

Session 2-2023 | Intune



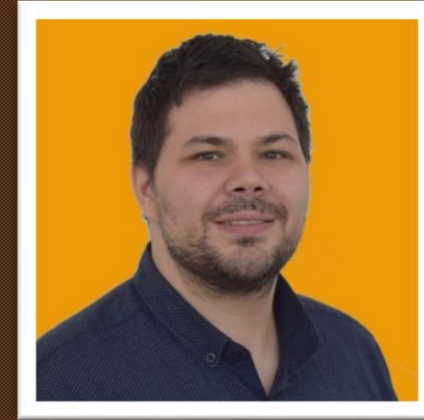
KQL | Cafe

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

Interactive KQL Cheatsheet

ABC of threat hunting

Bag_unpack / parse_commandline

Our KQL Guest

What did you do with KQL this month?

What's New

Interactive KQL Cheatsheet

<https://blog.amestofortytwo.com/kqlcheat/>

Go HUnt - ABC of threat hunting

[https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/01/ABCs of Threat Hunting.pdf](https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/01/ABCs_of_Threat_Hunting.pdf)

bag_unpack

```
1 DeviceEvents
2 | where Timestamp > ago (30d)
3 | where ActionType == @"TamperingAttempt"
4 | extend AF = parse_json(AdditionalFields)
5 | evaluate bag_unpack(AF)
6
7 DeviceEvents
8 | where Timestamp > ago (30d)
9 | where ActionType == @"TamperingAttempt"
10 | extend AF = parse_json(AdditionalFields)
11 | evaluate bag_unpack(AF, columnsConflict='keep_source') : (DeviceName:string, TimeGenerated:datetime, ActionType:string, Status:string, TamperingAction:long, Target:string)
```

Getting started **Results**

Export 69 items Search 0:0.16 Low Chart type

<input type="checkbox"/> DeviceName ↑	TimeGenerated	ActionType	Blocked	TamperingAction	Target
<input type="checkbox"/> securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp
<input type="checkbox"/> securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp
<input type="checkbox"/> securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp
<input type="checkbox"/> securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp

parse_command_line

The screenshot shows a Kusto query editor interface. At the top, there are tabs for 'New Query 1*' and 'parse_cmd*'. Below the tabs, the query is written in Kusto syntax. The query filters for 'PowerShell' events, projects specific fields, and uses the 'parse_command_line' function to parse the 'InitiatingProcessCommandLine' field with the 'windows' parser. The results are summarized by the command string.

```
1 DeviceEvents
2 | where ActionType contains "PowerShell"
3 | project TimeGenerated, DeviceName, InitiatingProcessCommandLine
4 | extend Cmd1 = parse_command_line(InitiatingProcessCommandLine,"windows")
5 | mv-expand Cmd1
6 | summarize count() by tostring(Cmd1)
7
```

Below the query, the 'Results' tab is active, showing a table with two columns: 'Cmd1' and 'count_'. The table lists various command strings and their corresponding counts.

Cmd1	count_ ↑↓
> powershell	666
> -command	666
> (Get-WmiObject Win32_OperatingSy...	666
> powershell.exe	199
> -ExecutionPolicy	163
> -NoProfile	104
> =	99
> -File	89
> Bypass	86

Today's | Guest



Ugur Koc

[@UgurKocDe](#)

<https://github.com/ugurkocde?tab=repositories>

Thanks for attending

