Session 3-2023 |Azure Kusto

KQL|Cafe

Your | hosts

Alex Verboon

Gianni Castaldi

MVP Microsoft® Most Valuable Professional

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/

Show | Agenda

Welcome

What is new in KQL

Our KQL Guest

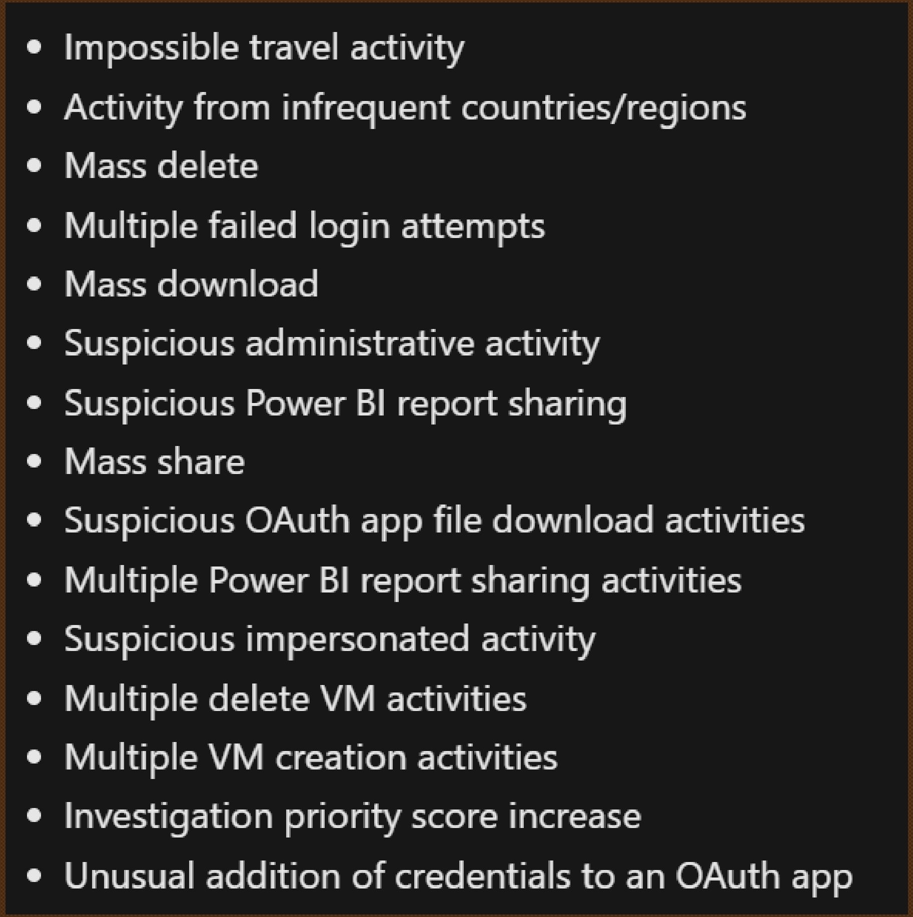
What did you do with KQL this month?

What's New

Investigate behaviors with advanced hunting (Preview)

https://learn.microsoft.com/en-us/defender-cloud-apps/behaviors

Table name	Description
BehaviorInfo	Record per behavior with its metadata, including behavior title, MITRE Attack categories, and techniques.
BehaviorEntities	Information on the entities that were part of the behavior. Can be multiple records per behavior.

