

Session 4-2023 | KQL & Automation



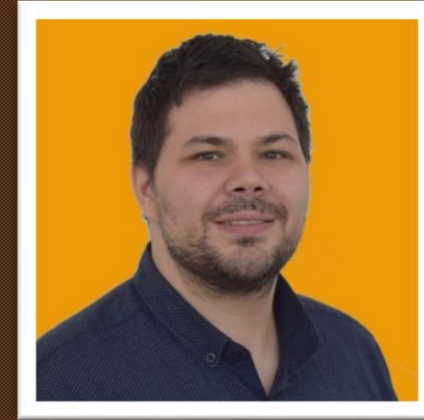
KQL | Cafe

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/>

Show | Agenda

Welcome

What is new/updates for KQL

Our KQL Guest

What did you do with KQL this month?

What's New

Enrich your advanced hunting experience using network layer signals from Zeek

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/enrich-your-advanced-hunting-experience-using-network-layer/ba-p/3794693>

Query

① Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 // Identify Server/Client pairs being used for SSH connections
2 DeviceNetworkEvents
3 | where ActionType == "SshConnectionInspected"
4 | extend json = todynamic(AdditionalFields)
5 | project Server = tostring(json.server), Client = tostring(json.client)
6 | distinct Server , Client
```

Getting started

Results

↓ Export

85

<input type="checkbox"/> Server	Client ↓
<input type="checkbox"/> SSH-2.0-OpenSSH_8.0	SSH-2.0-WinSCP_release_5.21.7
<input type="checkbox"/> SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6	SSH-2.0-WinSCP_release_5.21.7

What's New

Discovering internet-facing devices using Microsoft Defender for Endpoint

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/discovering-internet-facing-devices-using-microsoft-defender-for/ba-p/3778975>



Query

① Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 DeviceInfo
2 | where Timestamp > ago(7d)
3 | where IsInternetFacing
4 | extend InternetFacingInfo = AdditionalFields
5 | extend InternetFacingReason = extractjson("$.InternetFacingReason", InternetFacingInfo, typeof(string)),
6   InternetFacingLocalPort = extractjson("$.InternetFacingLocalPort", InternetFacingInfo, typeof(int)), InternetFacingScannedPublicPort = extractjson("$.InternetFacingScannedPublicPort",
7   InternetFacingInfo, typeof(int)), InternetFacingScannedPublicIp = extractjson("$.InternetFacingScannedPublicIp", InternetFacingInfo, typeof(string)),
8   InternetFacingLocalIp = extractjson("$.InternetFacingLocalIp", InternetFacingInfo, typeof(string)), InternetFacingTransportProtocol=extractjson("$.InternetFacingTransportProtocol",
9   InternetFacingInfo, typeof(string)), InternetFacingLastSeen = extractjson("$.InternetFacingLastSeen", InternetFacingInfo, typeof(datetime))
10 | summarize arg_max(Timestamp, *) by DeviceId
11 | project
12   DeviceName,
13   IsInternetFacing,
14   InternetFacingReason,
15   InternetFacingLocalIp,
16   InternetFacingLocalPort,
17   InternetFacingScannedPublicIp,
18   InternetFacingScannedPublicPort
19 | where InternetFacingLocalPort == 139
```

Getting started **Results**

↓ Export

<input type="checkbox"/>	DeviceName	IsInternetFacing	InternetFacingReason	InternetFacingLocalIp	InternetFacingLocalPort	InternetFacingScannedPublicIp	InternetFacingScannedPublicPort
<input type="checkbox"/>		1	PublicScan		139		


What's New

How Microsoft names threat actors

<https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide>

Use the following query on Microsoft 365 Defender and other Microsoft security products supporting the Kusto query language (KQL) to get information about a threat actor using the old name, new name, or industry name:

Kusto

 Copy

```
let TANames = externaldata(PreviousName: string, NewName: string, Origin: string, OtherNames: dynamic)[@"http
let GetThreatActorAlias = (Name: string) {
TANames
| where Name =~ NewName or Name =~ PreviousName or OtherNames has Name
};
GetThreatActorAlias("ZINC")
```

The following files containing the comprehensive mapping of old threat actor names with their new names are also available:

- [JSON format](#)
- [downloadable Excel](#)

Hidden Characters in your Data

<input type="checkbox"/>		Original
<input type="checkbox"/>	>	String
<input type="checkbox"/>	>	String
<input type="checkbox"/>	>	String
<input type="checkbox"/>	>	String Test
<input type="checkbox"/>	>	String Test

Today's | Guest



Thijs Lecomte

Sr. M365 Consultant | 365bythijs.be | MVP | M365
Security for the IT Pro E-Book

<https://m365securitybook.com/>

<https://practical365.com/author/thijs-lecomte/>

What did you do with KQL this month?

Deprecated PowerShell Modules

<https://github.com/alexverboon/MDATP/blob/master/AdvancedHunting/depr-psmodule.md>

Query

```
1 // Search for PowerShell commands included in the PowerShell module: AzureADPreview Version:2.0.2.149)
2 let pscommands = dynamic (["Add-AzureADAdministrativeUnitMember","Add-AzureADApplicationOwner","Add-AzureADApplicationPol
3 DeviceEvents
4 | where ActionType contains "PowerShellCommand"
5 | where AdditionalFields has_any (pscommands)
6 | extend command = parse_json(AdditionalFields)
7 | evaluate bag_unpack(command)
8 | project DeviceName,InitiatingProcessAccountName, InitiatingProcessFileName, Command
9 | summarize PowerShellCommands = make_set(Command) by DeviceName, InitiatingProcessAccountName
```

Getting started

Results

Export

1 item

Search

0:7.266

Medium

Chart type

Customize columns

<input type="checkbox"/>	DeviceName	InitiatingProcessAccountNa...	PowerShellCommands
<input type="checkbox"/>			["Get-AzureADUser","Se...

Thanks for attending



KQL | Cafe