

KQL Café | February 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://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: Fabian Bader

Learning KQL

What did you do with KQL this month?

# Learn KQL in one month book



Damien Van Robaey

[https://twitter.com/syst\\_and\\_deploy](https://twitter.com/syst_and_deploy)

<https://www.systanddeploy.com/2024/02/learn-kql-in-one-month-book.html>

LEARN KQL IN ONE MONTH

 DAY 9

## Exercises of the day

### Intune environment

1. Display records where free disk percent is lesser than 20%
2. Display records count
3. Display devices count where free disk percent is lesser than or equals to 5%
4. Display devices count where free disk percent is between 20% and 50%
5. Create different column as below:
  - Less 5%
  - Between 5% and 20%
  - Between 20% and 50%
  - Above 60%: percent > 60%

### Demo lab environment

1. In the SecurityEvent log, filter on column EventID equals to 4624
2. Count the number of records
3. Create different columns as below:
  - Logon failed: eventid equals 4625
  - Logoff failed: eventid equals 4634
  - Logon success: eventid equals 4624

## Key words

- summarize
- count, countif

# Device Query in Intune

## Intune Queries

This repository contains a wide array of KQL Queries ready for you to easily copy, paste, and execute within Intune.

<https://github.com/ugurkocde/IntuneDeviceQuery> or [www.kqlsearch.com](http://www.kqlsearch.com)

Thanks Ugur Koc |

The screenshot shows the Intune console interface for a device named 'DESKTOP-3JA010E'. The left sidebar contains a 'Manage' section with various categories. A green arrow labeled '1.' points to the 'Device query' option at the bottom of the sidebar. The main area shows a 'Device query' box with a 'Run' button. A yellow arrow labeled '2.' points to the 'Run' button. A blue arrow labeled '3.' points to the KQL query text inside the box. A yellow box on the right contains the following instructions:

1. Select "Device Query"
2. Paste your Query inside the box.
3. Click on "Run"
4. Check the Results

Below the query box, the 'Results' tab is active, showing a table of processes. A purple arrow labeled '4.' points to the results table.

ProcessName	StartDateTime	ElapsedTimeInMin...	ElapsedTimeMilliseconds
System Idle Process	2024-02-03T13:02...	503	30219773
System	2024-02-03T13:02...	503	30219803
Secure System	2024-02-03T13:02...	503	30221062
Registry	2024-02-03T13:02...	503	30221013
smss.exe	2024-02-03T13:02...	503	30219876
csrss.exe	2024-02-03T13:02...	503	30217797
wininit.exe	2024-02-03T13:02...	503	30217767
csrss.exe	2024-02-03T13:02...	503	30217784
winlogon.exe	2024-02-03T13:02...	503	30217778
services.exe	2024-02-03T13:02...	503	30217780
lsass.exe	2024-02-03T13:02...	503	30217751

<https://learn.microsoft.com/en-us/mem/analytics/device-query>


# Notable Articles & Queries

## Function: ListAllActionsAndOperations()

<https://github.com/Bert-JanP/Hunting-Queries-Detection-Rules/blob/main/Functions/ListAllActionsAndOperations.md>

If you want to get quick insight into all the ActionTypes, Operations and OperationNames in your Sentinel environment, the function below can be used. This function summarizes all different actions in different tables in a single view, which is optimal when you want to quickly know if some activities can be seen/detected in your environment.

Note: This query only works in Sentinel and NOT in 365 Defender.

```
// List all ActionTypes, Operations and OperationNames in a single view. This can be used to get insight into the activities that are detected in your environment.   
let ListAllActionsAndOperations = () {  
    union *  
    | extend Action = iff(isnotempty(ActionType), ActionType, iff(isnotempty(Operation), Operation, iff(isnotempty(OperationName), OperationName, 'Null'))),  
    | where Action != 'Null'  
    | distinct Action, Type  
};  
// Example  
ListAllActionsAndOperations
```

# Device Containment Notification

<https://www.michalos.net/2024/02/20/contained-an-endpoint-automate-tag-adding-and-notifications/>

<https://github.com/cyb3rmik3/KQL-threat-hunting-queries/blob/main/03.SecOps/identify-contained-endpoints.md>

```
DeviceRegistryEvents
| where ActionType == "RegistryValueSet"
| where RegistryKey ==
@"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Advanced Threat
Protection"
| where RegistryValueType == "Dword"
| where RegistryValueName ==
"DisableEnterpriseAuthProxyValueToRestoreAfterIsolation"
| where RegistryValueData == "1"
| where PreviousRegistryValueName ==
"DisableEnterpriseAuthProxyValueToRestoreAfterIsolation"
| project Timestamp, DeviceId, DeviceName
```



