# Session 3 | KQL Workbooks

KQL|Cafe

# Session 3 | KQL Workbooks

# Your | hosts

## Alex Verboon

https://twitter.com/alexverboon

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

https://github.com/alexverboon

https://www.verboon.info/

MVP Microsoft® Most Valuable Professional

## Gianni Castaldi

https://twitter.com/castello_johnny

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

https://github.com/KustoKing

https://www.kustoking.com/

# Show | Agenda

Welcome

What's new in KQL

Working with IOCs

Learning KQL

KQL Tools

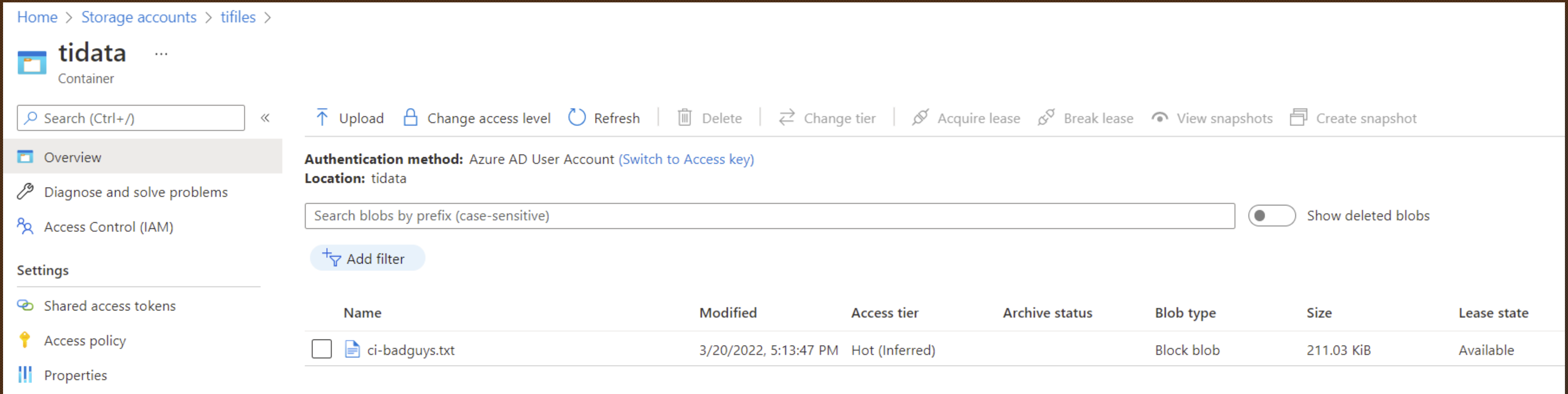
Our KQL Guest

What did you do with KQL this month?

KQL Challenge of the month

# Create a large watchlist from file in Azure Storage (public preview)

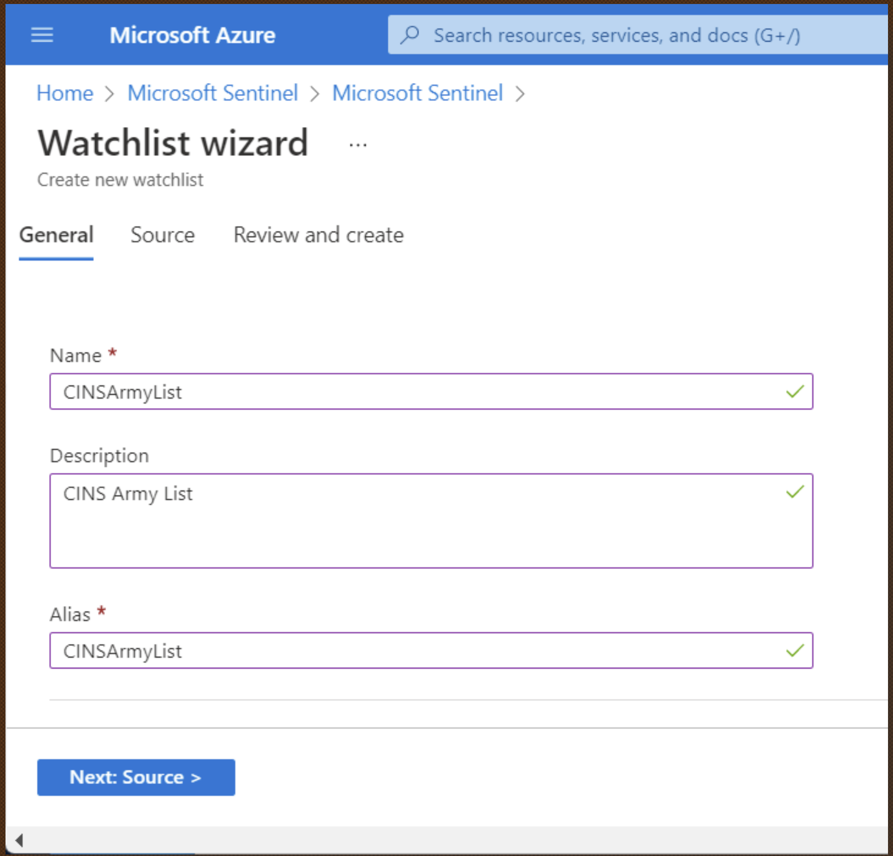
Create a watchlist from a large file that's up to **500 MB** in size by uploading the file to your Azure Storage account. When you add the watchlist to your workspace, you provide a shared access signature URL. Microsoft Sentinel uses the shared access signature URL to retrieve the watchlist data from Azure Storage.



**Authentication method:** Azure AD User Account (Switch to Access key)
**Location:** tidata

| | Name | Modified | Access tier | Archive status | Blob type | Size | Lease state |
|---|---|---|---|---|---|---|---|
| □ | ci-badguys.txt | 3/20/2022, 5:13:47 PM | Hot (Inferred) | | Block blob | 211.03 KiB | Available |

# Create a large watchlist from file in Azure Storage (public preview)


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
General
Source
Review and create
Next: Source >

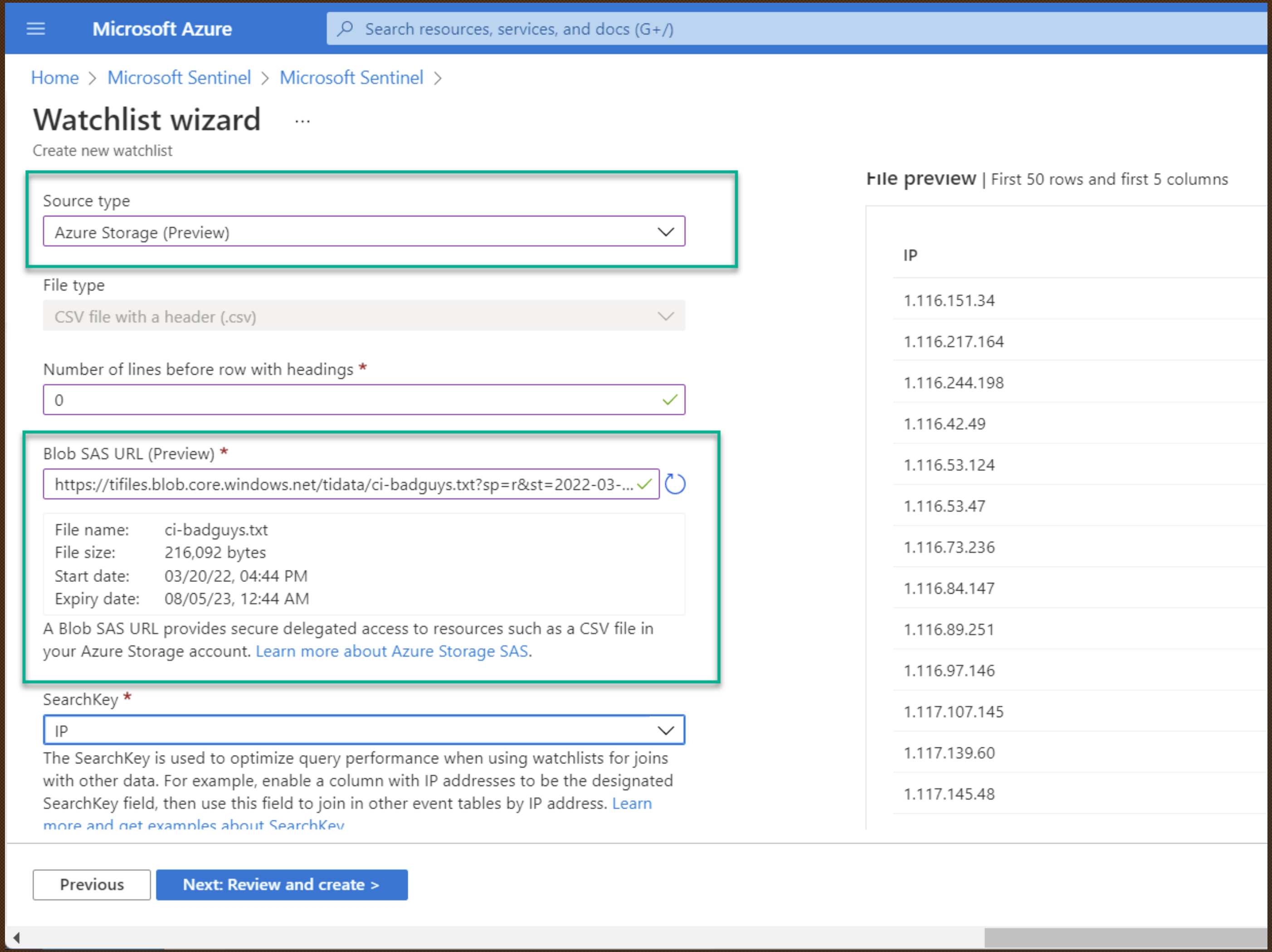
Watchlist wizard ...

