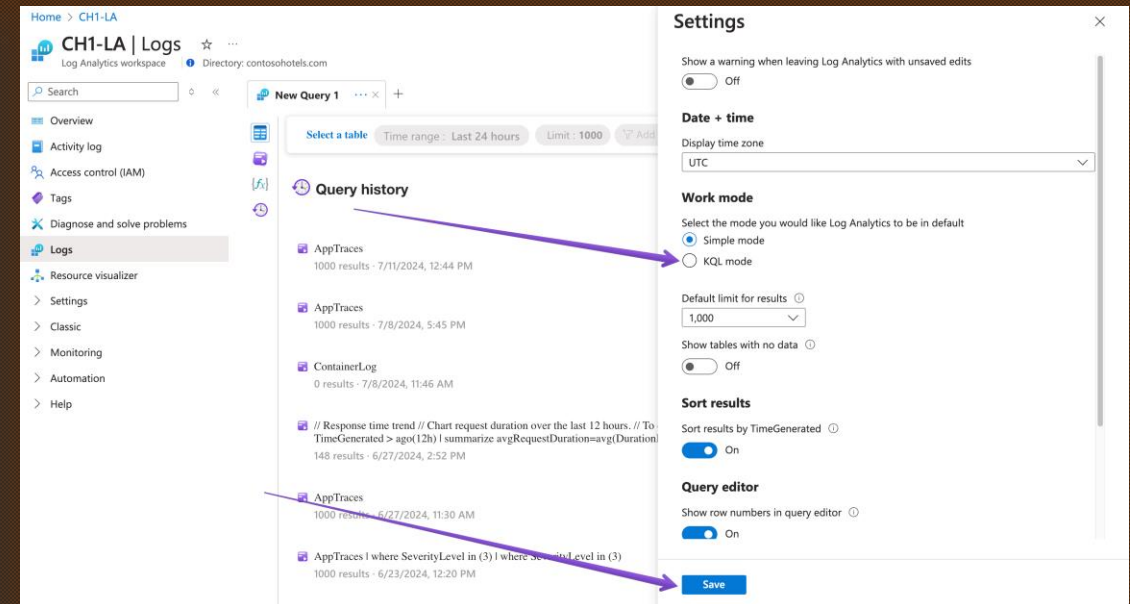
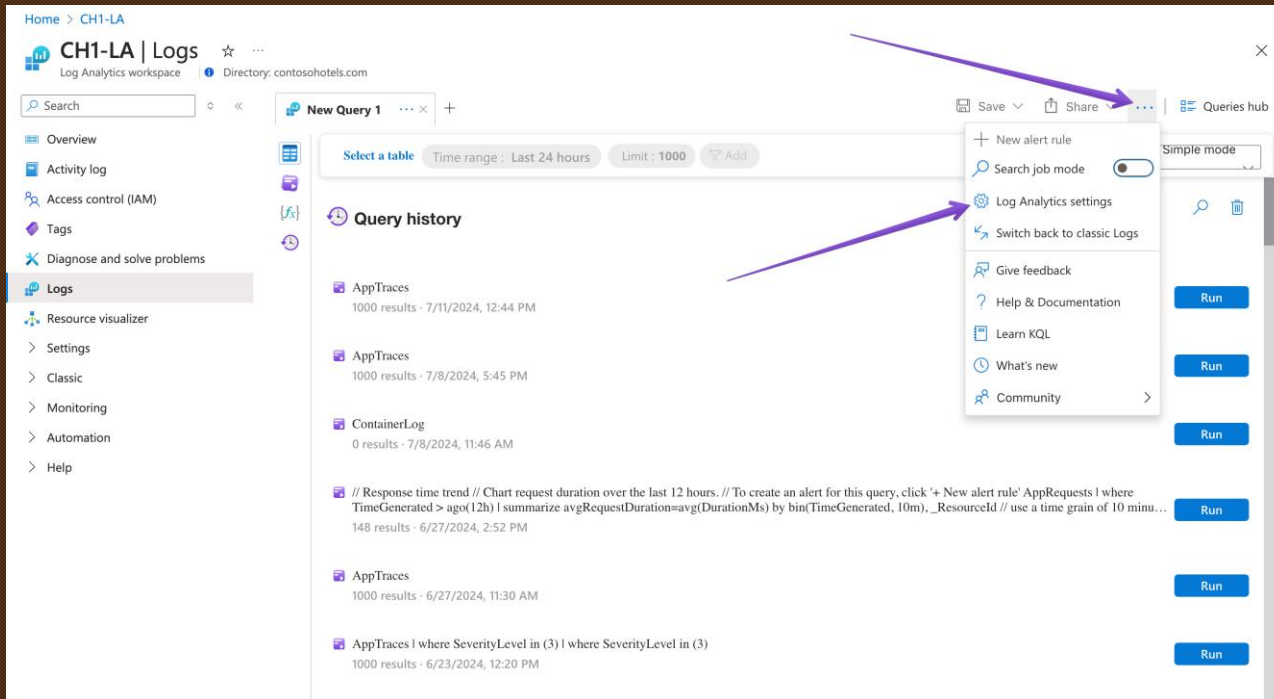
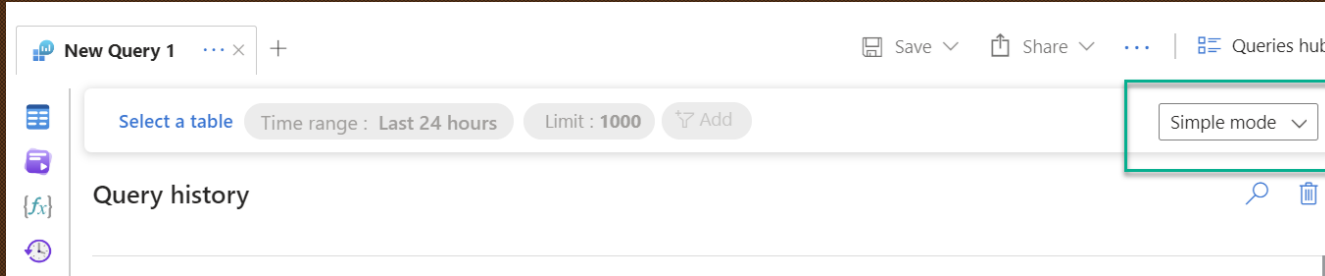
Learning KQL