# Update Records in ADX

<https://azure.microsoft.com/en-us/updates/update-kusto-db/>

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide#contain-devices-from-the-network>

Our Guest:



Fabian Bader

Cyber Security Architect @ glueckkanja | Microsoft MVP

# Learning KQL

## Next and previous values

```
SigninLogs
| where TimeGenerated > ago(7d)
| where UserPrincipalName =~ "gianni@kustoking.com"
| project TimeGenerated, ResultType, ResultDescription, UserPrincipalName
| sort by TimeGenerated desc
| extend PreviousResult = prev(ResultType)
```

# What did you do with KQL this month?

Monitoring Windows built-in local security Groups with Microsoft Defender XDR or Sentinel

```
8 let SensitiveBuiltInGroups = datatable(GroupsSID: string,BuildInGroupName: string)
9 [
0     "S-1-5-32-544","Administrators",
1     "S-1-5-32-546","Guests",
2     "S-1-5-32-547","Power Users",
3     "S-1-5-32-555","Remote Desktop Users",
4     "S-1-5-32-580","Remote Management Users",
5 ];
```

<https://www.verboon.info/2024/02/monitoring-windows-built-in-local-security-groups-with-microsoft-defender-xdr-or-sentinel/>

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

# What did you do with KQL this month?

## Microsoft Sentinel - TAXII Connector failures

The screenshot displays a KQL query in the Microsoft Sentinel console and its corresponding results. The query filters for error-level activities related to the TAXII connector. The results table shows four entries, all with error codes like 'BadRequest' or 'Transient' and messages indicating timeouts or invalid configurations.

```
1 AzureActivity
2 | where Level == "Error"
3 | where OperationNameValue == "MICROSOFT.SECURITYINSIGHTS/DATACONNECTORS/WRITE"
4 | extend resourceGroup_ = tostring(parse_json(Properties).resourceGroup)
5 | extend code = tostring(parse_json(tostring(parse_json(tostring(parse_json(Properties).statusMessage)).error)).code)
6 | extend message = tostring(parse_json(tostring(parse_json(tostring(parse_json(Properties).statusMessage)).error)).message)
7 | where message contains "TAXII"
8 | project TimeGenerated, ResourceGroup, Caller, code, message
```

TimeGenerated [Local Time]	ResourceGroup	Caller	code	message
> 2/3/2024, 3:48:41.776 PM	RG_SENTINEL01		BadRequest	Timed out waiting for the TAXII server
> 2/3/2024, 3:50:05.505 PM	RG_SENTINEL01		Transient	Transient error verifying TAXII server. P
> 2/3/2024, 3:51:22.375 PM	RG_SENTINEL01		BadRequest	Timed out waiting for the TAXII server
> 2/3/2024, 3:52:24.512 PM	RG_SENTINEL01		BadRequest	Timed out waiting for the TAXII server

On the right, a detailed view of the error messages is shown:

- Failed to add TAXII connector**  
The TAXII connector could not be configured due to an unexpected error.
- Failed to add TAXII connector**  
The TAXII connector could not be configured due to an unexpected error.
- Failed to add TAXII connector**  
TAXII API root URL or Collection ID is not valid.

<https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Sentinel/HealthAndAudit/Sentinel-TaxiiConnectorFailures.md>

# What did you do with KQL this month?

## Auditing Defender Controlled Folder Access

```
DeviceEvents
| where ActionType == "ControlledFolderAccessViolationBlocked"
| where AccountName !contains "system"
```

```
1 DeviceRegistryEvents
2 | where RegistryKey =~ @"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager"
3 | where RegistryValueName == "AllowedApplications"
4 | sort by Timestamp desc
5 | project-reorder Timestamp, DeviceId, DeviceName, RegistryValueData
6
```

Getting started

Results

Query history

↓ Export

10 items

🔍 Search

🕒 00:00.123

■ ■ ■ Low ⓘ

📊 Chart type ▾

⚙️ Customize columns

☐ Timestamp ↓

DeviceId

DeviceName

RegistryValueData

☐ > Feb 9, 2024 3:52:4... 🖨 730f3b21b04107eec4... 🖨 kw-g12pst3

C:\Users\GianniCastaldi\AppData\Local\Microsoft\OneDrive\OneDrive.exe|C:\Use

Thanks for attending



**KQL** | Cafe