Create new watchlist

Name *: CINSArmyList ✓

Description: CINS Army List ✓

Alias *: CINSArmyList ✓


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
Previous
Next: Review and create >

Watchlist wizard ...

Create new watchlist

Source type: Azure Storage (Preview)

File type: CSV file with a header (.csv)

Number of lines before row with headings *: 0 ✓

Blob SAS URL (Preview) *: https://tifiles.blob.core.windows.net/tidata/ci-badguys.txt?sp=r&st=2022-03-... ✓

| | |
|---|---|
| File name: | ci-badguys.txt |
| File size: | 216,092 bytes |
| Start date: | 03/20/22, 04:44 PM |
| Expiry date: | 08/05/23, 12:44 AM |

A Blob SAS URL provides secure delegated access to resources such as a CSV file in your Azure Storage account. Learn more about Azure Storage SAS.

SearchKey *: IP

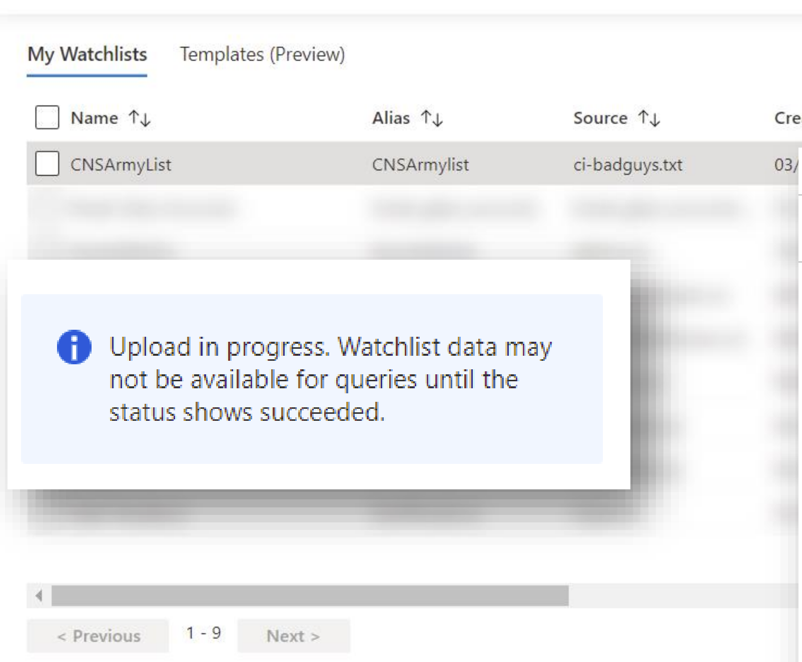
The SearchKey is used to optimize query performance when using watchlists for joins with other data. For example, enable a column with IP addresses to be the designated SearchKey field, then use this field to join in other event tables by IP address. Learn more and get examples about SearchKey

File preview | First 50 rows and first 5 columns

| IP |
|---|
| 1.116.151.34 |
| 1.116.217.164 |
| 1.116.244.198 |
| 1.116.42.49 |
| 1.116.53.124 |
| 1.116.53.47 |
| 1.116.73.236 |
| 1.116.84.147 |
| 1.116.89.251 |
| 1.116.97.146 |
| 1.117.107.145 |
| 1.117.139.60 |
| 1.117.145.48 |

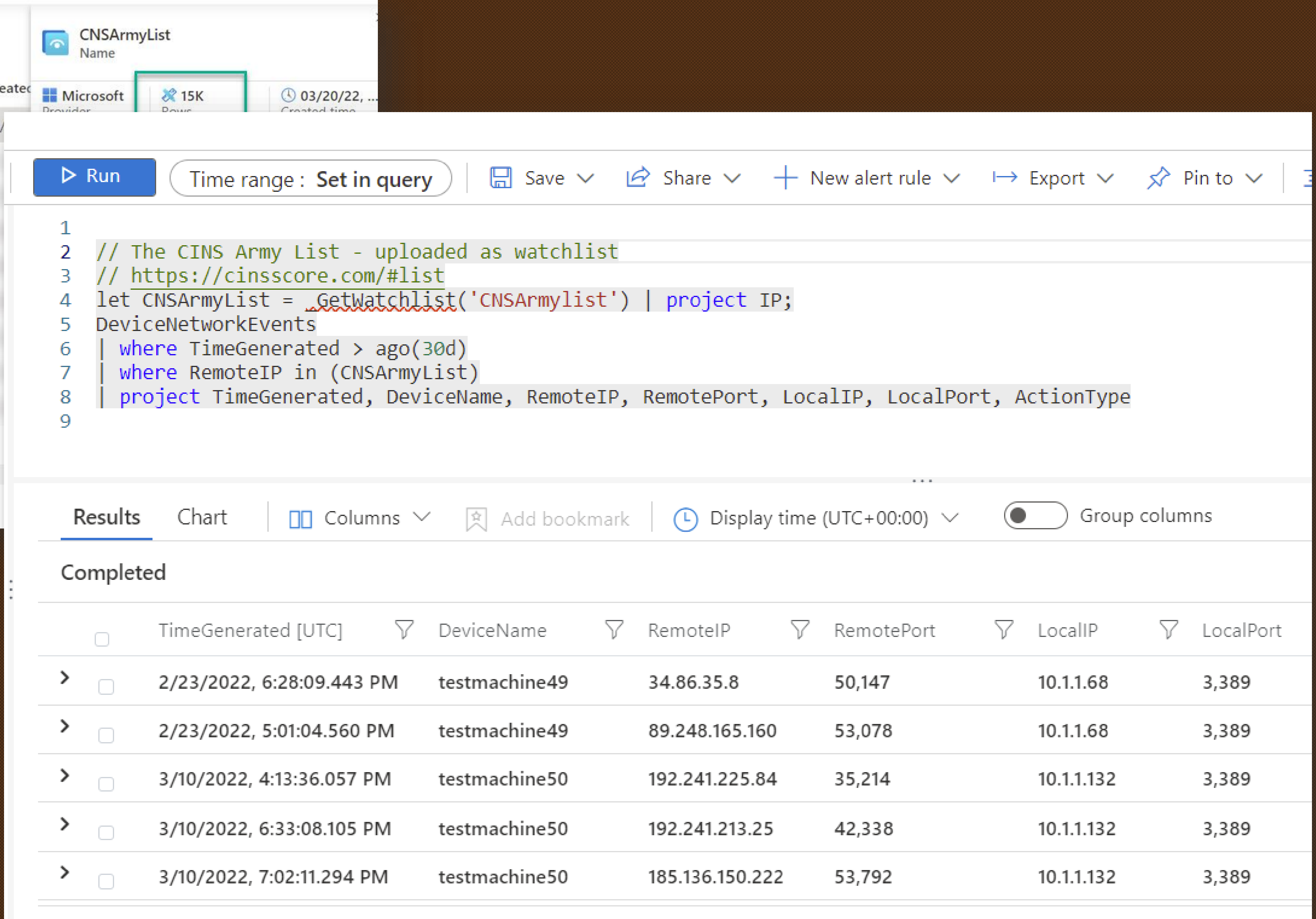
# Create a large watchlist from file in Azure Storage (public preview)

