KQL Café | April 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: Henning Rauch
Learning KQL
What did you do with KQL this month?

News

Introduction to KQL for Security Analysis

Course - Lifetime Access (14-day lab access)

Learn the basics of KQL to start your journey into security investigations, threat hunting, and detection engineering with hands-on experience in a hyper-realistic lab environment! If you utilize Microsoft Sentinel or Microsoft Defender XDR and want to learn KQL, this course is for you!

This offering also serves as a preview of our comprehensive paid courses, providing a solid foundation for further learning.

The lab access starts immediately!

Certificate of Completion is included!

Enroll for Free
50 seats are made available every 1st and 15th of the month.

News

Hands-On KQL for Security Analysts

Elevate your security analysis skills with the Kusto Query Language (KQL) training course, offering hands-on experience in a hyper-realistic lab environment! Whether you're a security analyst or incident responder utilizing Microsoft Sentinel, Defender for Endpoint, or Microsoft 365 Defender XDR, or simply aspiring to master the KQL for security analysis, this course is for you!

Starting from €75

News

Steven Lim

Slim's Elite KQL Detection & Cyber Defense Tips

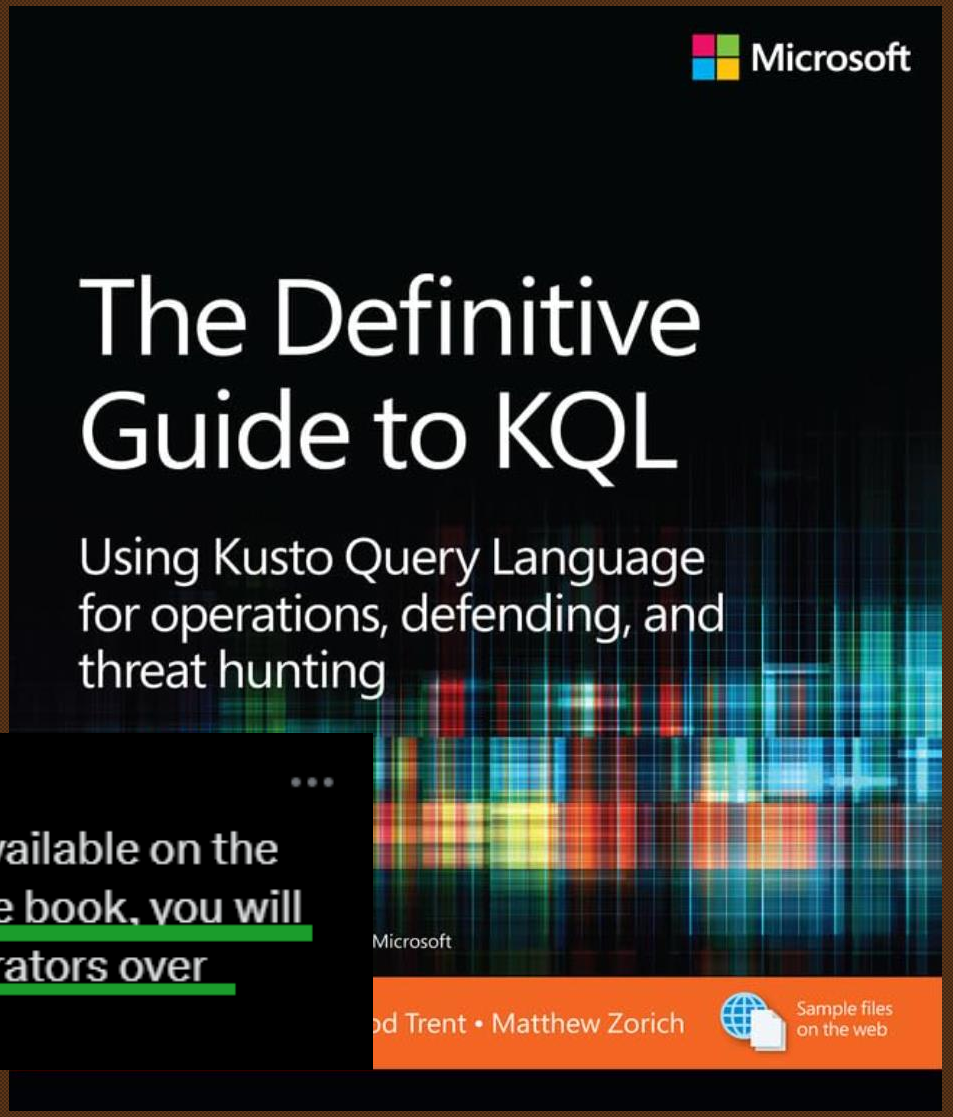
https://www.linkedin.com/pulse/slims-elite-kql-detection-cyber-defense-tips-steven-lim-wujbc/?trackingId=kmHuitogSda6wj0lk%2FtV%2Bg%3D%3D

