Session 2-2023 | Intune

KQL|Cafe

Your | hosts

Alex Verboon

https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

Gianni Castaldi

https://twitter.com/castello_johnny

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

https://github.com/KustoKing

https://www.kustoking.com/

Microsoft® MVP Most Valuable Professional

Show | Agenda

Welcome

Interactive KQL Cheatsheet

ABC of threat hunting

Bag_unpack / parse_commandline

Our KQL Guest

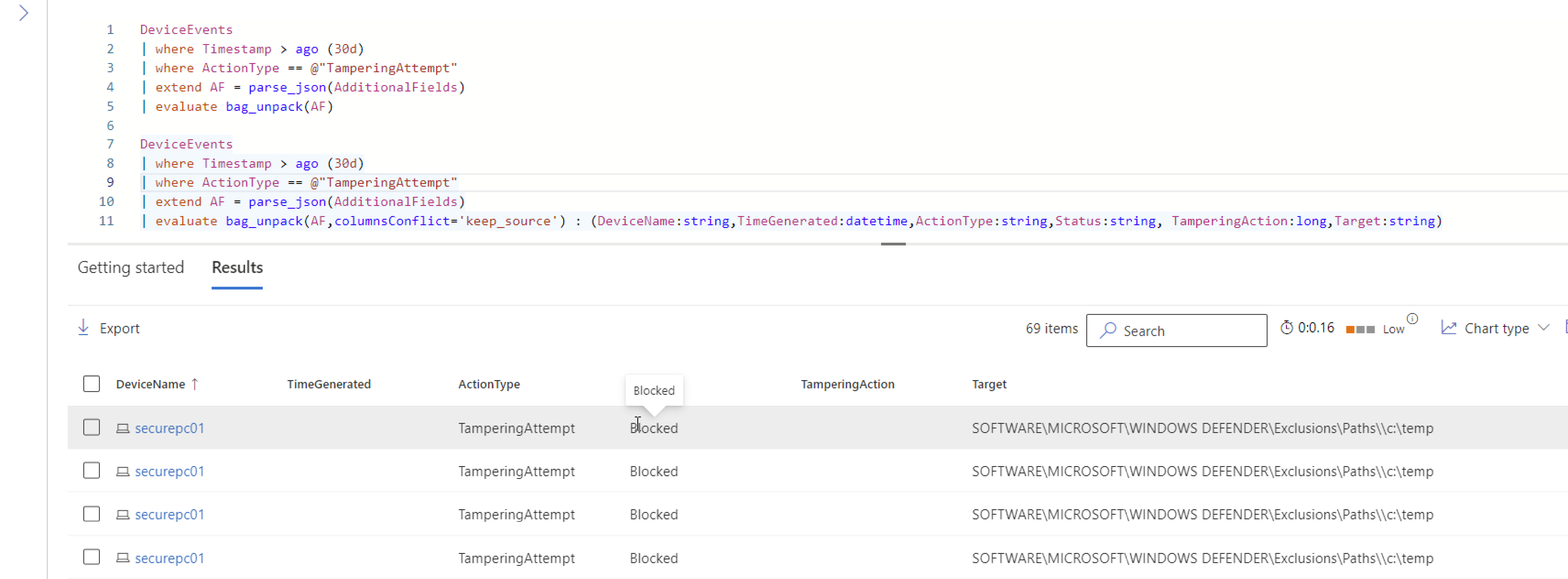
What did you do with KQL this month?

