

Session 7-2023 | Jupyter Notebooks

# 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 Brian Bønke Rueløkke

What did you do with KQL this month?

# What's New – MDE - Zeek

With the recent integration of Zeek providing advanced protocol parsing capabilities, which result in better visibility into full network sessions.

The previous ActionType in the DeviceNetworkEvents table “**NetworkSignatureInspected**” is replaced by the ActionTypes listed below

## ActionType

- DnsConnectionInspected
- SslConnectionInspected
- NtlmAuthenticationInspected
- HttpConnectionInspected
- IcmpConnectionInspected
- SshConnectionInspected
- InboundInternetScanInspected
- FtpConnectionInspected
- SntpConnectionInspected

[Enrich your advanced hunting experience using network layer signals from Zeek \(microsoft.com\)](https://microsoft.com/zeek)

# What's New – MDE - Zeek

Identify systems that are scanned from the internet

```
25 DeviceNetworkEvents
26 | where ActionType == "InboundInternetScanInspected"
27 | project TimeGenerated, DeviceName, LocalIP, LocalPort, RemoteIP, RemotePort, ActionType
28 | extend current_geoinfo = geo_info from ip_address(LocalIP)
29 | extend country = tostring(current_geoinfo.country)
30 | extend city = tostring(current_geoinfo.city)
31 | extend state = tostring(current_geoinfo.state)
32 | join IP_Indicators on $left. LocalIP == $right. TI_ipEntity
33
```

# What's New – MDE - Zeek

## Identify systems with FTP activity

```
4
5 DeviceNetworkEvents
6 | where ActionType == "FtpConnectionInspected"
7 | extend json = todynamic(AdditionalFields)
8 | extend command = tostring(json.command)
9 | extend reply_code = tostring(json.reply_code)
10 | extend reply_msg = tostring(json.reply_msg)
11 | extend direction = tostring(json.direction)
12 | extend user = tostring(json.user)
13 | extend arg = tostring(json.arg)
14 | extend cwd = tostring(json.cwd)
15 | extend geoinfo = geo info from ip address(RemoteIP)
```

Results Chart Add bookmark

	direction	user	arg ↑↓	cwd	country
	Out	www	ftp://1[REDACTED]	pi	France
t.conf	Out	www	ftp://1[REDACTED]	pi	France
ed here), 0.56 Kbytes per second	Out	www	ftp://1[REDACTED]	pi	France
	Out	[REDACTED]	ftp://[REDACTED]	arkeepass.kdbx /	Germany
	Out	[REDACTED]	ftp://[REDACTED]	arkeepass.kdbx /	Germany
	Out	[REDACTED]	ftp://[REDACTED]	arkeepass.kdbx /	Germany

# What's New - Azure Resource Graph

[Query Azure Resource Graph from Azure Monitor](#)

[Query data in Azure Data Explorer and Azure Resource Graph from Azure Monitor](#)

[Azure Resource Graph table and resource type reference](#)

```
arg('').Resources  
| distinct type
```

List Log Analytics Workspace information

```
arg('').Resources  
| where type == "microsoft.operationalinsights/workspaces"  
| extend SKUName = tostring(parse_json(tostring(properties.sku)).name)  
| extend dailyQuotaGb = tostring(parse_json(tostring(properties.workspaceCapping)).dailyQuotaGb)  
| extend quotaNextResetTime =  
todatetime(tostring(parse_json(tostring(properties.workspaceCapping)).quotaNextResetTime))  
| extend retentionInDays = tostring(properties.retentionInDays)  
| project name, location, resourceGroup, retentionInDays, SKUName, dailyQuotaGb, quotaNextResetTime
```



# What's New - Azure Resource Graph

List active resource health alerts






```
arg("").servicehealthresources
| extend EventSource = tostring(properties.EventSource)
| extend Status = tostring(parse_json(tostring(parse_json(tostring(properties.Impact))[0].ImpactedRegions))[0].Status)
| extend Title = tostring(properties.Title)
| extend TrackingId = tostring(properties.TrackingId)
| extend ImpactStartTime_ = todatetime(tostring(properties.ImpactStartTime))
| extend LastUpdateTime = todatetime(tostring(properties.LastUpdateTime))
| where Status == "Active"
```

