

KQL Café | June 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: Nicola Suter

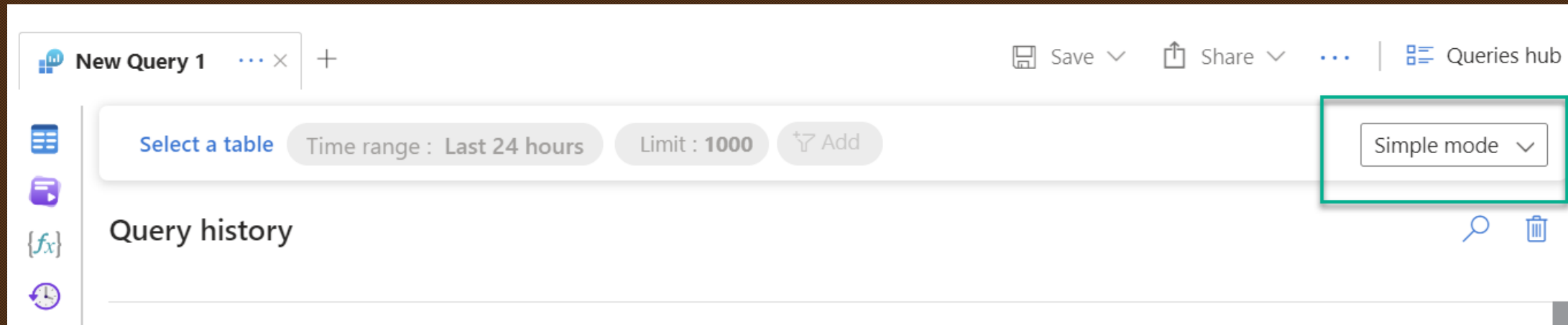
Learning KQL

What did you do with KQL this month?

News

Analyze data using Log Analytics Simple mode (Preview)

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



News

Definitive Guide to KQL Book - Microsoft Employee Submitted Queries

<https://github.com/KQLMSPress/definitive-guide-kql/tree/main/Extra%20Microsoft%20Employee%20Submitted%20Queries>

Monitoring Cosmos DB's request unit consumption.
Identifying top N queries by consumption in Cosmos DB.
Checking for requests that are throttled in Cosmos DB.
Checking for antivirus exclusions.
Identifying applications using auto proxy (WPAD).
Detecting changes to evade detection.
Analyzing Microsoft Graph API usage patterns.
Analyzing traffic patterns to Microsoft Graph APIs.
Monitoring ID Governance in Microsoft Entra for usage patterns.
Visualizing authentication method use over time.
Understanding administrative activities.
Monitoring short-lived connections in PostgreSQL.
Monitoring failed login attempts in PostgreSQL.
Resource utilization monitoring in PostgreSQL.
Summarizing sign-ins via iOS and macOS SSO Extensions.
Searching for MFA phone number changes using regex.
Tracking dynamic group membership changes.

Session breakdown by legacy vs modern TLS.
Understanding email authentication patterns for security.
Monitoring token protection impact and managing conditional access.
Analyzing Intune device management events and enrollments.
Monitoring failed operations and sign-in events.
Network traffic monitoring.
Identity governance operations.
Detecting suspicious activities and anomalies.
Identifying vulnerabilities and attack surfaces via IP range and CVE ID tracking.
Detecting administrative actions and user re-enabling.
High-risk sign-in patterns detection.
Reporting on antimalware versions.
Detecting email anomalies.
Performance troubleshooting for SQL servers.
Monitoring conditional access policy applications and failures.

News

Definitive Guide to KQL Book - Microsoft Employee Submitted Queries

<https://github.com/KQLMSPress/definitive-guide-kql/tree/main/Extra%20Microsoft%20Employee%20Submitted%20Queries>

Estefani Arroyo

Michael Barbush

Kristopher Bash

Bailey Bercik

Keith Brewer

Chad Cox

Varun Dhawan

Michael Epping

Marius Folling

Cosmin Guilman

Tim Haintz

Franck Heilmann

Mark Hopper

Laura Hutchcroft

Jef Kazimer

Corissa Koopmans

Gloria Lee

Michael Lindsey

Rudnei Oliveira

Razi Rais

Yong Rhee

Sravani Salura

Krishna Venkit

Thank
you!

