Session 9-2023 | KQL Search

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/

KQL|Cafe

Show | Agenda

Welcome

What is new/updates for KQL

Our guest: Ugur Koc

What did you do with KQL this month?

What's New – Notable KQL Queries

Detect malware communication using SSL inspection
https://github.com/cyb3rmik3/KQL-threat-hunting-queries/blob/main/02.ThreatDetection/ssl-inspection-for-malware-cnc.md

Analysing MITRE ATT&CK Detection with KQL
https://github.com/LearningKijo/KQL/blob/main/KQL-Effective-Use/17-kql-MITRE-ATTCK-Detection.md

KQL Functions For Network Operations
https://kqlquery.com/posts/kql-for-network-operations/

DNS requests to suspicious TLDs
https://github.com/cyb3rmik3/KQL-threat-hunting-queries/blob/main/01.ThreatHunting/dns-requests-to-suspicious-tlds.md

Other News

The KQL Mysteries: Prologue
https://github.com/rod-trent/KQLMysteries

The KQL Mysteries is a fun, fictional story but with real-world educational impact.
Its A new, continuing way to learn KQL and expert approaches to security threats

Public Preview: Azure Log Alerts support for Azure Resource Graph (ARG)
https://azure.microsoft.com/en-us/updates/public-preview-azure-log-alerts-support-for-azure-resource-graph-arg/

Azure Monitor Data Collection API Retirement
https://azure.microsoft.com/en-us/updates/azure-monitor-data-collection-api-retirement/

KQL Training

Hands-On Kusto Query Language (KQL) for Security Analysts
https://academy.bluraven.io/

Learning KQL

as operator

Our Guest: Ugur Koc

https://twitter.com/UgurKocDe

What did you do with KQL this month?

ASR Revisited

Thanks for attending

KQL|Cafe