

Session 1-2023 | 1 Year KQL Cafe



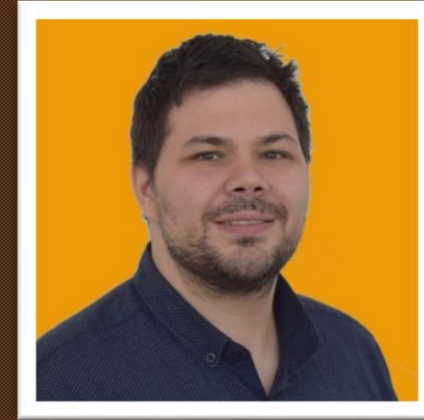
**KQL** | Cafe

# 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://twitter.com/castello_johnny)

<https://www.linkedin.com/in/giannicastaldi/>

<https://github.com/KustoKing>

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

## KQL Café – 1 Year

- 10 Shows in 2022
- 9 Guests in 2022
- 293 Members in Meetup
- 180 Members in the LinkedIn Group
- 231 Subscribers in YouTube
- 2,554 views in YouTube

## KQL Café – 1 Year

Rod Trend	Jan-22
Matt Zorich	Feb-22
Mathew Lowe	Mar-22
Olaf Hartong	Apr-22
Mehmet Ergene	Jun-22
Ashwin Patil	Aug-22
Mattias Borg	Sep-22
Jan Ketil Skanke	Oct-22
Bert-Jan Pals	Nov-22

**Thank You!**

# Today's | Guest

Last minute cancelation.....

Show | Agenda

Welcome

What's new in KQL

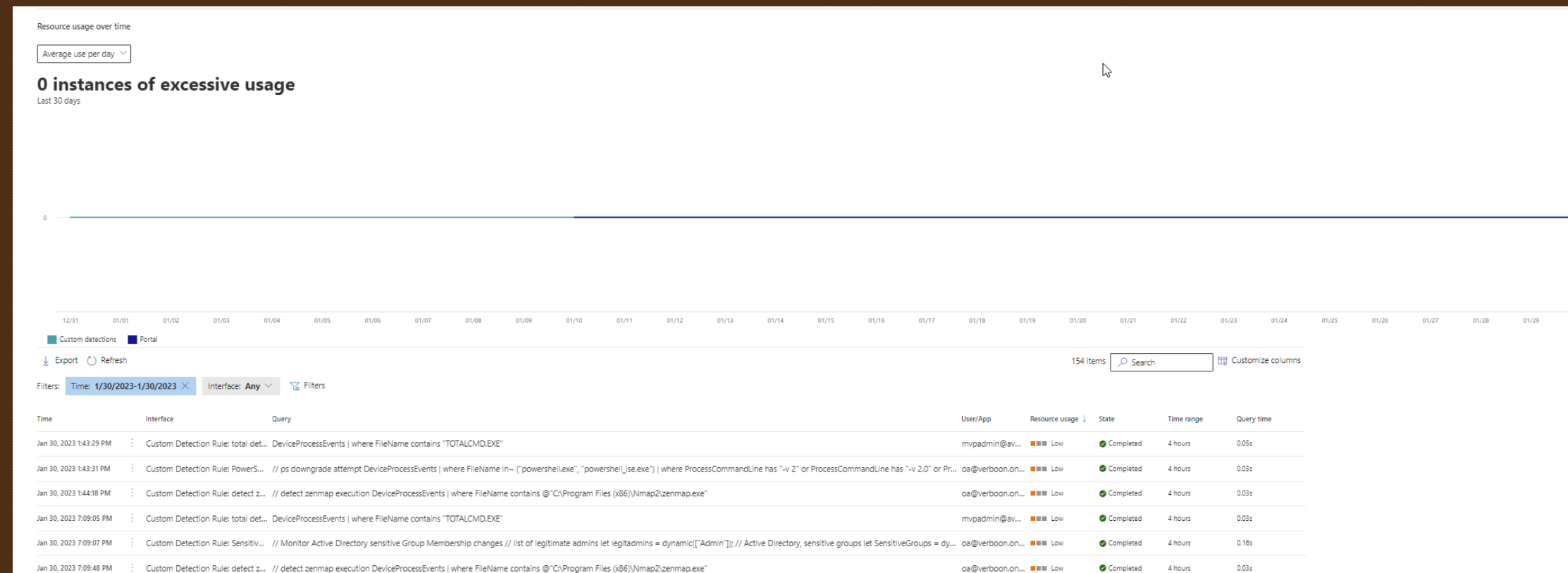
Our KQL Guest

What did you do with KQL this month?