News

Microsoft Defender for Endpoint Advanced Hunting and Application Control for Business – WDACConfig

<https://www.youtube.com/watch?app=desktop&si=tJbFbzRJNy79lUo7&v=oyz0jFzOOGA&feature=youtu.be>

<https://github.com/HotCakeX/Harden-Windows-Security>

[How to Use Microsoft Defender for Endpoint Advanced Hunting With WDAC App Control - SpyNetGirl Blog](#)

News

Audit Defender XDR Activities

<https://kqlquery.com/posts/audit-defender-xdr/>

The screenshot displays the Microsoft Sentinel interface. On the left is a navigation pane with categories like Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, SOC optimization, Reports, Learning hub, Trials, More resources, System, Audit, Permissions, Health, and Settings. The main area is titled 'Endpoints' and contains a 'General' section with 'Advanced features' (Licenses, Email notifications, Auto remediation), 'Permissions' (Roles, Device groups), 'APIs' (SIEM), and 'Rules' (Alert suppression, Deception rules, Indicators). A 'Unified audit log' section is also visible with a toggle set to 'On'. Overlaid on this is a KQL query window. The query is:

```
1 CloudAppEvents
2 | extend WorkLoad = tostring(parse_json(RawEventData).Workload)
3 | where WorkLoad contains "Defender"
4 | distinct WorkLoad
5
```

 The window shows 'Run query' and 'Last 30 days' options. Below the query, there are tabs for 'Getting started', 'Results', and 'Query history'. The 'Results' tab shows 3 items with a search bar and a 'Filters' section containing 'WorkLoad', 'Microsoft365Defender', 'MicrosoftDefenderForEndpoint', and 'MicrosoftDefenderForIdentity'.

Microsoft Sentinel

Endpoints

General

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups

APIs

SIEM

Rules

Alert suppression

Deception rules

Indicators

Unified audit log

On

Block access to websites containing unwanted content and track web activity across all domains. To specify the web content categories you want to block, create a [web content filtering policy](#). Ensure you have network protection in block mode when deploying the [Microsoft Defender for Endpoint security baseline](#).

When an audited activity is performed by a user or admin, an audit record is generated and stored in the Office 365 audit log for your organization. For more information, see the [Search the audit log in the Security & Compliance Center](#).

Device discovery

On

Allows unhardened devices to discover unmanaged devices in your network and access vulnerabilities and risks. For more information, see [Device discovery](#).

Run query

Last 30 days

Save

Share link

Manage rules

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

Don't want to see it again

```
1 CloudAppEvents
2 | extend WorkLoad = tostring(parse_json(RawEventData).Workload)
3 | where WorkLoad contains "Defender"
4 | distinct WorkLoad
5
```

Getting started

Results

Query history

Export

3 items

Search

00:00.361

Low

Chart type

Customize columns

Filters:

Add filter

WorkLoad

Microsoft365Defender

MicrosoftDefenderForEndpoint

MicrosoftDefenderForIdentity

News

Detect suspicious processes running on hidden desktops

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/detect-suspicious-processes-running-on-hidden-desktops/ba-p/4072322>

Our Guest: Michalis Michalos

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



What did you do with KQL this month?

- Automation Account Runbook logs

```
AzureDiagnostics
| where Category == 'JobLogs'
| extend RunbookName = RunbookName_s
| project TimeGenerated,RunbookName,ResultType,CorrelationId,JobId_g
| summarize StartTime = minif(TimeGenerated,ResultType == 'Started'),EndTime =
minif(TimeGenerated,ResultType in ('Completed','Failed','Failed')),
Status = tostring(parse_json(make_list_if(ResultType,ResultType in ('Completed','Failed','Stopped')))[0])
by JobId_g,RunbookName
| extend DurationSec = datetime_diff('second', EndTime,StartTime)
| join kind=leftouter (AzureDiagnostics
| where Category == "JobStreams"
| where StreamType_s == "Error"
| summarize TotalErrors = dcount(StreamType_s) by JobId_g, StreamType_s)
on $left.JobId_g == $right.JobId_g
| extend HasErrors = iff(StreamType_s == 'Error',true,false)
| project StartTime, EndTime, DurationSec,RunbookName,Status,HasErrors,TotalErrors,JobId_g
```

▶ Run

Time range : Custom

Limit : 1000

```
1 AzureDiagnostics
2 | where Category == 'JobLogs'
3 | extend RunbookName = RunbookName_s
4 | project TimeGenerated,RunbookName,ResultType,CorrelationId,JobId_g
5 | summarize StartTime = minif(TimeGenerated,ResultType == 'Started'),EndTime = minif(TimeGenerated,ResultType in ('Completed','Failed','Failed')),
6 Status = tostring(parse_json(make_list_if(ResultType,ResultType in ('Completed','Failed','Stopped')))[0]) by JobId_g,RunbookName
7 | extend DurationSec = datetime_diff('second', EndTime,StartTime)
```

What did you do with KQL this month?

- JA3

What did you do with KQL this month?

- | where InternetFacingReason == "ExternalNetworkConnection"

<https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Endpoint/MDE-InternetFacing.md>

Thanks for attending



KQL | Cafe