What did you do with KQL this month?

News

Analyze data using Log Analytics Simple mode (Preview) - UPDATE

<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-simple-mode>



Detect compromised RDP sessions with Microsoft Defender for Endpoint

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/detect-compromised-rdp-sessions-with-microsoft-defender-for-ba-p/4201003>

- Additional properties (not yet synched to Sentinel)
- Potential additional data volume when storing in Sentinel

News

Hunting for Copilot Activities

CloudAppEvents

| where ActionType == @"CopilotInteraction"

<https://github.com/SlimKQL/Hunting-Queries-Detection-Rules/blob/main/DefenderXDR/Microsoft%20Defender%20Advanced%20Hunting%20Copilot%20Activities.kql>

News

Identify outdated devices through SignIn Logs

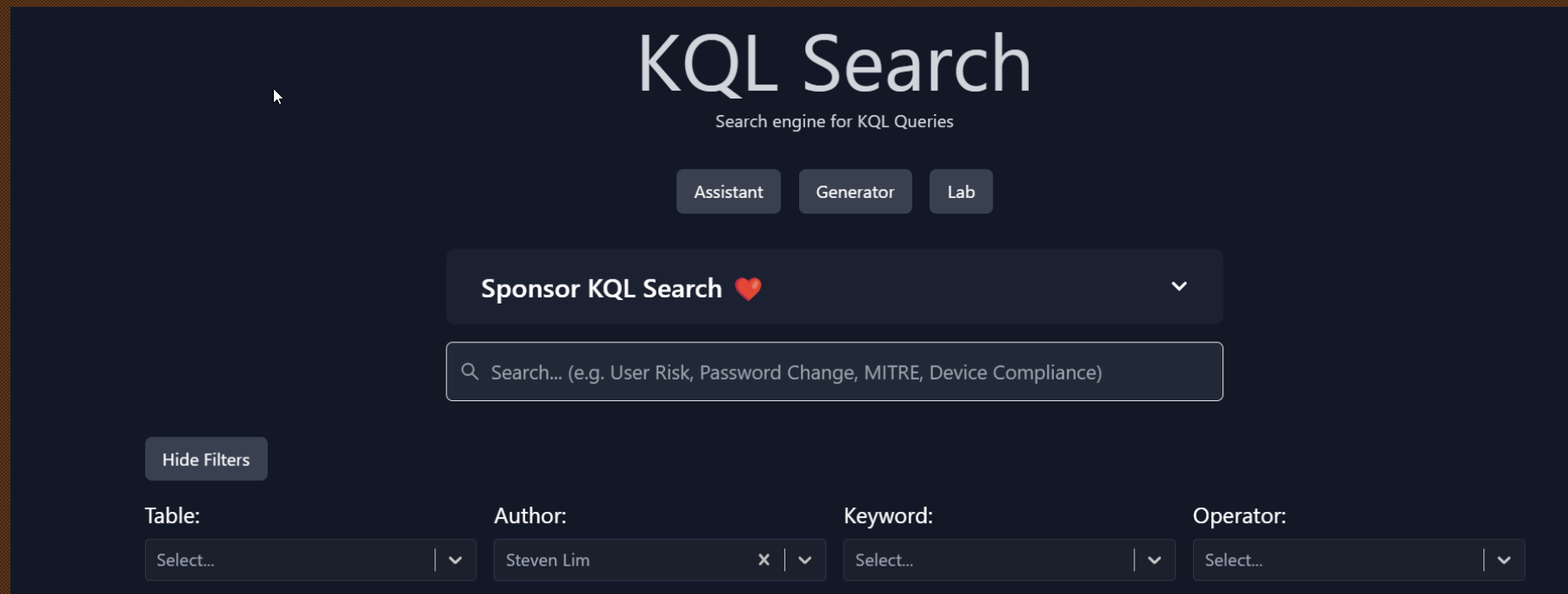
```
union isfuzzy=true SigninLogs, AADNonInteractiveUserSignInLogs | where  
ResultType != 0 and ResultDescription == "Other" | where ResultType ==  
"500061" | distinct Category, Identity
```

<https://techcommunity.microsoft.com/t5/microsoft-entra-blog/what-s-new-in-microsoft-entra-june-2024/ba-p/3796387>

News

Steven Lim's awesome KQL queries are now available on GitHub and KQLSearch.com

[SlimKQL/Hunting-Queries-Detection-Rules: KQL Queries. Microsoft Defender, Microsoft Sentinel \(github.com\)](https://github.com/SlimKQL/Hunting-Queries-Detection-Rules)



The screenshot shows the KQL Search web application interface. At the top, the title "KQL Search" is displayed in a large, white font, with the subtitle "Search engine for KQL Queries" below it. Below the subtitle are three buttons: "Assistant", "Generator", and "Lab". A dark blue button labeled "Sponsor KQL Search" with a red heart icon and a dropdown arrow is positioned below these buttons. A search bar with a magnifying glass icon and placeholder text "Search... (e.g. User Risk, Password Change, MITRE, Device Compliance)" is located below the sponsor button. On the left side, there is a "Hide Filters" button. At the bottom, there are four filter sections: "Table:" with a dropdown menu showing "Select...", "Author:" with a text input containing "Steven Lim" and a close button, "Keyword:" with a dropdown menu showing "Select...", and "Operator:" with a dropdown menu showing "Select...".

KQL Search

Search engine for KQL Queries

Assistant Generator Lab

Sponsor KQL Search ❤️

Search... (e.g. User Risk, Password Change, MITRE, Device Compliance)

Hide Filters

Table: Author: Keyword: Operator:

Select... Steven Lim Select... Select...

News – Summary Rules

A summary rule lets you aggregate log data at a regular cadence and send the aggregated results to a custom log table in your Log Analytics workspace.

Scenarios

Analysis and reports, especially over large data sets and time ranges, as required for security and incident analysis, month-over-month or annual business reports, and so on. Complex queries on a large data set often time out. It's easier and more efficient to analyze and report on cleaned and aggregated summarized data.

Cost savings on verbose logs, which you can retain for as little or as long as you need in a cheap Basic log table, and send summarized data to an Analytics table for analysis and reports.

Security and data privacy by removing or obfuscating privacy details in summarized shareable data and limiting access to tables with raw data.

