KQL Café | February 2024

Your | hosts

Alex Verboon









https://twitter.com/alexverboon

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

https://github.com/alexverboon

https://www.verboon.info/

https://twitter.com/castello_johnny

<u> nttps://www.linkedin.com/in/giannicastaldi/</u>

https://github.com/KustoKing

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



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



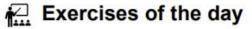
Damien Van Robaey

<u> https://twitter.com/syst_and_deploy</u>

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

LEARN KQL IN ONE MONTH





Intune environment

- 1. Display records where free disk percent is lesser than 20%
- 2. Display records count
- Display devices count where free disk percent is lesser than or equals to 5%
- 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

- 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

Q Key words

- summarize
- count, countif

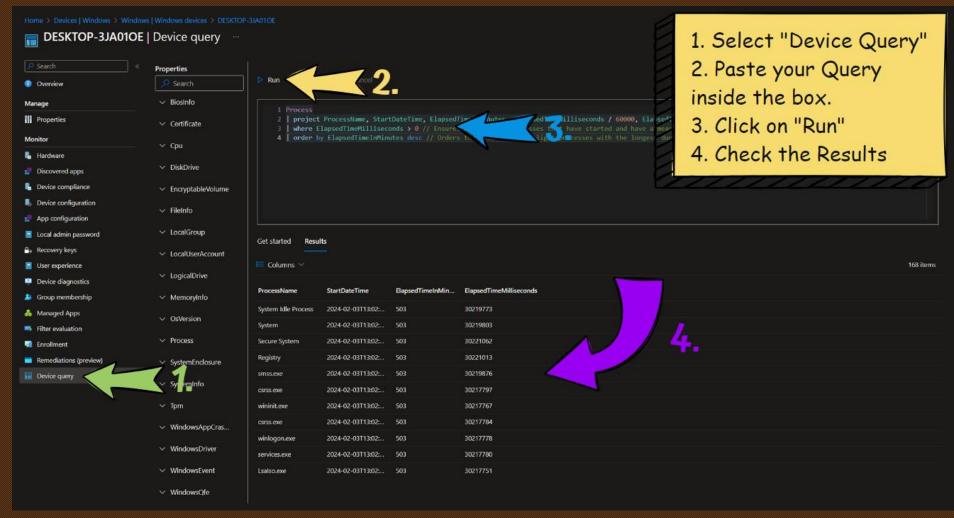
Device Query in Intune

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

Thanks Ugur Koc |



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.mc

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 let ListAllActionsAndOperations = () {
   union *
   | extend Action = iff(isnotempty(ActionType), ActionType, iff(isnotempty(Operation), Operation, iff(isnotempty(OperationName), (
   | 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.mc

```
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
```



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 PrevousResult = prev(ResultType)
```

What did you do with KQL this month?

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

```
let SensitiveBuiltInGroups = datatable(GroupsSID: string,BuildInGroupName: string)

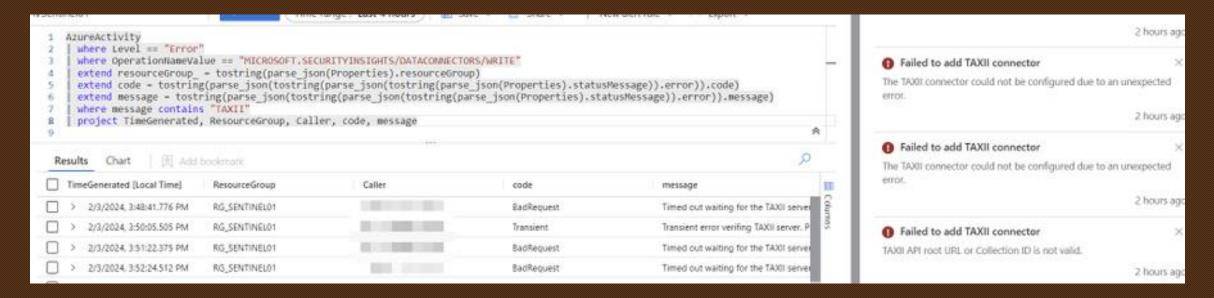
"S-1-5-32-544","Administrtors",
    "S-1-5-32-546","Guests",
    "S-1-5-32-547","Power Users",
    "S-1-5-32-555","Remote Desktop Users",
    "S-1-5-32-580","Remote Management Users",
];
```

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.mc

What did you do with KQL this month?

Microsoft Sentinel - TAXII Connector failures



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	5 project-reorder Timestamp, DeviceId, DeviceName, RegistryValueData				
6					
Getting s	tarted Results	Query history			
<u>↓</u> Ехрог	t		10 items Search	© 00:00.123 ■■■ Low	∠ Chart type ∠ □ Customize columns
Timestamp ↓		DeviceId	DeviceName	Registry Value Data	
☐ > Feb 9, 2024 3:52:4 ☐ 730f3b21b04107eec4 ☐ kw-g12pst3		$C: \ \ C: \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $			

Thanks for attending

