

KQL Café | March 2024

# 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** | Cafe

Show | Agenda

Welcome

What is new/updates for KQL

Our guest: Purav Desai

Learning KQL

What did you do with KQL this month?

## News

A Common KQL Mistake in Threat Hunting and Detection Engineering

<https://posts.bluraven.io/a-common-kql-mistake-in-threat-hunting-and-detection-engineering-61053b4f3308>

Microsoft Security Exposure Management

<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/introducing-microsoft-security-exposure-management/ba-p/4080907>

Unraveling the Mysteries of Kusto's Parse-Kv Operator: A Deep Dive

<https://www.linkedin.com/pulse/unraveling-mysteries-kustos-parse-kv-operator-deep-dive-naveen-matthi-fdz7c/>

Our Guest:



Purav Desai

<https://www.linkedin.com/in/purav-da346393/>

<https://github.com/PuravsPoint>

<https://github.com/PuravsPoint/DecipheringUAL>

# Learning KQL

## Datatables and Scoring

<input type="checkbox"/> AlertSeverity	Score
<input type="checkbox"/> > Informational	1
<input type="checkbox"/> > Low	3
<input type="checkbox"/> > Medium	5
<input type="checkbox"/> > High	8

# Learning KQL

## Security Exposure Management

### Schema

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-exposuregraphnodes-table?view=o365-worldwide>

<https://learn.microsoft.com/en-us/security-exposure-management/schemas-operators>

[Query the enterprise exposure graph in Microsoft Security Exposure Management - Microsoft Security Exposure Management | Microsoft Learn](#)



What did you do with KQL this month?

Microsoft Security Exposure Management - Remote Desktop Protocol (RDP)

<https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/ExposureManagement/EEG-RDP.md>

Microsoft Security Exposure Management - Managed Identity

<https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/ExposureManagement/EEG-ManagedIdentity.md>

Microsoft Security Exposure Management – Critical Assets

<https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/ExposureManagement/EEG-CriticalAssets.md>

# What did you do with KQL this month?

## Parse Netsh advfirewall commands

[https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Endpoint/DefenderFirewall/MDE-  
ParseNetsh.md](https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Endpoint/DefenderFirewall/MDE-ParseNetsh.md)

↓ Export

<input type="checkbox"/>	actionname	name	program	protocol	dir	action	localport	enable	rule name	profile	ProcessCommandLine
<input type="checkbox"/>	> set	winamp	c:\program files (x86)\winamp\winamp.exe	tcp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
<input type="checkbox"/>	> add	winamp	c:\program files (x86)\winamp\winamp.exe	tcp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
<input type="checkbox"/>	> set	winamp	c:\program files (x86)\winamp\winamp.exe	udp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
<input type="checkbox"/>	> add	winamp	c:\program files (x86)\winamp\winamp.exe	udp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
<input type="checkbox"/>	> delete	winamp	c:\program files (x86)\winamp\winamp.exe						winamp		netsh advfirewall firewall...

# What did you do with KQL this month?

## Stream and filter data from Windows DNS servers with the AMA connector

<https://learn.microsoft.com/en-us/azure/sentinel/connect-dns-ama>

## Filtering DNS Events

The screenshot shows the configuration page for the 'Windows DNS Events via AMA' connector in Microsoft Sentinel. The page is divided into two main sections: a left-hand pane with details and a right-hand pane with instructions and configuration options.

**Left-hand pane details:**

- Header:** Windows DNS Events via AMA
- Connected Status:** Microsoft Provider, Last Log Received: --
- Description:** The Windows DNS log connector allows you to easily filter and stream all analytics logs from your Windows DNS servers to your Azure Sentinel workspace using the Azure Monitoring agent (AMA). Having this data in Azure Sentinel helps you identify issues and security threats such as:
  - Trying to resolve malicious domain names.
  - Stale resource records.
  - Frequently queried domain names and talkative DNS clients.
  - Attacks performed on DNS server.
- You can get the following insights into your Windows DNS servers from Azure Sentinel:**
  - All logs centralized in a single place.
  - Request load on DNS servers.
  - Dynamic DNS registration failures.
- Windows DNS events are supported by Advanced SIEM Information Model (ASIM) and stream data into the ASimDnsActivityLogs table.** [Learn more](#)
- Last data received:** --

**Right-hand pane details:**

- Instructions:** To integrate with Windows DNS Events via AMA make sure you have:
  - ✓ **Workspace data sources:** read and write permissions.
  - ❗ To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. [Learn more](#)
- Configuration:**
  - Enable data collection rule**
    - DNS logs are collected only from **Windows** agents.
    - 1 resources were selected
    - [Edit data collection rule](#)
  - Define data collection filters to exclude events**
    - [+Add data collection filters](#)
- Buttons:** [Apply changes](#), [Delete data collection rule](#)

Thanks for attending



**KQL** | Cafe