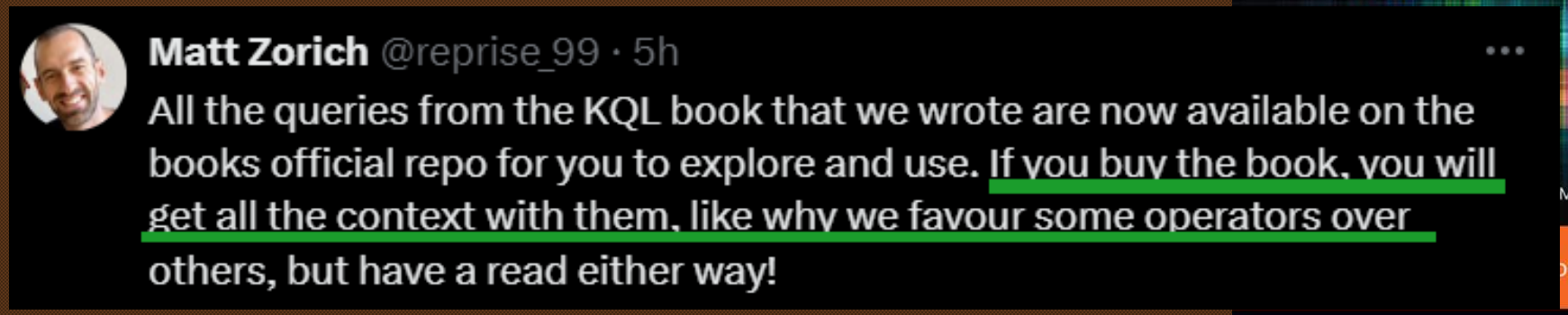
News

The Definitive Guide to KQL: Using Kusto Query Language for Operations, Defending and Threat Hunting

https://github.com/KQLMSPress/definitive-guide-kql

Chapter 1: Introduction	Add files via upload	2 weeks ago
Chapter 2: Data Aggregation	Add files via upload	2 weeks ago
Chapter 3: Advanced KQL	Add files via upload	2 weeks ago
Chapter 4: Operational Excellence	Add files via upload	2 weeks ago
Chapter 5: KQL for Cyber Security	Update 7. Ransomware TTPs.md	yesterday
Chapter 6: Advanced KQL for Cyber...	Add files via upload	2 weeks ago
Extra Microsoft Employee Submitte...	MSFT Employee Query Contributions	2 days ago





News

Strategies to monitor and prevent vulnerable driver attacks

Useful MDE queries

https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/strategies-to-monitor-and-prevent-vulnerable-driver-attacks/ba-p/4103985

Defender for Cloud (CSPM) (Jarkko Kinnunen)

KQL for Pricing

https://github.com/Jaekk0/Sentinel/blob/main/Random_Kql/az-resource-graph-list-cspm-enable-%26-price.kql

News

CloudAppEvents

New columns

- **LastSeenForUser** - Shows how many days back the attribute was recently in use by the user in days (i.e. ISP, ActionType etc.)

- **UncommonForUser** - Lists the attributes in the event that are uncommon for the user, using this data to help rule out false positives and find out anomalies

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

Our Guest:

Henning Rauch

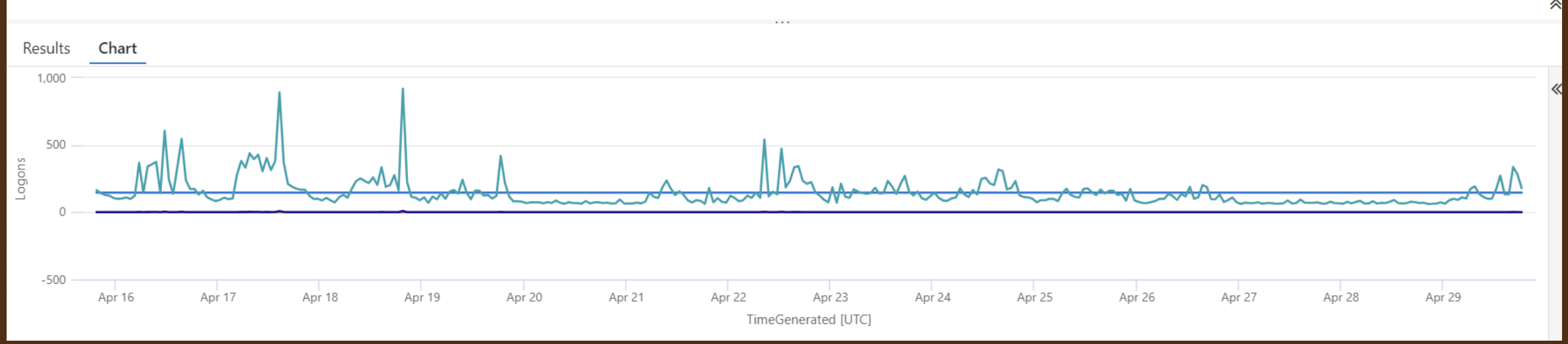
https://www.linkedin.com/in/henning-rauch-adx/

Learning KQL

Series in Kusto

```
SigninLogs
| where TimeGenerated > ago(14d)
| make-series Logons=count() default=0 on TimeGenerated from ago(14d) to now() step 1h
| extend (AnomaliesDetected, AnomaliesScore, AnomaliesBaseline) = series_decompose_anomalies(Logons)
| mv-expand Logons to typeof(double), TimeGenerated to typeof(datetime), AnomaliesDetected to typeof(double), AnomaliesScore to typeof(double), AnomaliesBaseline to typeof(long)
| render timechart

```



What did you do with KQL this month?

Defender for Endpoint - Azure Information Protection Client

https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Endpoint/MDE-AIPClient.md

What did you do with KQL this month?

Defender for IoT

https://github.com/alexverboon/Hunting-Queries-Detection-Rules/tree/main/Defender4IoT

What did you do with KQL this month?

EntraID - Microsoft Defender for Endpoint - Security Settings Management - Device Registrations
https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Azure%20Active%20Directory/EntraID-MDEDeviceRegistrations.md

Results | Chart | Add bookmark

TimeGenerated [UTC]	DeviceName	OldValue	NewValue	Identity	AADOperationType
4/25/2024, 11:16:55.972 AM	SERVER2022-001		Windows Server	Microsoft Intune	Add
4/25/2024, 3:55:57.935 PM	SERVER2019-001	Windows	Windows Server	Microsoft Intune	Update
4/27/2024, 9:16:09.329 AM	SERVER2016-001		Windows Server	Microsoft Intune	Add

What did you do with KQL this month?

Azure Files

Thanks for attending