Once we imported the data stored on Azure Storage, we can use the watchlist



| Name | Alias | Source | Created |
|---|---|---|---|
| CNSArmyList | CNSArmylist | ci-badguys.txt | 03/ |

Upload in progress. Watchlist data may not be available for queries until the status shows succeeded.



```
// The CINS Army List - uploaded as watchlist
// https://cinsscore.com/#list
let CNSArmyList = _GetWatchlist('CNSArmylist') | project IP;
DeviceNetworkEvents
| where TimeGenerated > ago(30d)
| where RemoteIP in (CNSArmyList)
| project TimeGenerated, DeviceName, RemoteIP, RemotePort, LocalIP, LocalPort, ActionType
```

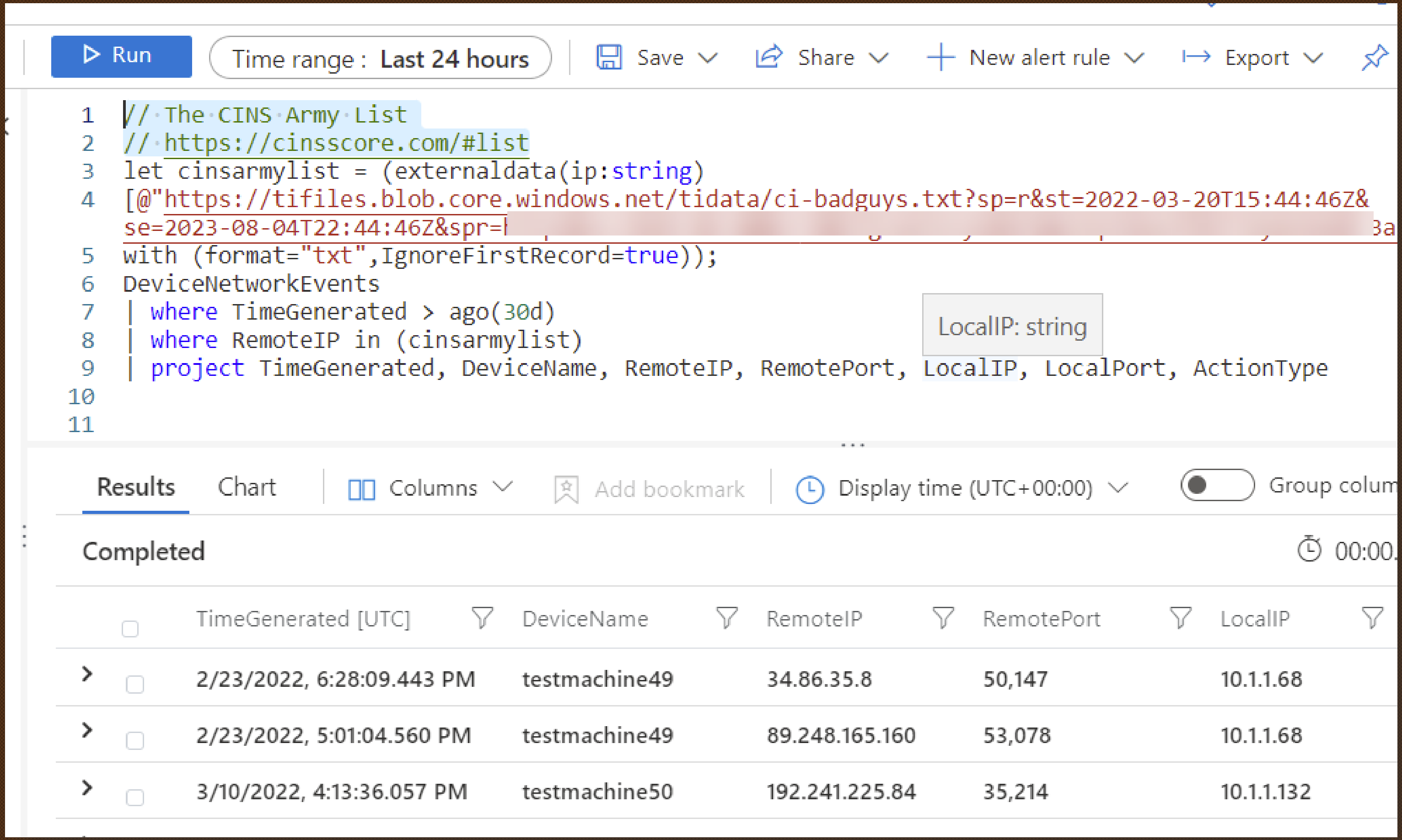
Completed

| TimeGenerated [UTC] | DeviceName | RemoteIP | RemotePort | LocalIP | LocalPort |
|---|---|---|---|---|---|
| 2/23/2022, 6:28:09.443 PM | testmachine49 | 34.86.35.8 | 50,147 | 10.1.1.68 | 3,389 |
| 2/23/2022, 5:01:04.560 PM | testmachine49 | 89.248.165.160 | 53,078 | 10.1.1.68 | 3,389 |
| 3/10/2022, 4:13:36.057 PM | testmachine50 | 192.241.225.84 | 35,214 | 10.1.1.132 | 3,389 |
| 3/10/2022, 6:33:08.105 PM | testmachine50 | 192.241.213.25 | 42,338 | 10.1.1.132 | 3,389 |
| 3/10/2022, 7:02:11.294 PM | testmachine50 | 185.136.150.222 | 53,792 | 10.1.1.132 | 3,389 |

```
AzureActivity
| where CategoryValue == "Administrative"
| where OperationNameValue has "/WATCHLISTS"
```

# Create a large watchlist from file in Azure Storage (public preview)

And of course we can also reference the file directly with externaldata



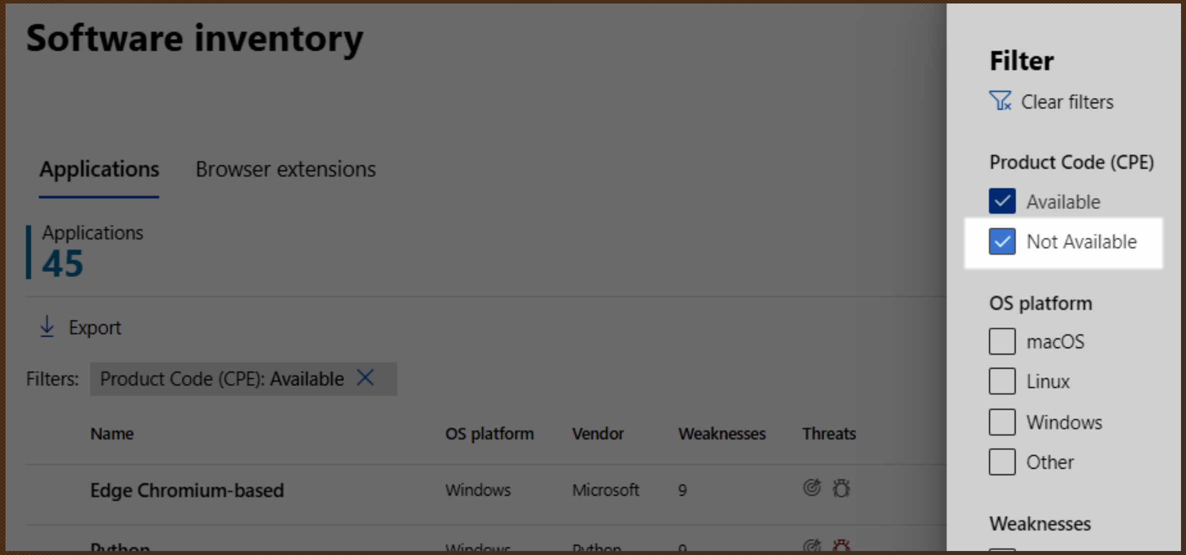
```
// The CINS Army List
// https://cinsscore.com/#list
let cinsarmylist = (externaldata(ip:string)
[@"https://tifiles.blob.core.windows.net/tidata/ci-badguys.txt?sp=r&st=2022-03-20T15:44:46Z&
se=2023-08-04T22:44:46Z&spr=[redacted]
with (format="txt",IgnoreFirstRecord=true));
DeviceNetworkEvents
| where TimeGenerated > ago(30d)
| where RemoteIP in (cinsarmylist)
| project TimeGenerated, DeviceName, RemoteIP, RemotePort, LocalIP, LocalPort, ActionType
```