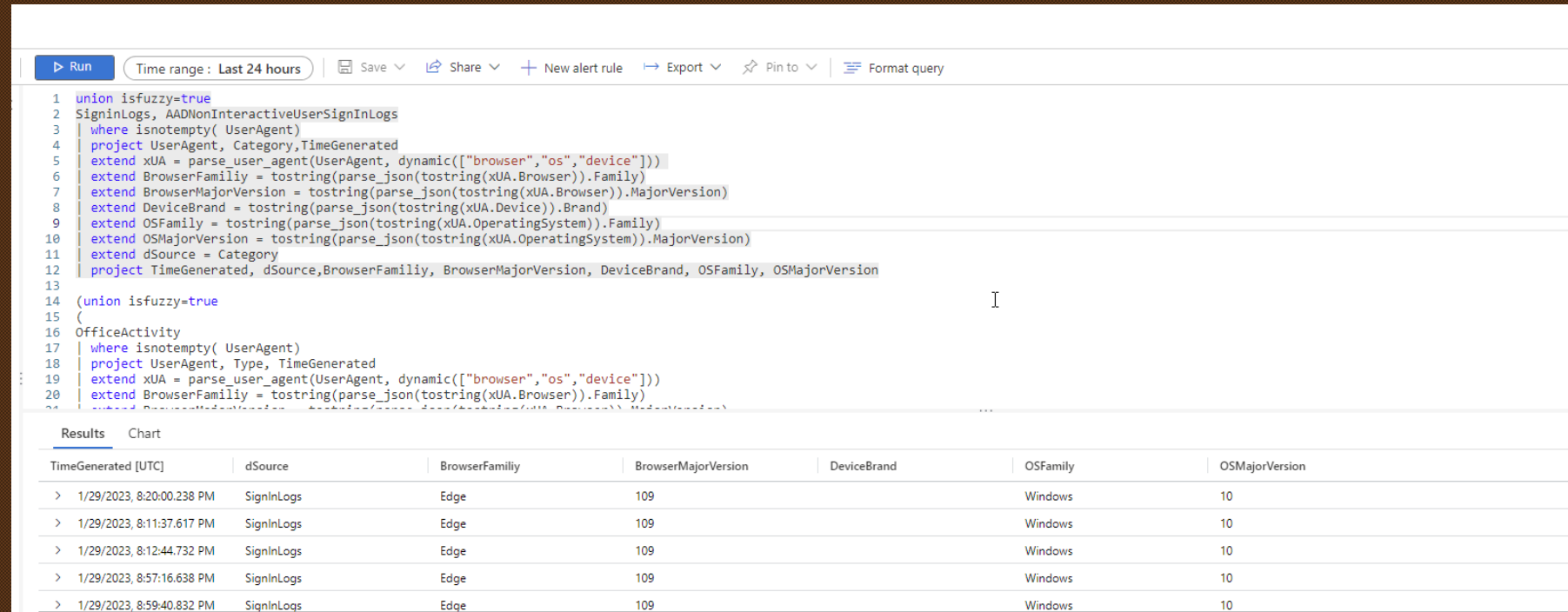


# MD365 Query Resources



# parse\_user\_agent()

```
union isfuzzy=true
SigninLogs, AADNonInteractiveUserSignInLogs
| where isnotempty( UserAgent)
| project UserAgent, Category,TimeGenerated
| extend xUA = parse_user_agent(UserAgent, dynamic(["browser","os","device"]))
| extend BrowserFamiliy = tostring(parse_json(tostring(xUA.Browser)).Family)
| extend BrowserMajorVersion = tostring(parse_json(tostring(xUA.Browser)).MajorVersion)
| extend DeviceBrand = tostring(parse_json(tostring(xUA.Device)).Brand)
| extend OSFamily = tostring(parse_json(tostring(xUA.OperatingSystem)).Family)
| extend OSMajorVersion = tostring(parse_json(tostring(xUA.OperatingSystem)).MajorVersion)
| extend dSource = Category
| project TimeGenerated, dSource,BrowserFamiliy, BrowserMajorVersion, DeviceBrand, OSFamily, OSMajorVersion
```