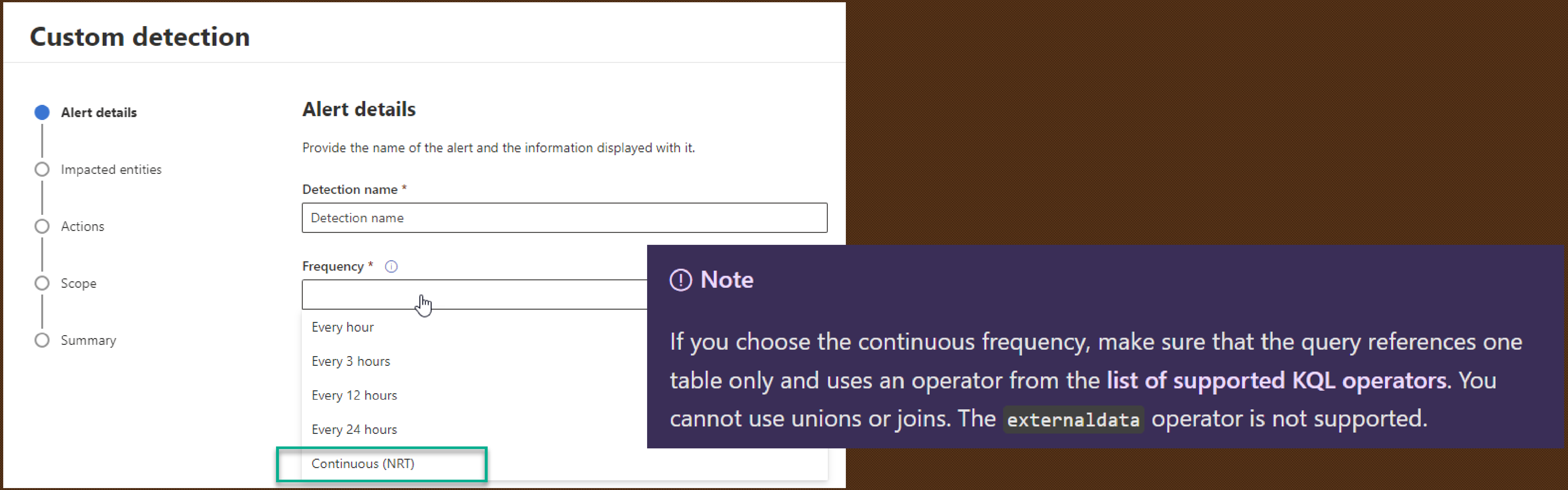


- Impossible travel activity
- Activity from infrequent countries/regions
- Mass delete
- Multiple failed login attempts
- Mass download
- Suspicious administrative activity
- Suspicious Power BI report sharing
- Mass share
- Suspicious OAuth app file download activities
- Multiple Power BI report sharing activities
- Suspicious impersonated activity
- Multiple delete VM activities
- Multiple VM creation activities
- Investigation priority score increase
- Unusual addition of credentials to an OAuth app

What's New

Respond to threats in near real-time with custom detections

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/respond-to-threats-in-near-real-time-with-custom-detections/ba-p/3761243



Custom detection

● Alert details
○ Impacted entities
○ Actions
○ Scope
○ Summary

Alert details

Provide the name of the alert and the information displayed with it.

Detection name *

Detection name

Frequency *

- Every hour
- Every 3 hours
- Every 12 hours
- Every 24 hours
- Continuous (NRT)