Completed ⏱ 00:00.

| TimeGenerated [UTC] | DeviceName | RemoteIP | RemotePort | LocalIP |
|---|---|---|---|---|
| 2/23/2022, 6:28:09.443 PM | testmachine49 | 34.86.35.8 | 50,147 | 10.1.1.68 |
| 2/23/2022, 5:01:04.560 PM | testmachine49 | 89.248.165.160 | 53,078 | 10.1.1.68 |
| 3/10/2022, 4:13:36.057 PM | testmachine50 | 192.241.225.84 | 35,214 | 10.1.1.132 |

# DeviceTvmSoftwareInventory

```
DeviceTvmSoftwareInventory
| where ProductCodeCpe == @"Not Available"
| project SoftwareVendor, SoftwareName, SoftwareVersion
```



## Software inventory

Applications | Browser extensions

Applications
45

Export

Filters: Product Code (CPE): Available

| Name | OS platform | Vendor | Weaknesses | Threats |
|---|---|---|---|---|
| Edge Chromium-based | Windows | Microsoft | 9 | |
| Python | Windows | Python | 9 | |

**Filter**

Clear filters

Product Code (CPE)

☑ Available

☑ Not Available

OS platform

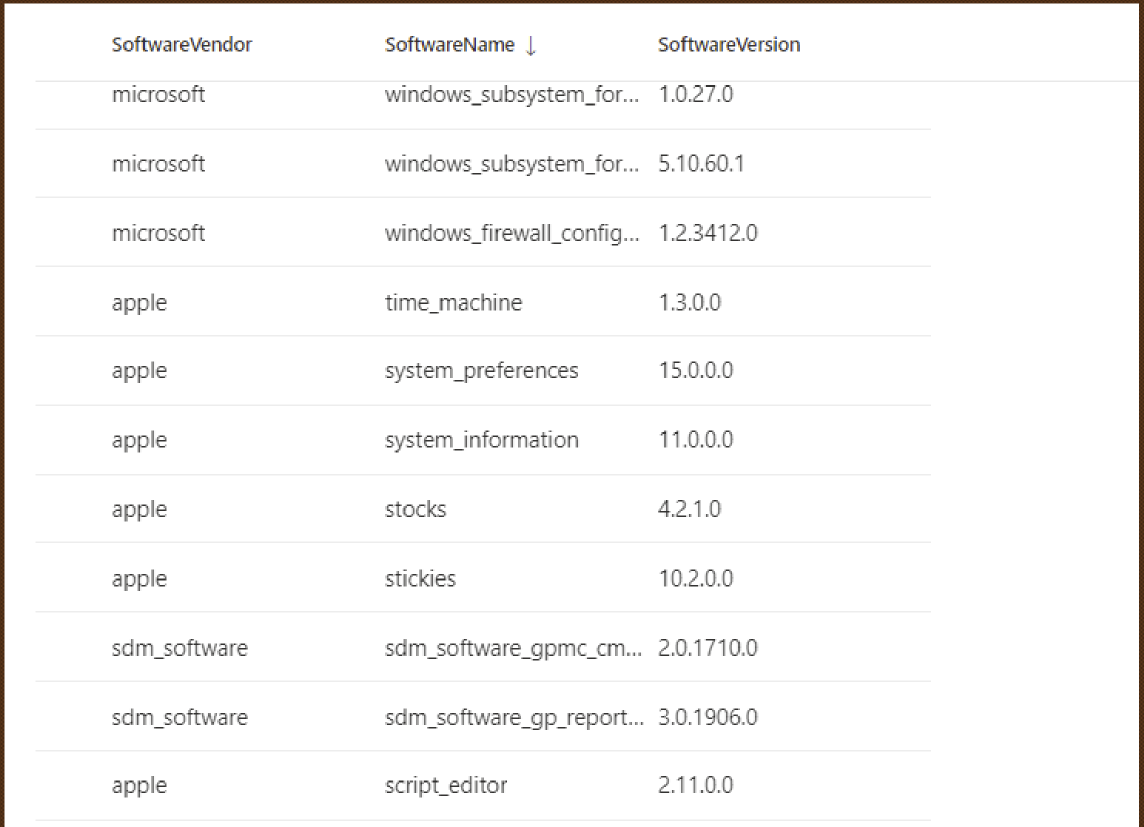
□ macOS

□ Linux

□ Windows

□ Other

Weaknesses



| SoftwareVendor | SoftwareName ↓ | SoftwareVersion |
|---|---|---|
| microsoft | windows_subsystem_for... | 1.0.27.0 |
| microsoft | windows_subsystem_for... | 5.10.60.1 |
| microsoft | windows_firewall_config... | 1.2.3412.0 |
| apple | time_machine | 1.3.0.0 |
| apple | system_preferences | 15.0.0.0 |
| apple | system_information | 11.0.0.0 |
| apple | stocks | 4.2.1.0 |
| apple | stickies | 10.2.0.0 |
| sdm_software | sdm_software_gpmc_cm... | 2.0.1710.0 |
| sdm_software | sdm_software_gp_report... | 3.0.1906.0 |
| apple | script_editor | 2.11.0.0 |

# Conti Leaks | Microsoft 365 Defender

## Vulnerability management

https://pastebin.com/raw/pv1mDGYC

kudos to @c3rb3ru5d3d53c

## Advanced hunting

https://ddanchev.blogspot.com/2022/02/exposing-conti-ransomware-gang-osint_28.html

kudos to @dancho_danchev

# Conti Leaks | Microsoft Sentinel

DNSEvents

Office 365

SigninLogs

# External Data

| | Watchlists | KQL functions | Custom tables | Externaldata |
|---|---|---|---|---|
| Size | 3.8MB / 500MB | 10000 characters | 500 columns wide and 500000 records long or 64MB (query results) | Large |
| Cost | Free | Free | Ingestion and Sentinel | Depending of locations |
| Data | CSV / Multiple | Multiple | Multiple | Multiple |
| Performance | Fastest | Fastest | Fast | Slower |