Aggregate data in a Log Analytics workspace by using summary rules (Preview)

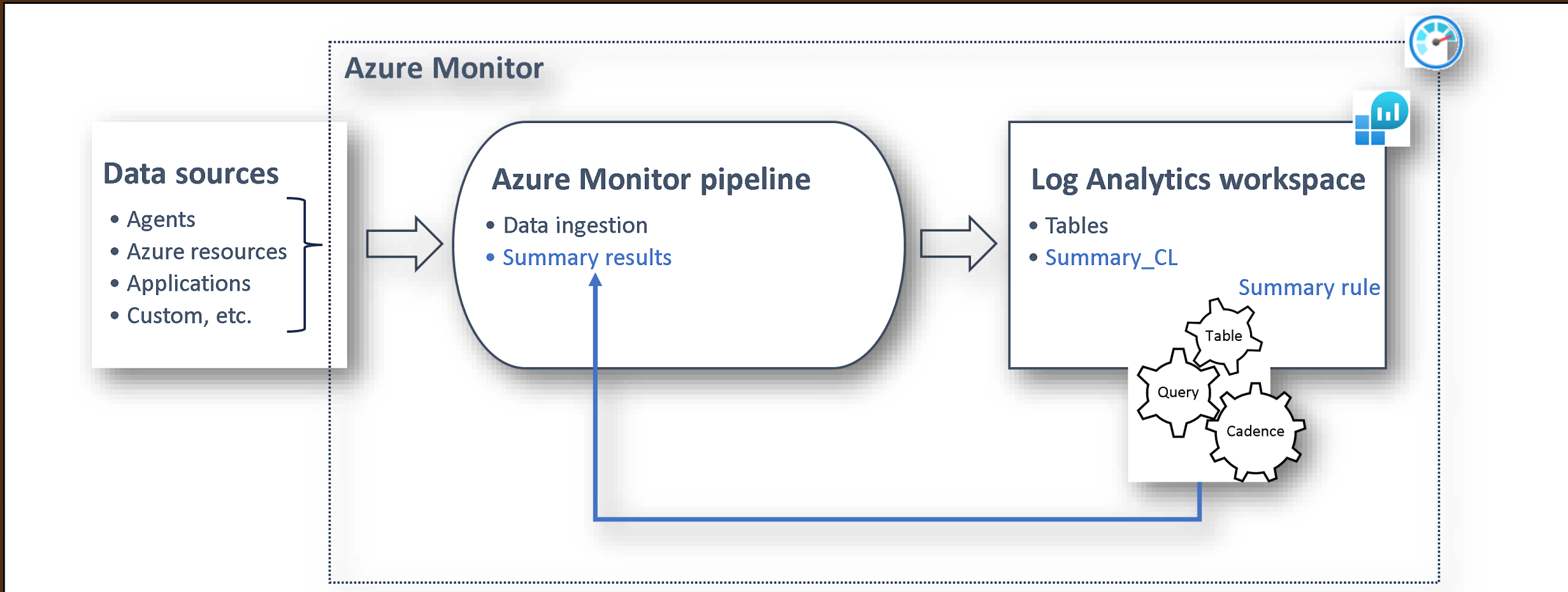
<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/summary-rules?tabs=api>

Aggregate Microsoft Sentinel data with summary rules (preview)

<https://learn.microsoft.com/en-us/azure/sentinel/summary-rules>

News – Summary Rules

Summary rules perform batch processing directly in your Log Analytics workspace. The summary rule aggregates chunks of data, defined by bin size, based on a KQL query, and reingests the summarized results into a custom table with an Analytics log plan in your Log Analytics workspace.



News – Summary Rules

For our KPI Reporting we need to the total Number of devices broken down by their Exposure Level. This is the query we would run manually.

```
1 DeviceInfo
2 | where TimeGenerated > ago(1d)
3 | where OnboardingStatus == 'Onboarded'
4 | summarize arg_max(TimeGenerated, *) by DeviceId
5 | summarize
6     Low = dcountif(DeviceId, ExposureLevel == 'Low'),
7     Medium = dcountif(DeviceId, ExposureLevel == 'Medium'),
8     High = dcountif(DeviceId, ExposureLevel == 'High'),
9     None = dcountif(DeviceId, ExposureLevel == 'None')
10 | extend Time = now()
```

ResultsChart

Add bookmark

<input type="checkbox"/> Low	Medium	High	None	Time [UTC] ↑↓
<input type="checkbox"/> > 11	893	1482	4	8/15/2024, 5:24:28.085 PM

News – Summary Rules

We create a Summary rule to run the query daily and save the results into a custom table.

Summary rule wizard

General

Set summary logic

Review + create

Create a summary rule to persist the results of scheduled query jobs.