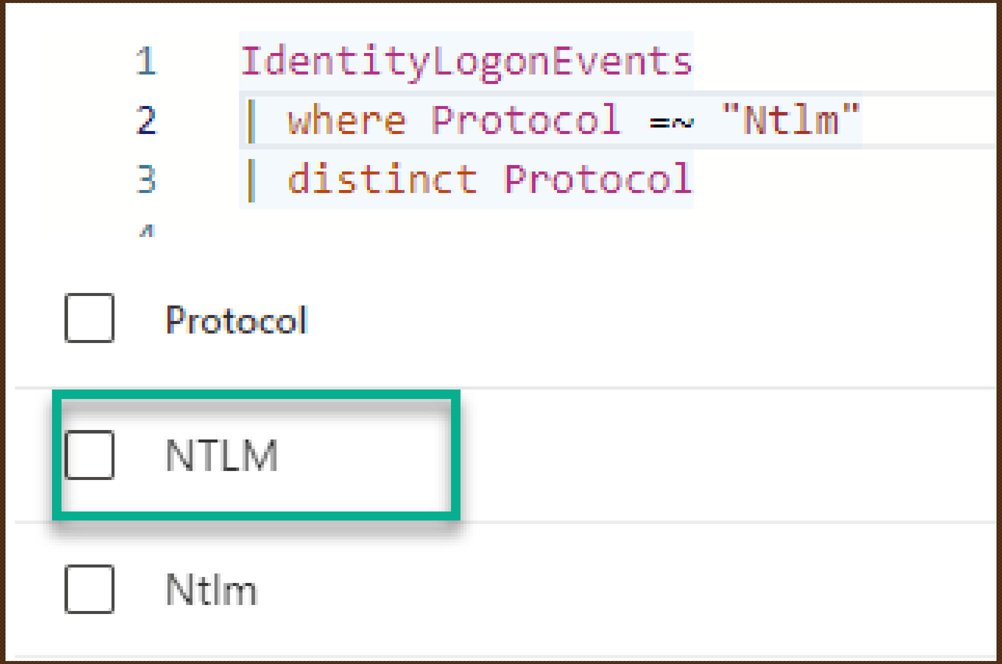
Note

If you choose the continuous frequency, make sure that the query references one table only and uses an operator from the **list of supported KQL operators**. You cannot use unions or joins. The `externaldata` operator is not supported.

What's New

Updated NTLM Protocol Name for the Identity Advanced Hunting Tables
https://admin.microsoft.com/Adminportal/Home?source=applauncher&ref=MessageCenter/:/messages/MC509576
The old protocol name Ntlm will now be the new protocol name **NTLM**.

The tables affected are:
IdentityLogonEvents
IdentityQueryEvents
IdentityDirectoryEvents



```
IdentityLogonEvents
| where Protocol =~ "Ntlm"
| distinct Protocol
```

```
□ Protocol
□ NTLM
□ Ntlm
```

What's New

Advanced Hunting Updates in DeviceInfo

https://admin.microsoft.com/Adminportal/Home?source=applauncher&ref=MessageCenter/:/messages/MC524717

What's New

The following fields and values will change in **DeviceInfo** table in advanced hunting:

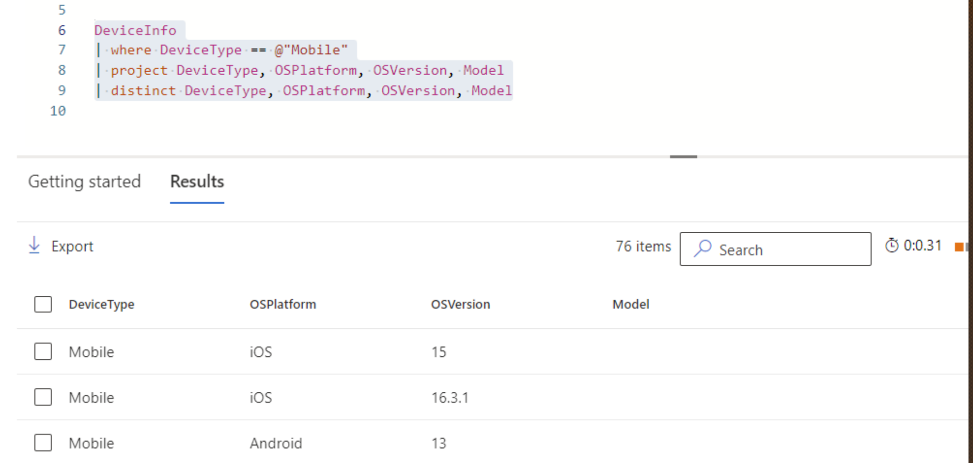
OsVersion – OS versions string will include the minor version also when it is ‘0’. For example: 9.0, 10.0, 11.0, etc.

DeviceType – Mobile devices will now be assigned with the DeviceType value ‘Mobile,’ instead of ‘Unknown’.

MergedMachineIds – MergedMachineIds field will be available for devices onboarded to MDE as well.