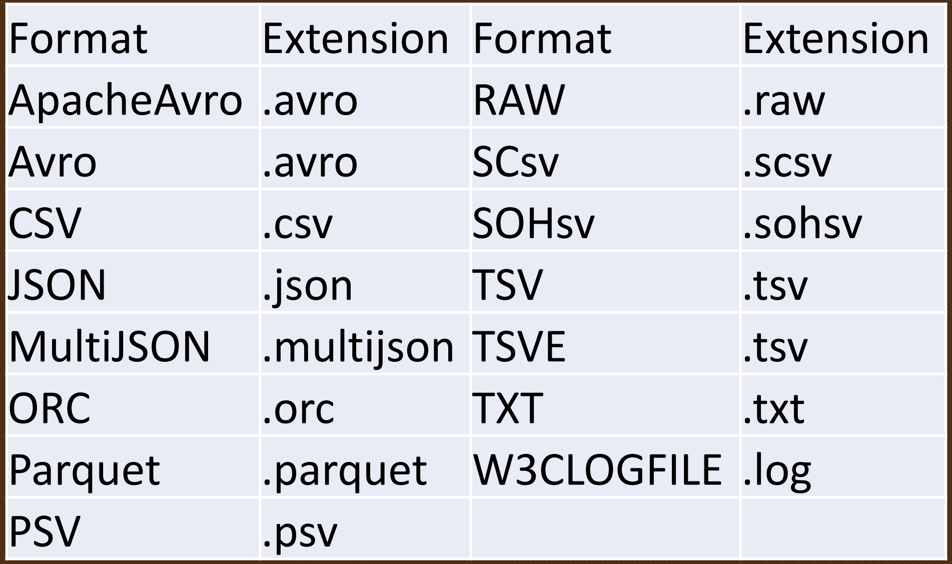
# Externaldata

Externaldata

Column Names and data types

StorageConnectionString

Properties

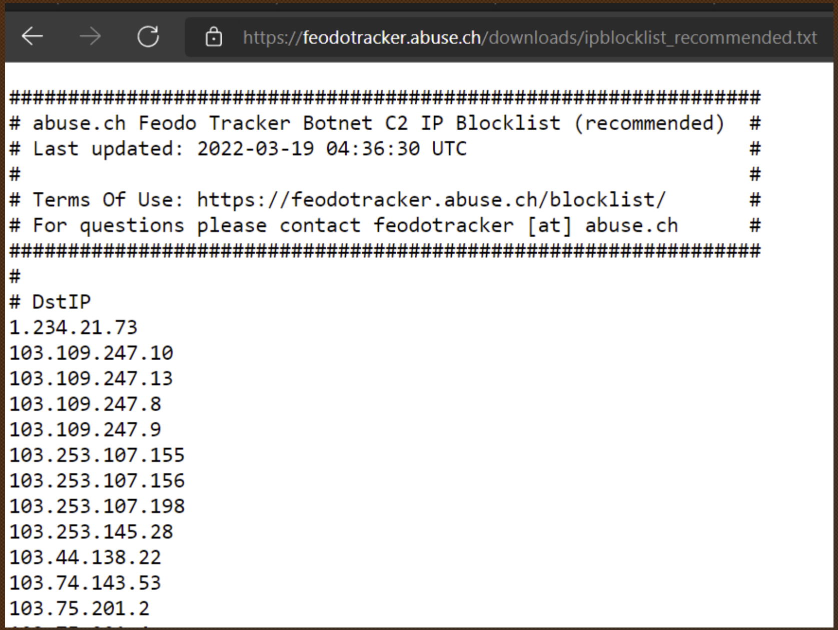


| Format | Extension | Format | Extension |
|---|---|---|---|
| ApacheAvro | .avro | RAW | .raw |
| Avro | .avro | SCsv | .scsv |
| CSV | .csv | SOHsv | .sohsv |
| JSON | .json | TSV | .tsv |
| MultiJSON | .multijson | TSVE | .tsv |
| ORC | .orc | TXT | .txt |
| Parquet | .parquet | W3CLOGFILE | .log |
| PSV | .psv | | |

# Uncoder CTI

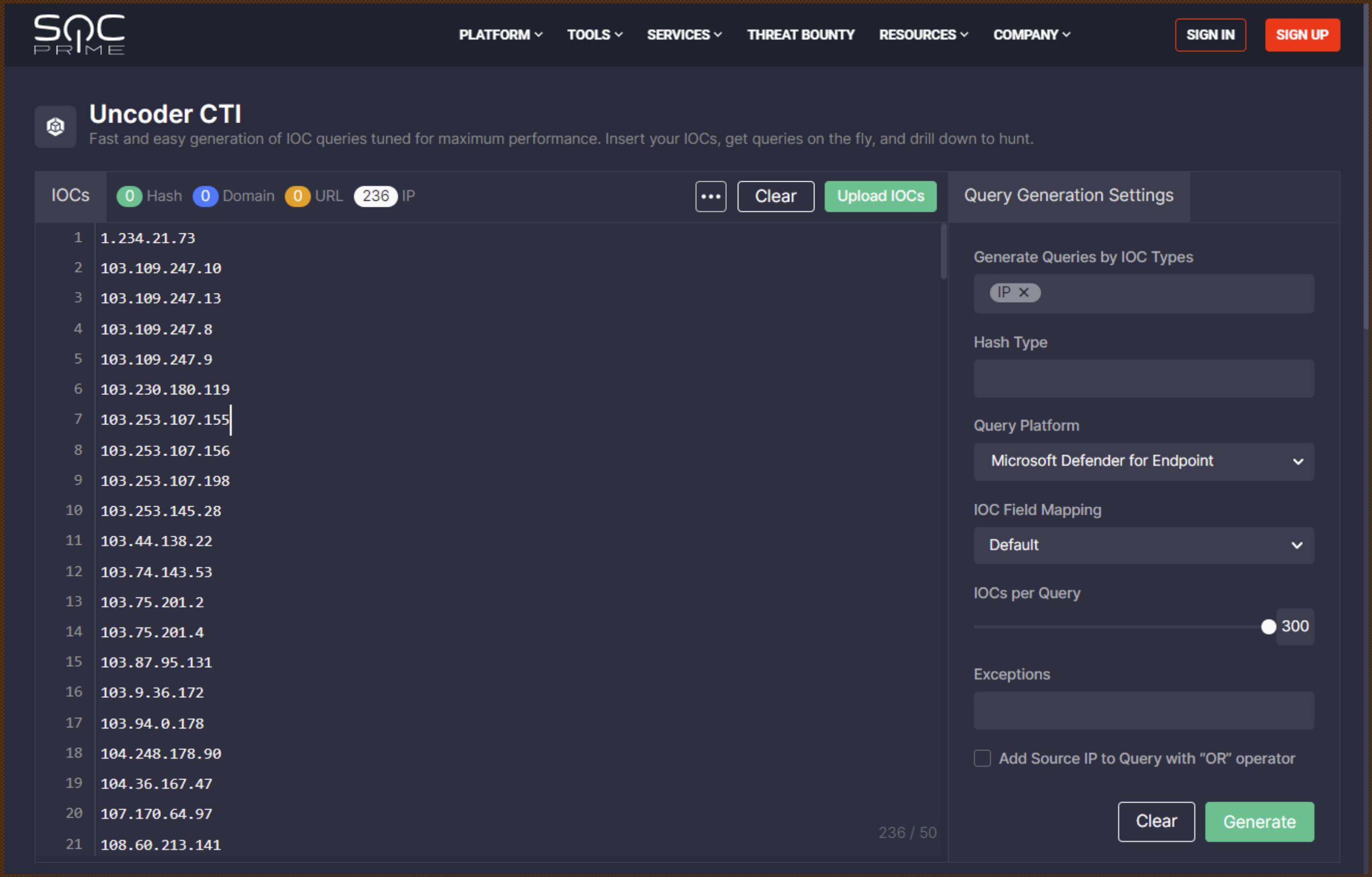
https://cti.uncoder.io/

Fast and easy generation of IOC queries tuned for maximum performance. Insert your IOCs, get queries on the fly, and drill down to hunt.



https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt

```
################################################################
# abuse.ch Feodo Tracker Botnet C2 IP Blocklist (recommended)  #
# Last updated: 2022-03-19 04:36:30 UTC                        #
#                                                              #
# Terms Of Use: https://feodotracker.abuse.ch/blocklist/       #
# For questions please contact feodotracker [at] abuse.ch      #
################################################################
#
# DstIP
1.234.21.73
103.109.247.10
103.109.247.13
103.109.247.8
103.109.247.9
103.253.107.155
103.253.107.156
103.253.107.198
103.253.145.28
103.44.138.22
103.74.143.53
103.75.201.2
```



## Uncoder CTI

Fast and easy generation of IOC queries tuned for maximum performance. Insert your IOCs, get queries on the fly, and drill down to hunt.

IOCs: 0 Hash, 0 Domain, 0 URL, 236 IP

```
1.234.21.73
103.109.247.10
103.109.247.13
103.109.247.8
103.109.247.9
103.230.180.119
103.253.107.155
103.253.107.156
103.253.107.198
103.253.145.28
103.44.138.22
103.74.143.53
103.75.201.2
103.75.201.4
103.87.95.131
103.9.36.172
103.94.0.178
104.248.178.90
104.36.167.47
107.170.64.97
108.60.213.141
```

236 / 50

Query Generation Settings

Generate Queries by IOC Types: IP

Hash Type:

Query Platform: Microsoft Defender for Endpoint

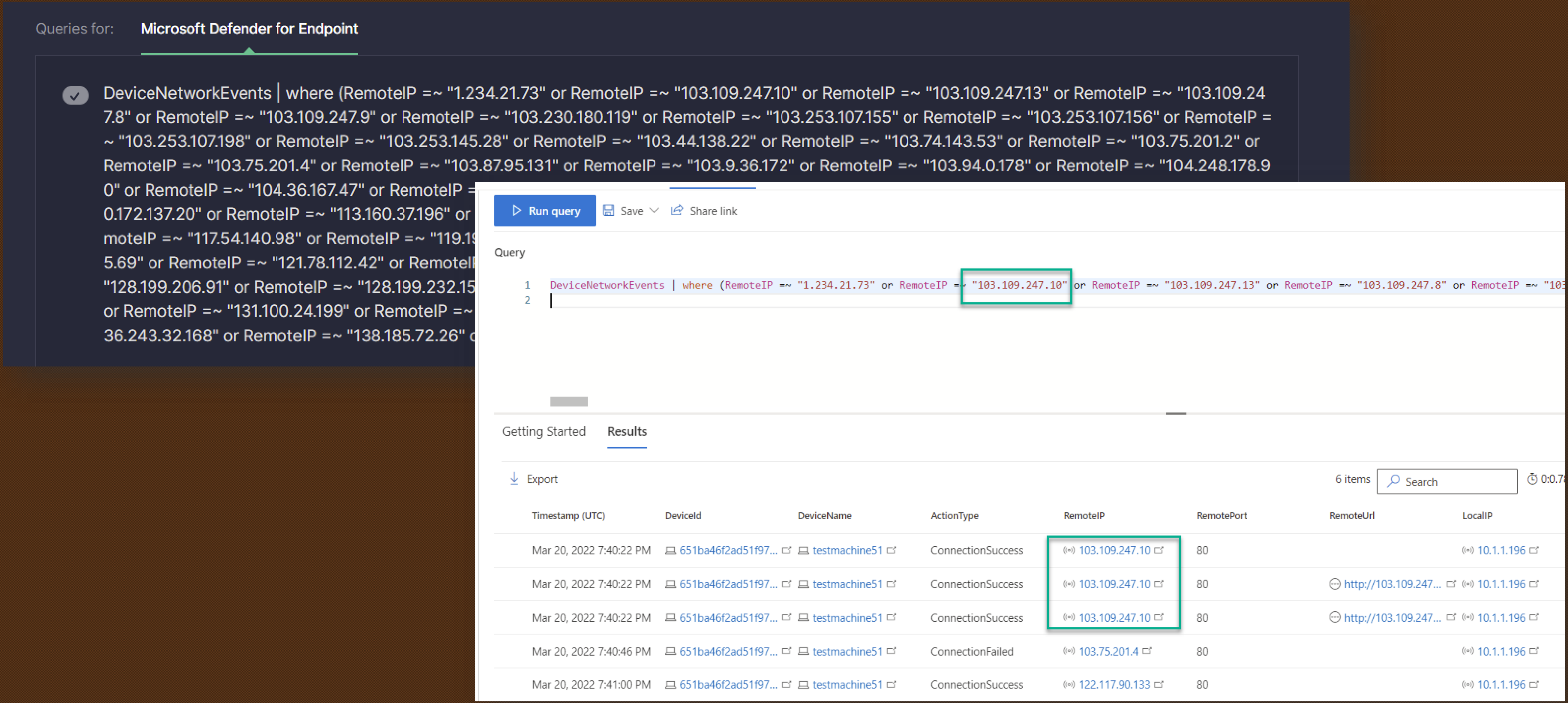
IOC Field Mapping: Default

IOCs per Query: 300

Exceptions:

□ Add Source IP to Query with "OR" operator

# Uncoder CTI



```
DeviceNetworkEvents | where (RemoteIP =~ "1.234.21.73" or RemoteIP =~ "103.109.247.10" or RemoteIP =~ "103.109.247.13" or RemoteIP =~ "103.109.24
7.8" or RemoteIP =~ "103.109.247.9" or RemoteIP =~ "103.230.180.119" or RemoteIP =~ "103.253.107.155" or RemoteIP =~ "103.253.107.156" or RemoteIP =
~ "103.253.107.198" or RemoteIP =~ "103.253.145.28" or RemoteIP =~ "103.44.138.22" or RemoteIP =~ "103.74.143.53" or RemoteIP =~ "103.75.201.2" or
RemoteIP =~ "103.75.201.4" or RemoteIP =~ "103.87.95.131" or RemoteIP =~ "103.9.36.172" or RemoteIP =~ "103.94.0.178" or RemoteIP =~ "104.248.178.9
0" or RemoteIP =~ "104.36.167.47" or RemoteIP =
0.172.137.20" or RemoteIP =~ "113.160.37.196" or
moteIP =~ "117.54.140.98" or RemoteIP =~ "119.1
5.69" or RemoteIP =~ "121.78.112.42" or RemoteI
"128.199.206.91" or RemoteIP =~ "128.199.232.15
or RemoteIP =~ "131.100.24.199" or RemoteIP =~
36.243.32.168" or RemoteIP =~ "138.185.72.26" c
```

```
DeviceNetworkEvents | where (RemoteIP =~ "1.234.21.73" or RemoteIP =~ "103.109.247.10" or RemoteIP =~ "103.109.247.13" or RemoteIP =~ "103.109.247.8" or RemoteIP =~ "103
```

6 items

| Timestamp (UTC) | DeviceId | DeviceName | ActionType | RemoteIP | RemotePort | RemoteUrl | LocalIP |
|---|---|---|---|---|---|---|---|
| Mar 20, 2022 7:40:22 PM | 651ba46f2ad51f97... | testmachine51 | ConnectionSuccess | 103.109.247.10 | 80 | | 10.1.1.196 |
| Mar 20, 2022 7:40:22 PM | 651ba46f2ad51f97... | testmachine51 | ConnectionSuccess | 103.109.247.10 | 80 | http://103.109.247... | 10.1.1.196 |
| Mar 20, 2022 7:40:22 PM | 651ba46f2ad51f97... | testmachine51 | ConnectionSuccess | 103.109.247.10 | 80 | http://103.109.247... | 10.1.1.196 |
| Mar 20, 2022 7:40:46 PM | 651ba46f2ad51f97... | testmachine51 | ConnectionFailed | 103.75.201.4 | 80 | | 10.1.1.196 |
| Mar 20, 2022 7:41:00 PM | 651ba46f2ad51f97... | testmachine51 | ConnectionSuccess | 122.117.90.133 | 80 | | 10.1.1.196 |

# Today's | Guest

# Matt Lowe

Program Manager 2 at Microsoft

LinkedIn https://www.linkedin.com/in/matthew-lowe-13b61990/

Get Hands-On KQL

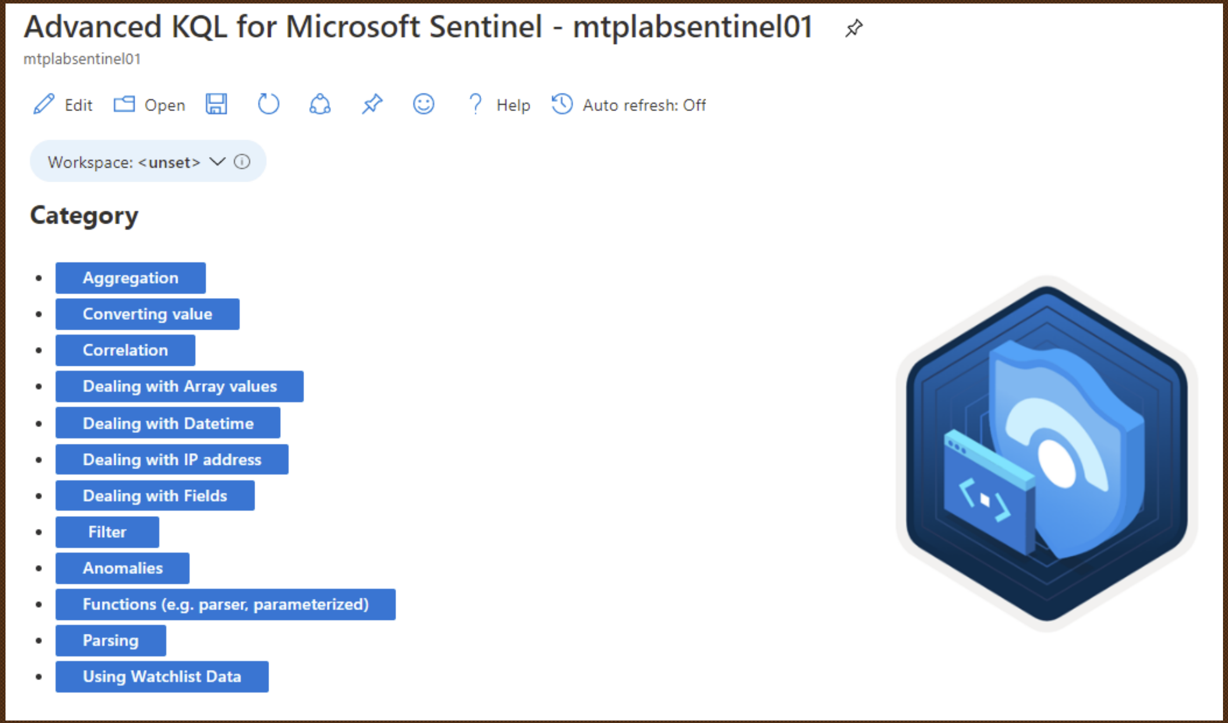
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/get-hands-on-kql-practice-with-this-microsoft-sentinel-workbook/ba-p/3055600

