

Session 7 | Advanced KQL Techniques



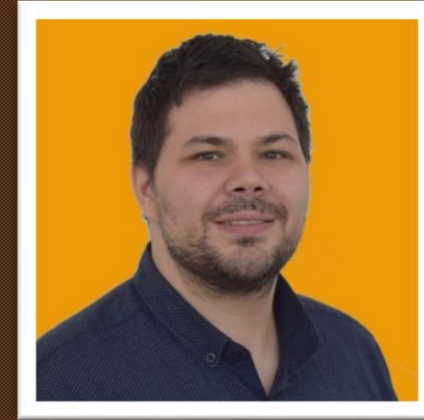
Session 7 | Advanced KQL Techniques

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/>

Session 7 | Advanced KQL
Techniques

Today's | Guest

Ashwin Patil



Senior Security Researcher, Microsoft Threat Intelligence Center

<https://twitter.com/ashwinpatil>

[ashwin-patil/blue-teaming-with-kql: Repository with Sample KQL Query examples for Threat Hunting \(github.com\)](#)

Session 7 | Advanced KQL
Techniques

Show | Agenda

Welcome

Whats New

TimeStamp - TimeGenerated

Sentinel – Data Retention, Archive & Restore

Guided Hunting in Microsoft 365 Defender

Working with IOCs

Learning KQL - parse-kv

Our KQL Guest

What did you do with KQL this month?

Session 7 | Advanced KQL
Techniques

Sentinel – Data Retention , Archive and Restore

The screenshot displays the Microsoft Azure portal interface for a Log Analytics workspace named 'MTPLabSentinel01'. The left-hand navigation pane includes sections for 'General' (Workspace summary, Workbooks, Logs, Solutions, Usage and estimated costs, Properties, Service Map) and 'Workspace Data Sources' (Virtual machines). The 'Tables (preview)' section is active, showing a list of 111 tables. The 'DeviceLogonEvents' table is selected, and its settings are displayed on the right.

DeviceLogonEvents

Description
This table is part of Microsoft Defender for Endpoints with Azure Sentinel. This table contains Sign-ins and other authentication events.

Table plan ⓘ
Analytics

Data retention settings

Workspace settings ⓘ
☒ Use default workspace settings

Interactive retention ⓘ
90 days

Total retention period ⓘ
180 days

Archive period of 90 days ⓘ
A progress bar shows the distribution of data retention: Interactive retention (blue) and Archive period (red). The legend indicates: ● Interactive retention ● Archive period.

Data collection rules ⓘ
N/A

Table name	Type
ContainerServiceLog	Azure table
DeviceEvents	Azure table
DeviceFileCertificateInfo	Azure table
DeviceFileEvents	Azure table
DeviceImageLoadEvents	Azure table
DeviceInfo	Azure table
DeviceLogonEvents	Azure table
DeviceNetworkEvents	Azure table

Sentinel – Data Retention , Archive and Restore

```
DeviceLogonEvents  
| where TimeGenerated between (datetime(2022-05-01) .. datetime(2022-08-30))
```

```
DeviceLogonEvents_8373182_SRCH  
| project-reorder _OriginalTimeGenerated, TimeGenerated
```

```
DeviceLogonEvents_8171567_RST  
| where TimeGenerated between (datetime(2022-03-01) .. datetime(2022-05-30))
```

```
DeviceLogonEvents_8171567_RST  
| where TimeGenerated between (datetime(2022-03-01) .. datetime(2022-05-30))  
| summarize arg_min(TimeGenerated,*)
```

```
DeviceLogonEvents_8171567_RST  
| where TimeGenerated between (datetime(2022-03-01) .. datetime(2022-05-30))  
| summarize arg_max(TimeGenerated,*)
```

Defender 365 Guided Hunting

The screenshot shows the 'Advanced Hunting' interface in Microsoft Defender 365. At the top, there's a header with 'Advanced Hunting' and navigation links for 'Help resources', 'Schema reference', and a toggle for 'Try the new Hunting page'. Below the header, there's a toolbar with 'New query' (twice), 'Create new', 'Run query', 'Save', and 'Share link'. The main area displays a query: 'Endpoints' and 'Changes to local group'. Below the query, there's a filter section with a toggle for 'All filters' and a 'Filter' button. The filter is set to 'AND' and contains a single condition: 'Device events: EventType equals DeviceEvents: UserAccountAd...'. There are also buttons for 'Add filter' and 'Add subgroup'. On the right side of the main area, there are additional controls: 'Sample size: 10', 'Last 7 days', 'Create detection rule', and 'Edit in KQL'.