The screenshot shows a KQL query editor interface with a toolbar at the top containing buttons for Run, Save, Share, New alert rule, Export, Pin to, and Format query. The query is a Kusto query that unions two data sources, SigninLogs and AADNonInteractiveUserSignInLogs, and projects various user agent fields. The results are displayed in a table below the query editor.

```
1 union isfuzzy=true
2 SigninLogs, AADNonInteractiveUserSignInLogs
3 | where isnotempty( UserAgent)
4 | project UserAgent, Category,TimeGenerated
5 | extend xUA = parse_user_agent(UserAgent, dynamic(["browser","os","device"]))
6 | extend BrowserFamiliy = tostring(parse_json(tostring(xUA.Browser)).Family)
7 | extend BrowserMajorVersion = tostring(parse_json(tostring(xUA.Browser)).MajorVersion)
8 | extend DeviceBrand = tostring(parse_json(tostring(xUA.Device)).Brand)
9 | extend OSFamily = tostring(parse_json(tostring(xUA.OperatingSystem)).Family)
10 | extend OSMajorVersion = tostring(parse_json(tostring(xUA.OperatingSystem)).MajorVersion)
11 | extend dSource = Category
12 | project TimeGenerated, dSource,BrowserFamiliy, BrowserMajorVersion, DeviceBrand, OSFamily, OSMajorVersion
13
14 (union isfuzzy=true
15 (
16 OfficeActivity
17 | where isnotempty( UserAgent)
18 | project UserAgent, Type, TimeGenerated
19 | extend xUA = parse_user_agent(UserAgent, dynamic(["browser","os","device"]))
20 | extend BrowserFamiliy = tostring(parse_json(tostring(xUA.Browser)).Family)
21 | extend BrowserMajorVersion = tostring(parse_json(tostring(xUA.Browser)).MajorVersion)
22 | extend DeviceBrand = tostring(parse_json(tostring(xUA.Device)).Brand)
23 | extend OSFamily = tostring(parse_json(tostring(xUA.OperatingSystem)).Family)
24 | extend OSMajorVersion = tostring(parse_json(tostring(xUA.OperatingSystem)).MajorVersion)
25 | project TimeGenerated, Type, dSource, BrowserFamiliy, BrowserMajorVersion, DeviceBrand, OSFamily, OSMajorVersion
26 )
27 )
```

TimeGenerated [UTC]	dSource	BrowserFamily	BrowserMajorVersion	DeviceBrand	OSFamily	OSMajorVersion
> 1/29/2023, 8:20:00.238 PM	SigninLogs	Edge	109		Windows	10
> 1/29/2023, 8:11:37.617 PM	SigninLogs	Edge	109		Windows	10
> 1/29/2023, 8:12:44.732 PM	SigninLogs	Edge	109		Windows	10
> 1/29/2023, 8:57:16.638 PM	SigninLogs	Edge	109		Windows	10
> 1/29/2023, 8:59:40.832 PM	SigninLogs	Edge	109		Windows	10

# ASR State

DeviceInfo

```
| where OnboardingStatus == 'Onboarded'  
| where isnotempty(OSPlatform)  
| summarize arg_max(Timestamp, *) by DeviceName  
| where OSPlatform startswith "Windows"  
| project DeviceName, OSPlatform  
| join kind=leftouter (  
    DeviceTvmInfoGathering  
    | extend AF = parse_json(AdditionalFields)  
    | extend ASR1 = parse_json(AdditionalFields.AsrConfigurationStates)  
    | project DeviceName, ASR1  
    | evaluate bag_unpack(ASR1)  
    )  
on $left.DeviceName == $right.DeviceName  
| project-away DeviceName1
```