Summary rule details

Name *

DeviceExposureLevel

Description

Summary of device

Destination table *

Existing custom

Summary_DeviceE

Diagnostic settings

In order to access the full summary rules experience, select Enable

Enabled

Configure advanced diagnostic settings

Home > Microsoft Sentinel | Summary rules (Preview)

Summary rule wizard

General

Set summary logic

Review + create

Summary query *

1 DeviceInfo

2 | where TimeGenerated > ago(1d)

3 | where OnboardingStatus == 'Onboarded'

4 | summarize arg_max(TimeGenerated, *) by DeviceId

5 | summarize

6 | Low = dcountif(DeviceId, ExposureLevel == 'Low'),

Query Scheduling

Starting automatically, the summary rule will run every 24 hours. To account for ingestion latency, each summary run will be delayed by 4 minutes.

Run summary every *

24 hours

Delay in minutes *

4

Start running *

Automatically

At specific time (UTC)

Results simulation

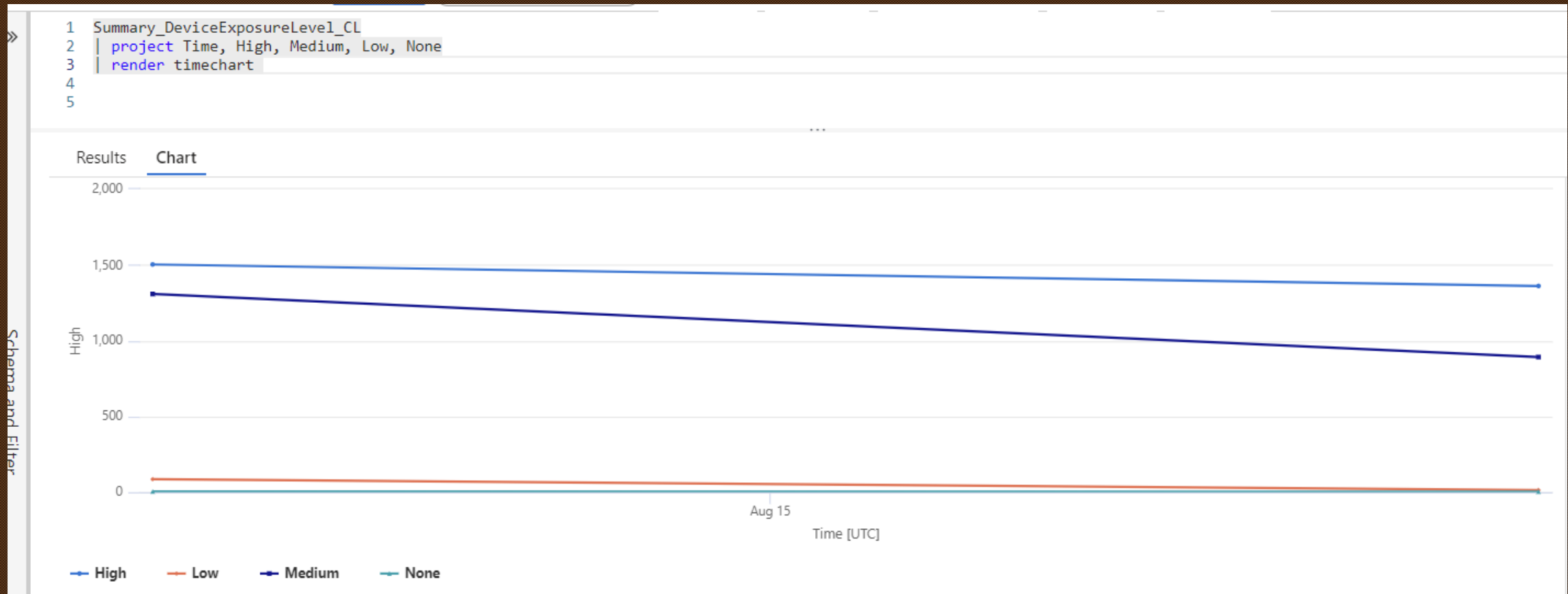
This chart shows the results of the last 50 evaluations and first 5 columns of the defined summary query.

Preview results

Low	Medium	High	None	Time
11	892	1483	4	2024-08-15T17...

News – Summary Rules

We can now easily access our KPI data , without the need for complex and time intensive KQL queries.



What did you do with KQL this month?

- OneDrive and Sharepoint downloads over API

Thanks for attending



KQL | Cafe