Advanced KQL Framework

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/advanced-kql-framework-workbook-empowering-you-to-become-kql/ba-p/3033766

Matt Lowe

# Microsoft Sentinel
# KQL Workbooks



## Advanced KQL for Microsoft Sentinel - mtplabsentinel01

mtplabsentinel01

Workspace: <unset>

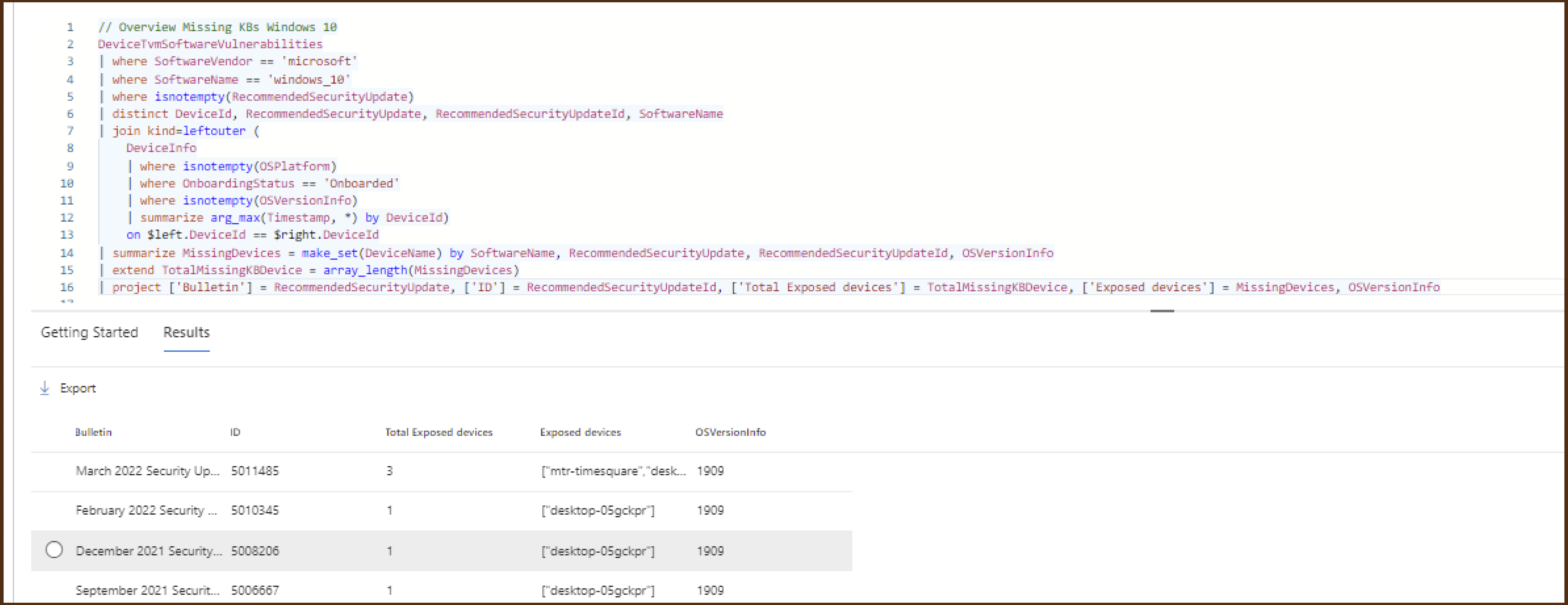
**Category**

- Aggregation
- Converting value
- Correlation
- Dealing with Array values
- Dealing with Datetime
- Dealing with IP address
- Dealing with Fields
- Filter
- Anomalies
- Functions (e.g. parser, parameterized)
- Parsing
- Using Watchlist Data