# What's New - Azure Resource Graph

Identify Azure Subscriptions that are not monitored by the Azure Activity Data Connector in Sentinel

```
// Identify Azure Subscriptions that are not monitored by the Azure Activity Data Connector in Sentinel
let allsubscriptions =
arg("").resourcecontainers
| where type == "microsoft.resources/subscriptions"
| distinct subscriptionId, name;
allsubscriptions
| join kind=leftouter (AzureActivity
| extend AzureActivitySyubscriptionId = SubscriptionId
| distinct AzureActivitySyubscriptionId)
on $left.subscriptionId == $right.AzureActivitySyubscriptionId
| extend IsMonitored = iff(isempty(AzureActivitySyubscriptionId),"No","Yes")
| project subscriptionId, name, AzureActivitySyubscriptionId, IsMonitored
```


# What's New - KQLQuery.com


 [https://kqlquery.com/posts/kql\\_sources/](https://kqlquery.com/posts/kql_sources/)


KQL Query


PostsTagsCategories


## KQL Security Sources

 Bert-Jan Pals

included in  KQL

 2023-09-07

 485 words

 3 minutes

## KQL Security Sources

This blog is dedicated to providing some of the KQL security sources that I use regularly. Those sources can be really helpful to learn KQL, but also to improve your detection coverage! Most of you know that I have my Github repository where I share KQL queries, even though I share some queries I also leverage a lot of other great community sources! If you are into KQL or want to get inspired I recommend checking all of them out!

### kqlsearch.com

Ever wondered if a search engine for KQL existed? The dream is over, it does exist! [Urrur Koc](#) has created a search engine for KQL queries for security and intune which can help you easily search for queries you need. At the moment of writing the engine has indexed more than 1400 unique KQL queries!

Link: <https://www.kqlsearch.com/>

## Azure Sentinel

# What's New - beta.KQLSearch.com

## KQL Search V2

[Query Assistant](#)[Query Generator](#)[Show Advanced Filters](#)[Statistics](#)

### MDI - ADGroupAdditions

*Author: Bert-Jan Pals*   *Released: 9/17/2023*



### PowerShellEncodedReconActivities

*Author: Bert-Jan Pals*   *Released: 9/16/2023*



### PowerShellEncodedWebRequests

*Author: Bert-Jan Pals*   *Released: 9/16/2023*

[Privacy policy](#)[Imprint](#)

Made by [Ugur Koc](#) with



# What's New - IdentityInfo

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identityinfo-table?view=o365-worldwide>

[Identity hunting with an enhanced IdentityInfo table \(microsoft.com\)](#)

Column	Data type	Description
Timestamp	datetime	The date and time that the line was written to the database.
DistinguishedName	string	The user's distinguished name
Manager	string	The listed manager of the account user
Phone	string	The listed phone number of the account user
CreatedDateTime	datetime	The date and time that the user was created
SourceProvider	string	The identity's source, such as Azure Active Directory, Active Directory, or a hybrid identity synchronized from Active Directory to Azure Active Directory
ChangeSource	string	Identifies which identity provider or process triggered the addition of the new row. For example, the System-UserPersistence value is used for any rows added by an automated process.
Tags	dynamic	Tags assigned to the account user by Defender for Identity
AssignedRoles	dynamic	For identities from Azure Active Directory only, the roles assigned to the account user

# Learning KQL

```
set query_now = datetime('2023-08-04T14:46:34.3319494Z');  
SigninLogs  
| where TimeGenerated between (ago(1d) .. now())
```

```
set query_now = datetime('20230804144634');  
SigninLogs  
| where TimeGenerated between (ago(1d) .. now())
```



# Brian Bønk Rueløkke

Principal & Enterprise arkitekt, Data & Analytics

*Fellowmind*



<https://linkedin.com/in/brianbonk>



<https://brianbonk.dk>



Microsoft

FastTrack Recognized  
Solution Architect  
Power BI  
2022 >>



Microsoft

Certified Trainer  
Data Platform

2018 >>



# What did you do with KQL this month?

## MDI Disabling Accounts (Automatic Attack Disruption)

### Action Center

PendingHistory

Export

1-2 of 2

✓	Action update time ↓	Investigation ID	Approval ID	Action type	Details	Entity type
✓	Jul 14, 2023 4:45 PM	8532	91e734	Disable user		Account
	May 30, 2023 7:31 PM	8496	f2868b	Disable user		Account

### Disable user

[Open investigation page](#) [Enable user](#) [Disable user](#)

Disables the user in on prem Active Directory. It might take a few minutes for this change to take effect.