Query

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

```
1 DeviceInfo  
2 | where OnboardingStatus == 'Onboarded'  
3 | where isnotempty(OSPlatform)  
4 | summarize arg_max(Timestamp, *) by DeviceName  
5 | where OSPlatform startswith "Windows"  
6 | project DeviceName, OSPlatform  
7 | join kind=leftouter (  
8     DeviceTvmInfoGathering  
9     | extend AF = parse_json(AdditionalFields)  
10    | extend ASR1 = parse_json(AdditionalFields.AsrConfigurationStates)  
11    | project DeviceName, ASR1  
12    | evaluate bag_unpack(ASR1)  
13    )  
14 on $left.DeviceName == $right.DeviceName  
15 | project-away DeviceName1
```

Getting started Results

Export 62 items Search

	DeviceName	OSPlatform	AdobeReaderChildProcess	ExecutableEmailContent	ExecutableOfficeContent	ObfuscatedScript	OfficeChildProcess	OfficeCommAppChildProcess	OfficeMac
<input type="checkbox"/>		Windows11	Block	Block	Block	Block	Block	Block	Block
<input type="checkbox"/>		Windows11	Block	Block	Block	Block	Block	Block	Block
<input type="checkbox"/>		Windows10	Block	Block	Block	Block	Block	Block	Block
<input type="checkbox"/>		Windows10	Off	Off	Off	Off	Off	Off	Off

# Multiple Not statements

```
1 CommonSecurityLog
2 | where TimeGenerated > ago(90d)
3 | where DeviceVendor == "Palo Alto Networks"
4     and DeviceProduct == "PAN-OS"
5     and Activity == "THREAT"
6 | summarize count() by DeviceEventClassID
7
```

Results Chart | Add bookmark

<input type="checkbox"/> DeviceEventClassID	count_ ↑↓
<input type="checkbox"/> > url	243,003
<input type="checkbox"/> > Microsoft Windows NTLMSSP Detection(92322)	61,420
<input type="checkbox"/> > HTTP-200(41003)	57,135
<input type="checkbox"/> > HTTP-100(41000)	29,564
<input type="checkbox"/> > Suspicious HTTP Evasion Found(14984)	6,336
<input type="checkbox"/> > file	4,424
<input type="checkbox"/> > HTTP-206(41009)	4,348
<input type="checkbox"/> > Suspicious TLS Evasion Found(14978)	2,714

```
8 CommonSecurityLog
9 | where TimeGenerated > ago(90d)
10 | where DeviceVendor == "Palo Alto Networks"
11     and DeviceProduct == "PAN-OS"
12     and Activity == "THREAT"
13 | count
14
```

Results Chart | Add bookmark

<input type="checkbox"/> Count
<input type="checkbox"/> > 413,062

```
15 CommonSecurityLog
16 | where TimeGenerated > ago(90d)
17 | where DeviceVendor == "Palo Alto Networks"
18     and DeviceProduct == "PAN-OS"
19     and Activity == "THREAT"
20     and DeviceEventClassID != "url"
21     or DeviceEventClassID != "file"
22     or DeviceEventClassID != "wildfire"
23 | count
24
```

Results Chart | Add bookmark

<input type="checkbox"/> Count
<input type="checkbox"/> > 3,289,868

## UrlHaus Playbooks

Status : All

Trigger kind : **All**

Subscription : **Visual Studio Enterprise Subscription - DEMO Lab**

Resour

<input type="checkbox"/> Name ↑↓	Status ↑↓	Plan ↑↓	Trigger kind ↑↓	Subscription ↑↓
<input type="checkbox"/> URLhaus-CheckURLAndEnrichIncident	Enabled	Consumption	Microsoft Sentinel Incident (Preview)	Visual Studio Enterprise Subscription ..
<input type="checkbox"/> URLhaus-CheckHashAndEnrichIncident	Enabled	Consumption	Microsoft Sentinel Incident (Preview)	Visual Studio Enterprise Subscription ..
<input type="checkbox"/> URLhaus-CheckHostAndEnrichIncident	Enabled	Consumption	Microsoft Sentinel Incident (Preview)	Visual Studio Enterprise Subscription ..

an Delete Incident Tasks (Preview)

soon: the new incident page - new features, in-context experiences and improved functionality!