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

bag_unpack

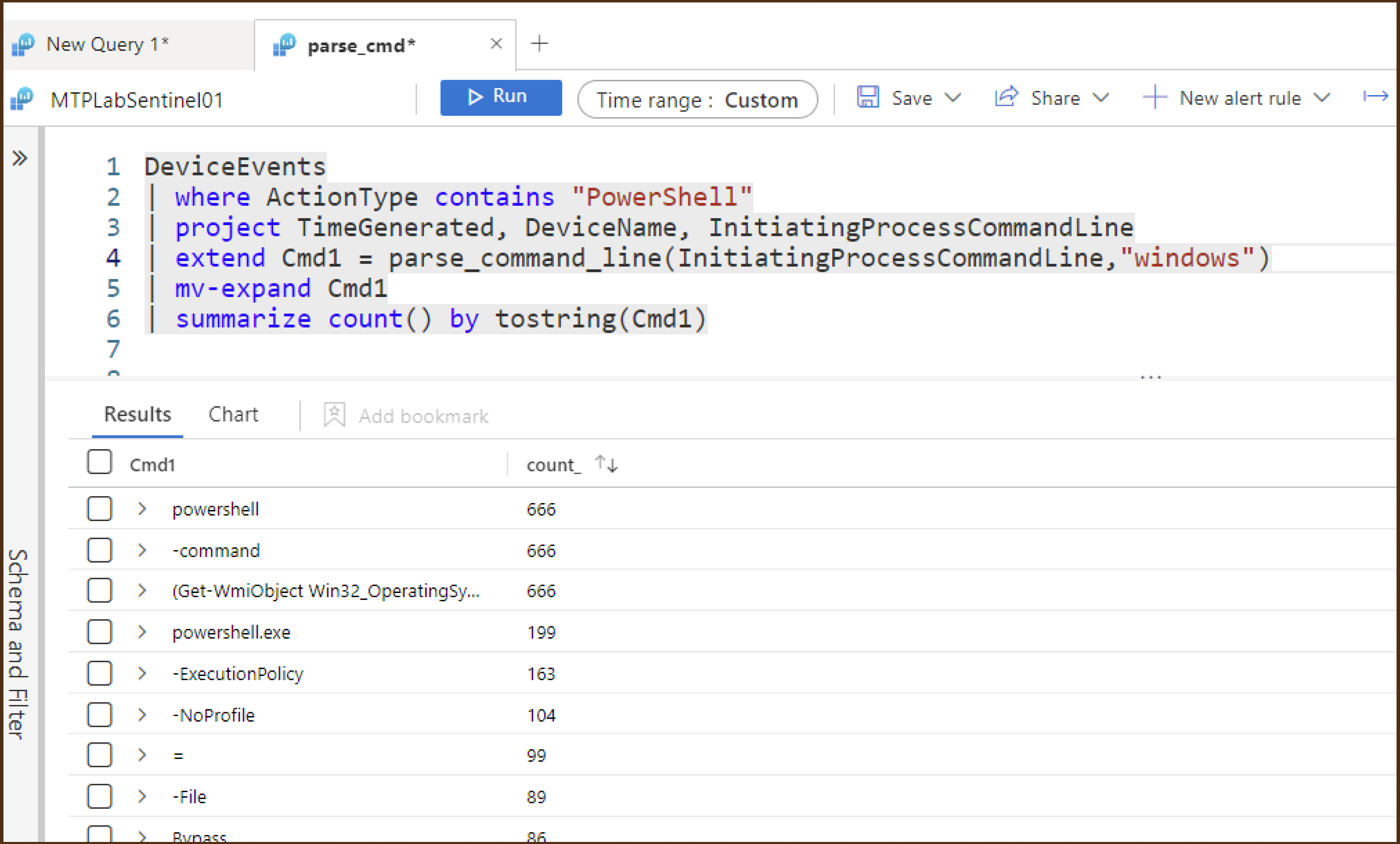


```
DeviceEvents
| where Timestamp > ago (30d)
| where ActionType == @"TamperingAttempt"
| extend AF = parse_json(AdditionalFields)
| evaluate bag_unpack(AF)

DeviceEvents
| where Timestamp > ago (30d)
| where ActionType == @"TamperingAttempt"
| extend AF = parse_json(AdditionalFields)
| evaluate bag_unpack(AF,columnsConflict='keep_source') : (DeviceName:string,TimeGenerated:datetime,ActionType:string,Status:string, TamperingAction:long,Target:string)
```

DeviceName ↑	TimeGenerated	ActionType		TamperingAction	Target
securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp
securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp
securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp
securepc01		TamperingAttempt	Blocked		SOFTWARE\MICROSOFT\WINDOWS DEFENDER\Exclusions\Paths\\c:\temp

parse_command_line



```
DeviceEvents
| where ActionType contains "PowerShell"
| project TimeGenerated, DeviceName, InitiatingProcessCommandLine
| extend Cmd1 = parse_command_line(InitiatingProcessCommandLine,"windows")
| mv-expand Cmd1
| summarize count() by tostring(Cmd1)
```

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

KQL|Cafe