#### Action details

Submission time

Jul 14, 2023, 4:45:12 PM

Submitted by

Attack disruption

Action source

MDI (Automatic)

Action status

✓ Completed

Approval ID

91e734

#### Comments and history

Attack disruption

Jul 14, 2023, 4:45:12 PM

The potentially compromised account was automatically disabled in Active Directory to prevent it from accessing resources.

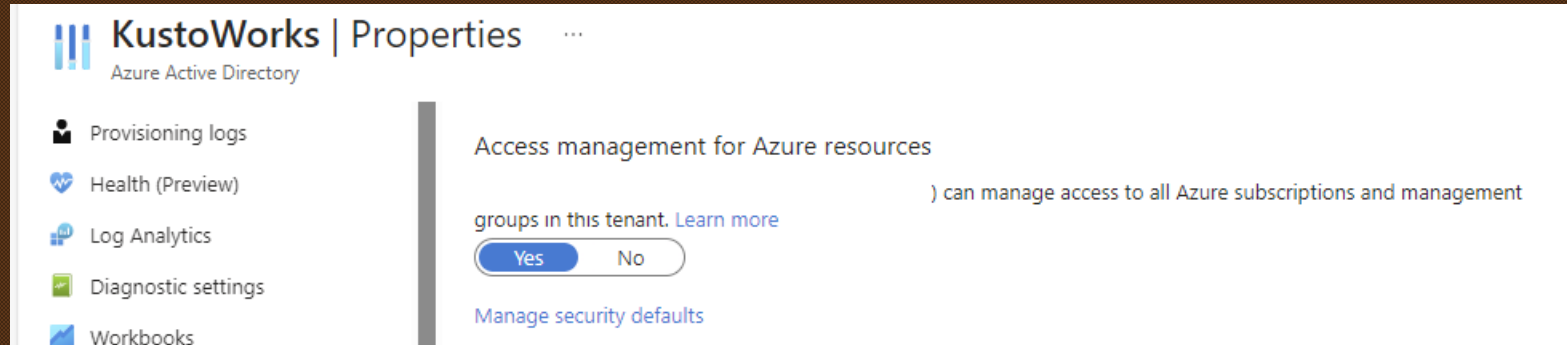
# What did you do with KQL this month?

## MDI Disabling Accounts (Automatic Attack Disruption)

```
let AllDomainControllers =  
    DeviceNetworkEvents  
    | where TimeGenerated > ago(7d)  
    | where LocalPort == 88  
    | where LocalIPType == "FourToSixMapping"  
    | extend DCDevicename = tostring(split(DeviceName,".")[0])  
    | distinct DCDevicename;  
IdentityDirectoryEvents  
| where TimeGenerated > ago(190d)  
| where ActionType == "Account disabled"  
| extend ACTOR_DEVICE = tolower(tostring(AdditionalFields["ACTOR.DEVICE"]))  
| where isnotempty( ACTOR_DEVICE)  
| where ACTOR_DEVICE in (AllDomainControllers)  
| project TimeGenerated, TargetAccountDisplayName, ACTOR_DEVICE
```

# What did you do with KQL this month?

## Monitor User Access Administrator elevation



```
arg("").authorizationresources
| where properties.roleDefinitionId == "/providers/Microsoft.Authorization/RoleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9"
```

```
1 arg("").authorizationresources
2 | where properties.roleDefinitionId == "/providers/Microsoft.Authorization/RoleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9"
3
```

Results Chart Add bookmark

id	name	type	tenantId	resourceGroup
/providers/Microsoft.Authorization/RoleAssignments/be4b8635-0cff-4d17-98f3-e9ac159b12ae	be4b8635-0cff-4d17-98f3-e9a...	microsoft.authorization/roleassignme...	53ff34c6-2184-43e1-9b57-ec3...	
id	/providers/Microsoft.Authorization/RoleAssignments/be4b8635-0cff-4d17-98f3-e9ac159b12ae			
name	be4b8635-0cff-4d17-98f3-e9ac159b12ae			
type	microsoft.authorization/roleassignments			
tenantId	53ff34c6-2184-43e1-9b57-ec32e21e222f			
apiVersion	2019-07-01			
properties	{ "roleDefinitionId": "/providers/Microsoft.Authorization/RoleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9", "principalType": "User", "description": null, "principalId": "e12ea9be-2b4b-49b4-a9ba-401235ade425", "updatedOn": "2023-09-18T20" }			

Thanks for attending



**KQL** | Cafe