<https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/hunt-in-microsoft-365-defender-without-kql/ba-p/3607989>

IOCs

<https://www.spamhaus.org/statistics/botnet-asn/>

The 10 Worst Botnet ASNs

As of 30 August 2022 the world's worst botnet infected Autonomous System Numbers are:

1	AS4134 China_Telecom_(ChinaNet)	Number of Bots: 489597
2	AS16509 AMAZON-02	Number of Bots: 344414
3	AS4837 China_Unicom	Number of Bots: 160583
4	AS45609 Bharti Airtel Ltd. AS for GPRS Service	Number of Bots: 155178
5	AS8452 TE_Data_SAE	Number of Bots: 112857
6	AS36947 Telecom_Algeria	Number of Bots: 97823
7	AS16135 Turkcell Iletisim Hizmetleri A.s.	Number of Bots: 96666
8	AS7713 PT_Telekomunikasi_Indonesia	Number of Bots: 92561
9	AS24560 Bharti_Airtel_Ltd._Telemedia_Services	Number of Bots: 78554
10	AS14618 NAME_NO_LONGER_AVAILABLE	Number of Bots: 64991

Learning KQL – parse-kv

- Faster
- Less complex
- Less error prone
- Cleaner KQL

Learning KQL – Microsoft learn

<https://docs.microsoft.com/en-us/learn/browse/?expanded=azure&terms=kusto%20query%20language>

The screenshot shows the Microsoft Learn search interface. On the left is a sidebar with filters for Products, Roles, Levels, and Subjects. The main area displays search results for 'kusto query language'. The search bar contains the text 'kusto query language' and a search button. Below the search bar, it says '5 results for "kusto query language"'. There are five result cards. The first card is a 'LEARNING PATH' titled 'SC-200: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)' with a duration of 2 hr 3 min and a 'Save' button. The second card is a 'MODULE' titled 'Work with data in Microsoft Sentinel using Kusto Query Language' with a duration of 36 min, a rating of 4.7 (614), and a 'Save' button. The third card is a 'MODULE' titled 'Write your first query with Kusto Query Language' with a duration of 39 min, a rating of 4.9 (182), and a 'Save' button. The fourth card is a 'MODULE' titled 'Locate threats using advanced hunting with Microsoft 365 Defender' with a duration of 30 min, a rating of 4.8 (62), and a 'Save' button. The fifth card is a 'MODULE' titled 'Gain insights from your data by using Kusto Query Language' with a duration of 48 min, a rating of 4.7 (28), and a 'Save' button. The sidebar filters include: Products (Azure, Data Explorer, Microsoft Sentinel, Microsoft 365), Roles (Business Analyst, Data Analyst, Data Scientist, Developer, Security Engineer, Security Operations Analyst), Levels (Beginner, Intermediate), and Subjects (Data and AI, Security).

Filter

Products

- ☐ Azure
 - ☐ Data Explorer
 - ☐ Microsoft Sentinel
- ☒ Microsoft 365

Roles

- ☐ Business Analyst
- ☐ Data Analyst
- ☐ Data Scientist
- ☐ Developer
- ☐ Security Engineer
- ☐ Security Operations Analyst

Levels

- ☐ Beginner
- ☐ Intermediate

Subjects

- ☒ Data and AI
- ☒ Security

Search results for "kusto query language"

LEARNING PATH
SC-200: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
2 hr 3 min
Azure Security Operations Analyst
Intermediate
Save

MODULE
Work with data in Microsoft Sentinel using Kusto Query Language
36 min ★★★★★ 4.7 (614)
Azure Security Operations Analyst
Intermediate
Save

MODULE
Write your first query with Kusto Query Language
39 min ★★★★★ 4.9 (182)
Azure Data Scientist Beginner
Save

MODULE
Locate threats using advanced hunting with Microsoft 365 Defender
30 min ★★★★★ 4.8 (62)
Microsoft 365 Security Engineer Beginner
Save

MODULE
Gain insights from your data by using Kusto Query Language
48 min ★★★★★ 4.7 (28)
Azure Business Analyst Intermediate
Save

KQL Quest: Ashwin Patil



Senior Security Researcher, Microsoft Threat Intelligence Center

<https://twitter.com/ashwinpatil>

[ashwin-patil/blue-teaming-with-kql: Repository with Sample KQL Query examples for Threat Hunting \(github.com\)](#)

What did you do with KQL this month?

IP Addresses, IP Ranges
Azure-Threat-Research-Matrix-KQL

Questions?

Thanks for attending

