KQL Cafe

Michalis Michalos, June 25th, 2024

About me

- Currently working as Cyber Resilience & Intelligence Manager
- Over 11 years experience in ICT
- Working in Cybersecurity since 2019
- Electrical Engineer BSc, MSc, MBA
- Father of 2, lifetime Scout, own a wine cooler, and a watch enthusiast

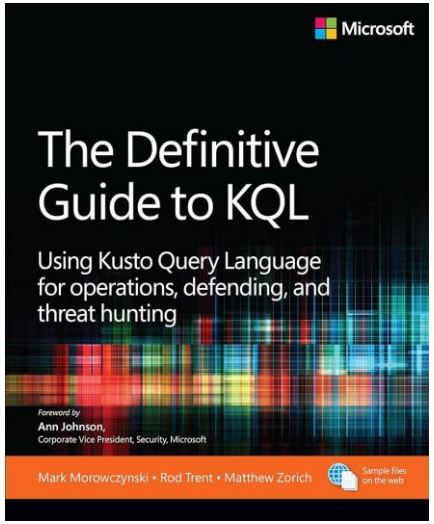
Projects

- Blogging at michalos.net
- github.com/cyb3rmik3/KQL-threat-hunting-queries
- github.com/cyb3rmik3/MDE-DFIR-Resources
- github.com/cyb3rmik3/Hunting-Lists (mostly a sidekick)

KQL Search

Search engine for KQL Queries

Kusto Insights



Keeping an eye on WSL through MDE

Microsoft definitely loves Linux.

What is WSL?

Windows Subsystem for Linux (WSL) is a feature of Windows that allows you to run a Linux environment on your Windows machine, without the need for a separate virtual machine or dual booting.

WSL is designed to provide a seamless and productive experience for developers who want to use both Windows and Linux at the same time.

Why should I care?

- Stack Overflow reported 15.68% of developers use WSL
- Bashware malware already available since 2017
- Almost 100 different malware associated to WSL reported in 2022
- WSL is generally limited to power users, those users often have elevated privileges in an organization.

Identify & Deploy

- KQL to identify associated endpoints
- Straightforward procedure to onboard

  https://learn.microsoft.com/en-us/defender-endpoint/mde-plugin-wsl

Let’s go hunt!

- DeviceNetworkInfo
- DeviceInfo
- ***DeviceNetworkEvents***
- ***DeviceFileEvents***
- ***DeviceProcessEvents***
- DeviceEvents
- DeviceTvmSoftwareEvidenceBeta
- DeviceTvmInfoGathering
- DeviceTvmSecureConfigurationAssessment
- DeviceTvmSoftwareInventory
- ExposureGraphNodes

Considerations

- What about the host?
- Isolation
- Device tables and automation
- Asset visibility


Check
michalos.net
for more

Thank you

michalos.net

x.com/cyb3rmik3

Linkedin.com/in/mmihalos