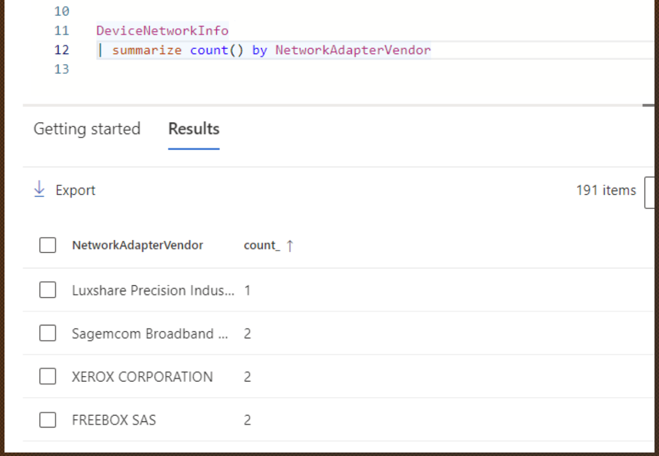
The following fields and values will change in **DeviceNetworkInfo** table in advanced hunting:

NetworkAdapterVendor – NetworkAdapterVendor field will be available for devices onboarded to MDE as well



```
DeviceInfo
| where DeviceType == @"Mobile"
| project DeviceType, OSPlatform, OSVersion, Model
| distinct DeviceType, OSPlatform, OSVersion, Model
```

DeviceType	OSPlatform	OSVersion	Model
Mobile	iOS	15	
Mobile	iOS	16.3.1	
Mobile	Android	13	



```
DeviceNetworkInfo
| summarize count() by NetworkAdapterVendor
```

NetworkAdapterVendor	count_ ↑
Luxshare Precision Indus...	1
Sagemcom Broadband ...	2
XEROX CORPORATION	2
FREEBOX SAS	2

What's New

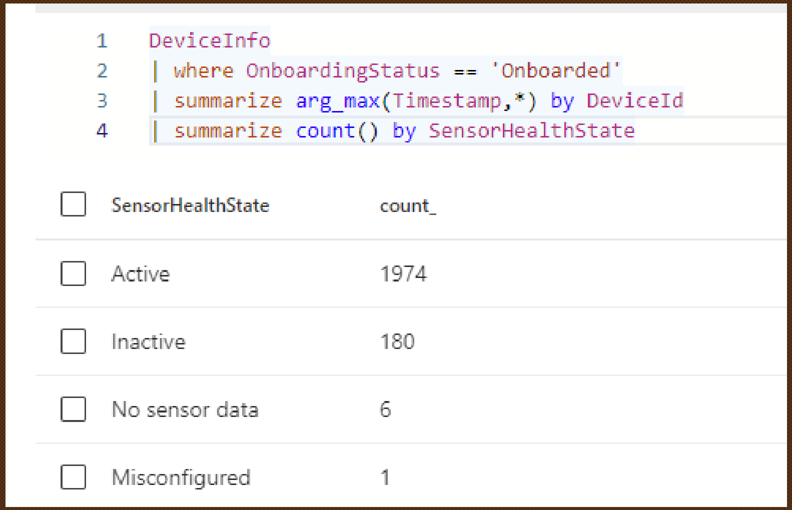
The following fields will be added to **DeviceInfo** table in advanced hunting:

SensorHealthState – gives you the health status of an onboarded device's EDR sensor. We hope this gives you additional insight about devices in your network.

IsInternetFacing – indicates whether the device is internet-facing and may be susceptible to external communication. Addition evidence regarding why this device was identified as internet-facing are available in the AdditionalFields column in DeviceInfo table.

IsExcluded – determines if the device is currently excluded from Microsoft Defender for Vulnerability Management experiences.

ExclusionReason – indicates the reason for device exclusion..