### MO - URL Detonate

Incident ID: 3600

Status: New Severity: Medium

1 Alerts 0 Bookmarks

Time: 5:28 PM Creation time: 01/09/23, 07:54 AM

94.130.190.4...  
147.108.150...  
65.192.63.20...  
182.119.219...

Book review

URL Detonate

mal.azure.com/assets/Microsoft\_Azure\_Security Insg...

Timeline Similar Incidents (Preview) Alerts Bookmarks Entities Comments (1)

AV

Normal B I U G

---

Comment created from playbook - URLhaus-CheckURLandEnrichIncident 01/09/23, 06:26 PM

URLhaus URL Checking Results:

blacklists	date_added	host	id	last_online	reporter	tags	threat	url	url_status	urlhaus_reference
spamhaus_dblnot listed.surbinot listed	2023-01-06 16:36:11 UTC	36.230.52.196	2499109	2023-01-07 01:00:00 UTC	lrz_urlhaus	&quot;e&quot;. &quot;Moz&quot;	malware_download	http://36.230.52.196:55679/Moz.a	offline	https://urlhaus.abuse.ch/url/2499109/
spamhaus_dblnot listed.surbinot listed	2023-01-06 19:39:13 UTC	85.192.63.204	2499243	2023-01-08 09:00:00 UTC	abuse_ch	&quot;d&quot;. &quot;RecordBreaker&quot;	malware_download	http://85.192.63.204/nTjDQoQ6kTSbkSbQ4eR8E1xP7H2vK/mccgslu.dll	offline	https://urlhaus.abuse.ch/url/2499243/
spamhaus_dblnot listed.surbinot listed	2023-01-06 00:50:13 UTC	219.157.57.34	2498267	2023-01-07 18:00:00 UTC	lrz_urlhaus	&quot;e&quot;. &quot;Moz&quot;	malware_download	http://219.157.57.34:52687/Moz.m	offline	https://urlhaus.abuse.ch/url/2498267/
spamhaus_dblnot listed.surbinot listed	2023-01-06 16:51:11 UTC	221.15.215.134	2499120	2023-01-08 16:00:00 UTC	lrz_urlhaus	&quot;e&quot;. &quot;Moz&quot;	malware_download	http://221.15.215.134:49467/Moz.m	offline	https://urlhaus.abuse.ch/url/2499120/
spamhaus_dblnot listed.surbinot listed	2023-01-06 20:51:12 UTC	61.52.159.232	2499298		lrz_urlhaus	&quot;e&quot;. &quot;Moz&quot;	malware_download	http://61.52.159.232:58196/Moz.a	online	https://urlhaus.abuse.ch/url/2499298/
spamhaus_dblnot listed.surbinot listed	2023-01-06 07:07:04 UTC	182.119.219.69	2498573	2023-01-06 22:00:00 UTC	geenensp	&quot;32-bit&quot;. &quot;e&quot;. &quot;mips&quot;. &quot;Moz&quot;	malware_download	http://182.119.219.69:56270/i	offline	https://urlhaus.abuse.ch/url/2498573/
spamhaus_dblnot listed.surbinot listed	2023-01-06 23:20:13 UTC	219.157.164.239	2499405	2023-01-07 18:00:00 UTC	lrz_urlhaus	&quot;e&quot;. &quot;Moz&quot;	malware_download	http://219.157.164.239:36152/Moz.m	offline	https://urlhaus.abuse.ch/url/2499405/
spamhaus_dblnot listed.surbinot listed	2023-01-06 12:35:06 UTC	27.215.52.136	2498903	2023-01-06 21:00:00 UTC	lrz_urlhaus	&quot;e&quot;. &quot;Moz&quot;	malware_download	http://27.215.52.136:55055/Moz.m	offline	https://urlhaus.abuse.ch/url/2498903/

Thanks for attending

