KQL Café | March 2024

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/


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

AlertSeverity	Score
Informational	1
Low	3
Medium	5
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

Export

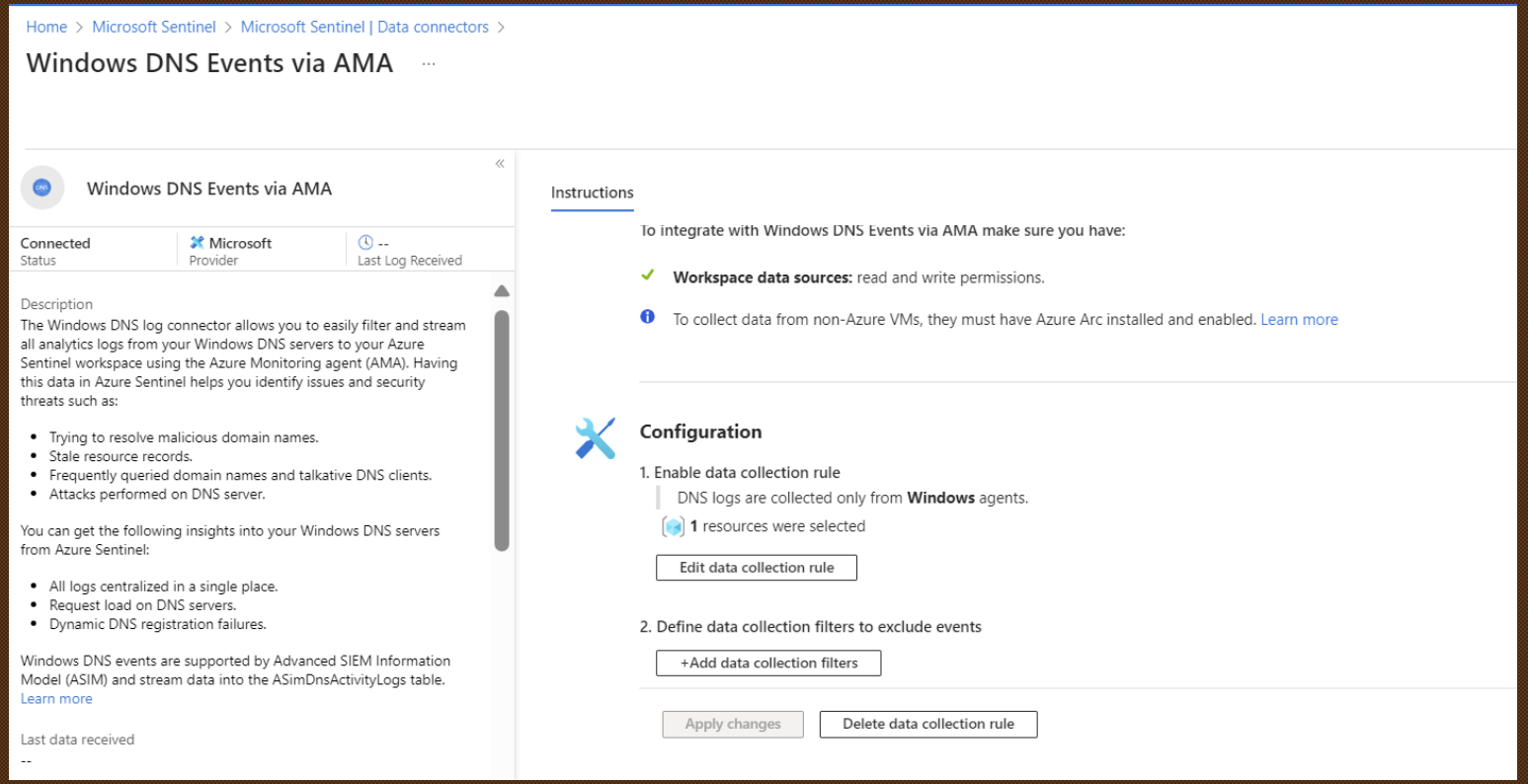
actionname	name	program	protocol	dir	action	localport	enable	rule name	profile	ProcessCommandLine
set	winamp	c:\program files (x86)\winamp\winamp.exe	tcp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
add	winamp	c:\program files (x86)\winamp\winamp.exe	tcp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
set	winamp	c:\program files (x86)\winamp\winamp.exe	udp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
add	winamp	c:\program files (x86)\winamp\winamp.exe	udp	in	allow		yes	winamp	private,public	netsh advfirewall firewall...
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)

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

Filtering DNS Events



Thanks for attending