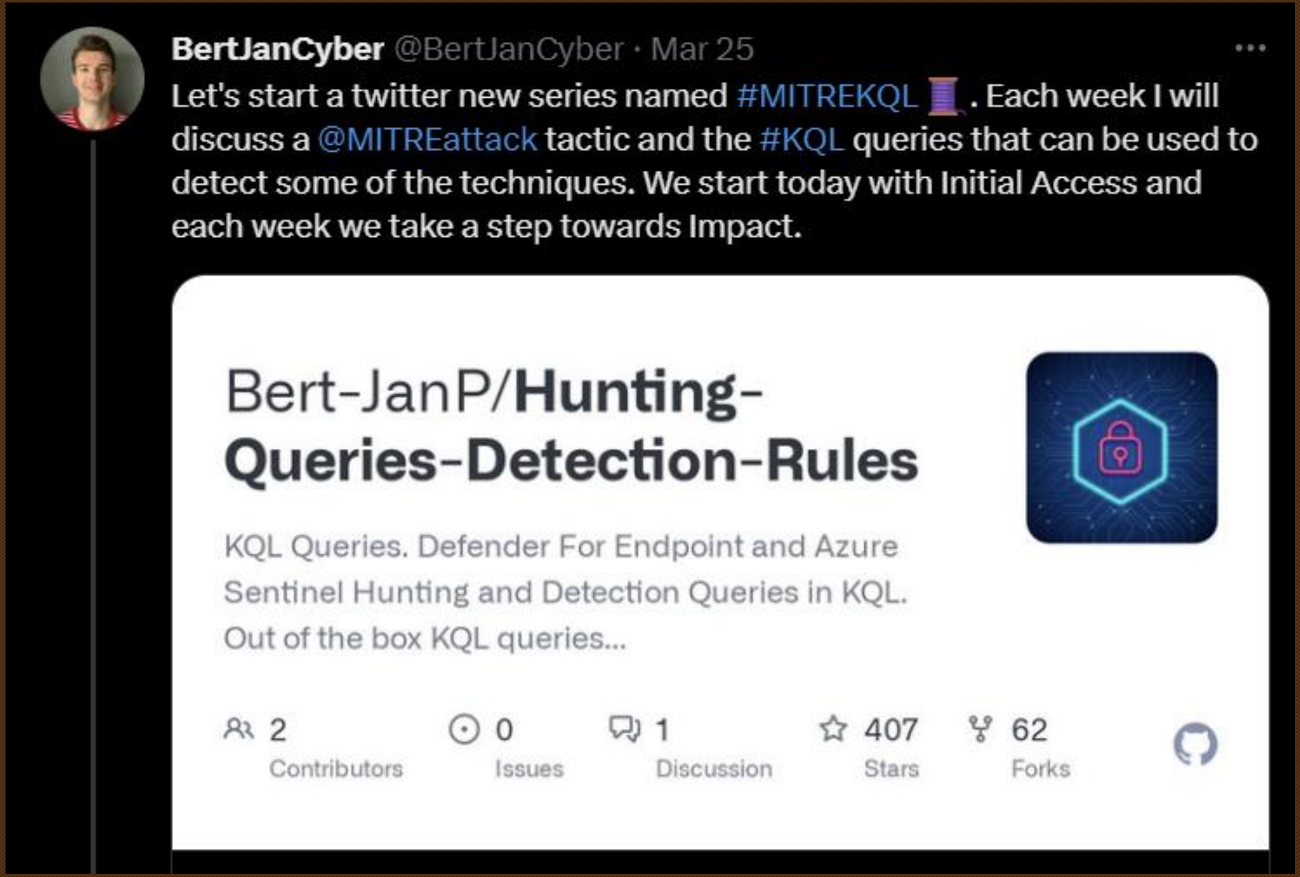


```
DeviceInfo
| where OnboardingStatus == 'Onboarded'
| summarize arg_max(Timestamp,*) by DeviceId
| summarize count() by SensorHealthState
```

□	SensorHealthState	count_
□	Active	1974
□	Inactive	180
□	No sensor data	6
□	Misconfigured	1

What's New

MITRE ATT&CK Mapping
https://github.com/Bert-JanP/Hunting-Queries-Detection-Rules/blob/main/MITRE%20ATT%26CK/Mapping.md



BertJanCyber @BertJanCyber · Mar 25

Let's start a twitter new series named #MITREKQL 🧵. Each week I will discuss a @MITREattack tactic and the #KQL queries that can be used to detect some of the techniques. We start today with Initial Access and each week we take a step towards Impact.

Bert-JanP/**Hunting-Queries-Detection-Rules**

KQL Queries. Defender For Endpoint and Azure Sentinel Hunting and Detection Queries in KQL. Out of the box KQL queries...

2	0	1	407	62
Contributors	Issues	Discussion	Stars	Forks

Today's | Guest

Alexander Sloutsky

Partner Software Engineering Manager at Microsoft

What did you do with KQL this month?

Thanks for attending

KQL|Cafe