Our KQL Guest

Session 3 | KQL Workbooks

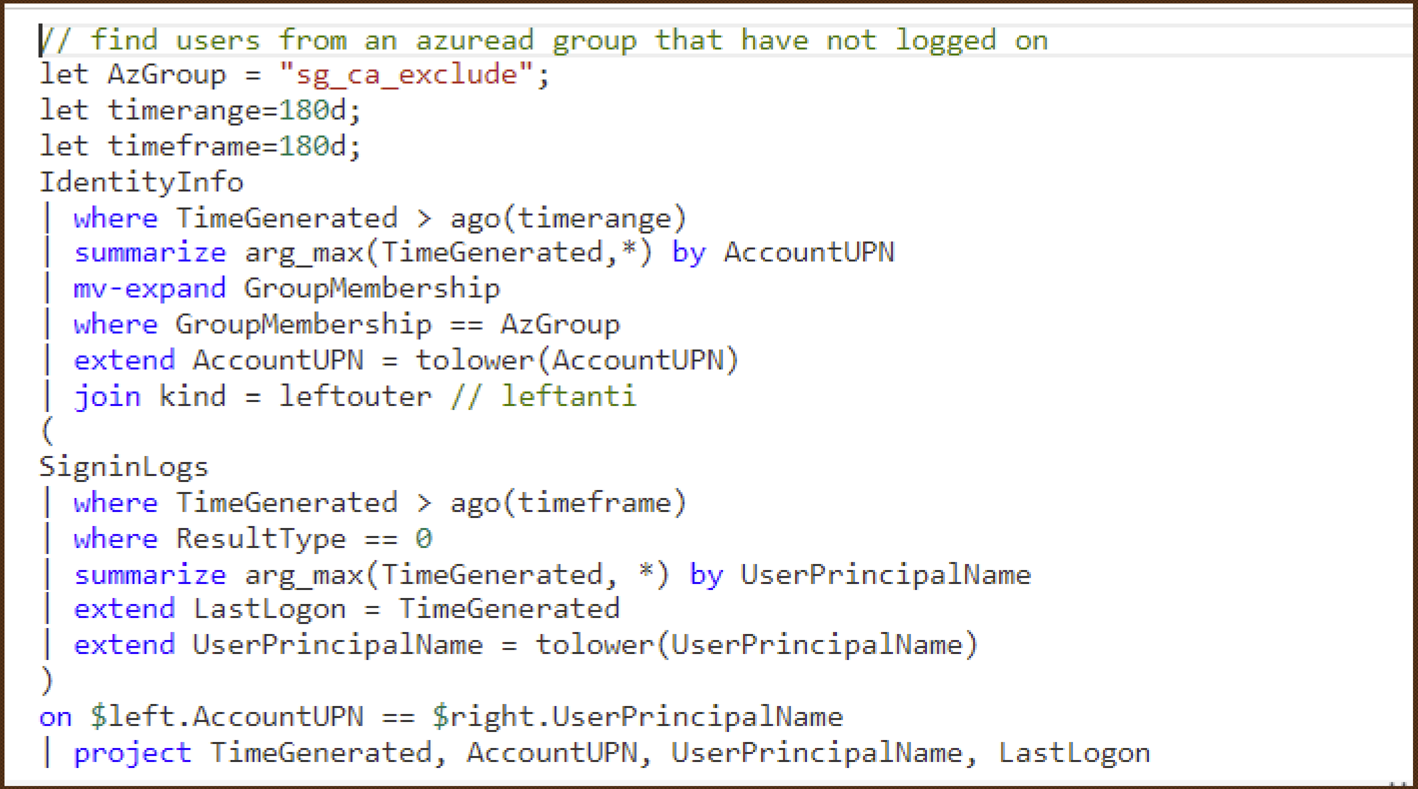
# Patch Management



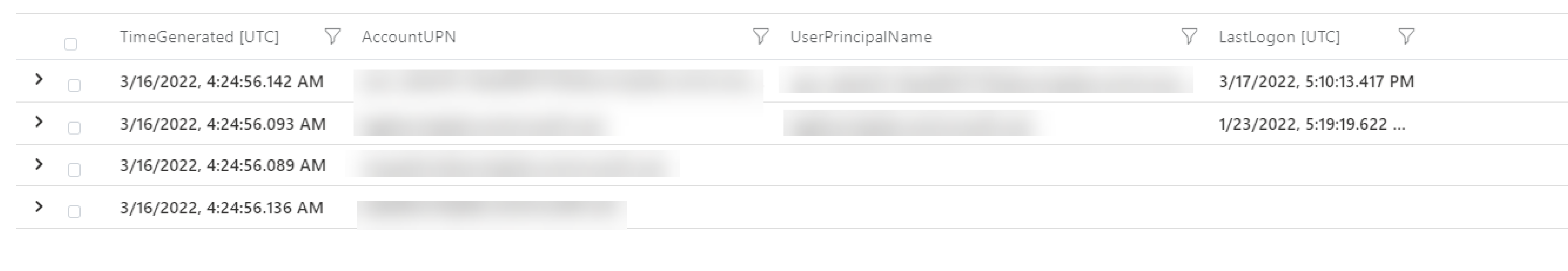
```
// Overview Missing KBs Windows 10
DeviceTvmSoftwareVulnerabilities
| where SoftwareVendor == 'microsoft'
| where SoftwareName == 'windows_10'
| where isnotempty(RecommendedSecurityUpdate)
| distinct DeviceId, RecommendedSecurityUpdate, RecommendedSecurityUpdateId, SoftwareName
| join kind=leftouter (
    DeviceInfo
    | where isnotempty(OSPlatform)
    | where OnboardingStatus == 'Onboarded'
    | where isnotempty(OSVersionInfo)
    | summarize arg_max(Timestamp, *) by DeviceId)
    on $left.DeviceId == $right.DeviceId
| summarize MissingDevices = make_set(DeviceName) by SoftwareName, RecommendedSecurityUpdate, RecommendedSecurityUpdateId, OSVersionInfo
| extend TotalMissingKBDevice = array_length(MissingDevices)
| project ['Bulletin'] = RecommendedSecurityUpdate, ['ID'] = RecommendedSecurityUpdateId, ['Total Exposed devices'] = TotalMissingKBDevice, ['Exposed devices'] = MissingDevices, OSVersionInfo
```

| | Bulletin | ID | Total Exposed devices | Exposed devices | OSVersionInfo |
|---|---|---|---|---|---|
| | March 2022 Security Up... | 5011485 | 3 | ["mtr-timesquare","desk... | 1909 |
| | February 2022 Security ... | 5010345 | 1 | ["desktop-05gckpr"] | 1909 |
| ○ | December 2021 Security... | 5008206 | 1 | ["desktop-05gckpr"] | 1909 |
| | September 2021 Securit... | 5006667 | 1 | ["desktop-05gckpr"] | 1909 |

# Find last logon date of users in a specific AzureAD Group

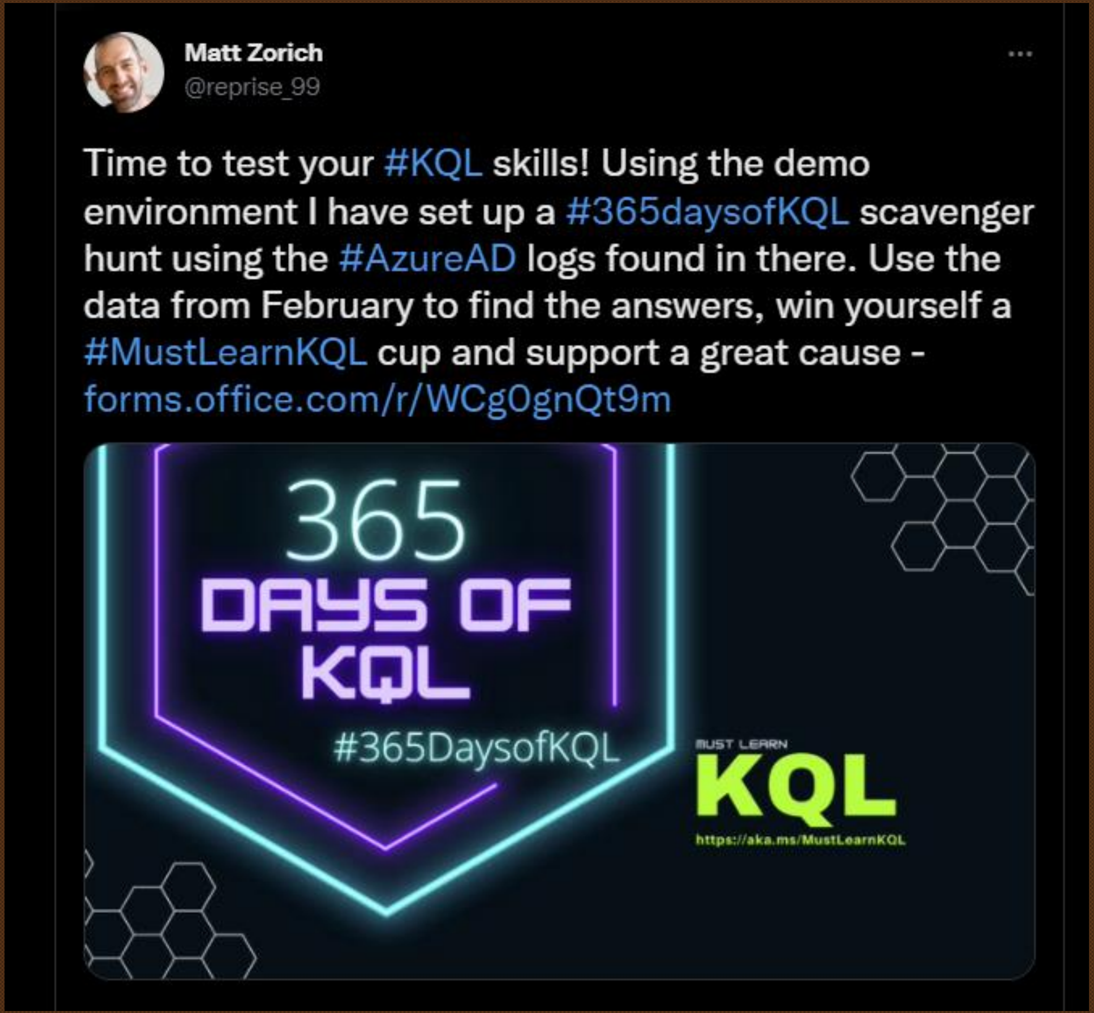


```
// find users from an azuread group that have not logged on
let AzGroup = "sg_ca_exclude";
let timerange=180d;
let timeframe=180d;
IdentityInfo
| where TimeGenerated > ago(timerange)
| summarize arg_max(TimeGenerated,*) by AccountUPN
| mv-expand GroupMembership
| where GroupMembership == AzGroup
| extend AccountUPN = tolower(AccountUPN)
| join kind = leftouter // leftanti
(
SigninLogs
| where TimeGenerated > ago(timeframe)
| where ResultType == 0
| summarize arg_max(TimeGenerated, *) by UserPrincipalName
| extend LastLogon = TimeGenerated
| extend UserPrincipalName = tolower(UserPrincipalName)
)
on $left.AccountUPN == $right.UserPrincipalName
| project TimeGenerated, AccountUPN, UserPrincipalName, LastLogon
```



| | | TimeGenerated [UTC] | AccountUPN | UserPrincipalName | LastLogon [UTC] |
|---|---|---|---|---|---|
| > | □ | 3/16/2022, 4:24:56.142 AM | [redacted] | [redacted] | 3/17/2022, 5:10:13.417 PM |
| > | □ | 3/16/2022, 4:24:56.093 AM | [redacted] | [redacted] | 1/23/2022, 5:19:19.622 ... |
| > | □ | 3/16/2022, 4:24:56.089 AM | [redacted] | | |
| > | □ | 3/16/2022, 4:24:56.136 AM | [redacted] | | |

# Challenge of the Month



Matt Zorich
@reprise_99

Time to test your #KQL skills! Using the demo environment I have set up a #365daysofKQL scavenger hunt using the #AzureAD logs found in there. Use the data from February to find the answers, win yourself a #MustLearnKQL cup and support a great cause - forms.office.com/r/WCg0gnQt9m

https://t.co/kl35p0Pj58

# Questions?

# Thanks for attending

KQL|Cafe