KQL Café | May 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

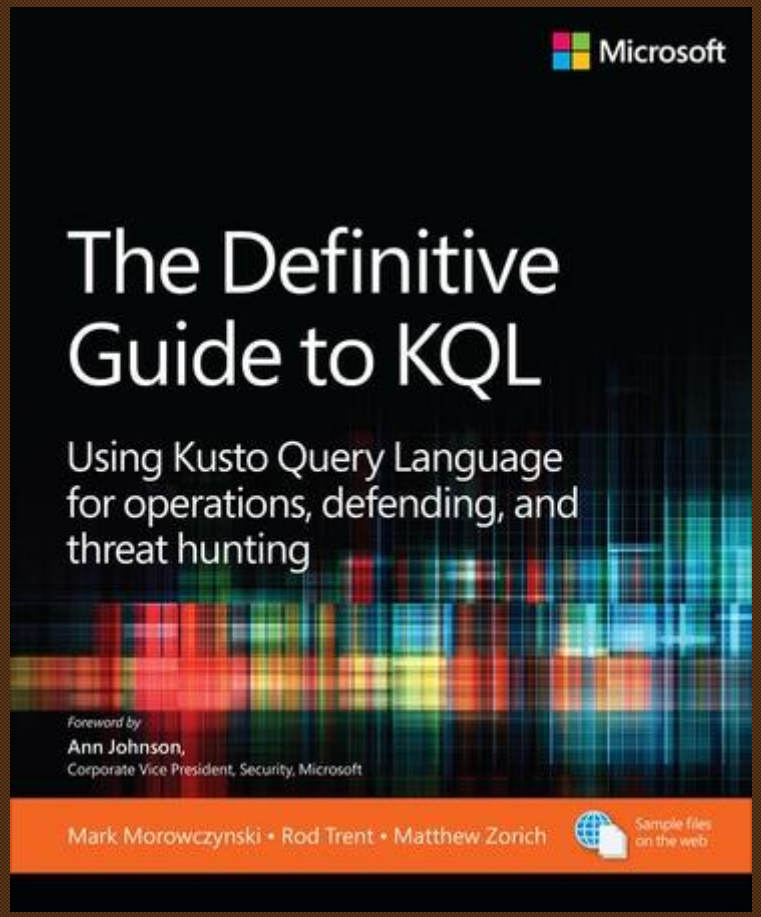
https://www.kustoking.com/


KQL|Cafe

Show | Agenda

Welcome
What is new/updates for KQL
Our guest: Nicola Suter
Learning KQL
What did you do with KQL this month?

News



Released

[KQLMSPress/definitive-guide-kql: Sample queries and data as part of the Microsoft Press book, The Definitive Guide to KQL (github.com)]

News

CloudAuditEvents

The CloudAuditEvents table in the advanced hunting schema contains information about cloud audit events for various cloud platforms protected by the organization's Microsoft Defender for Cloud

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-cloudauditevents-table

Hunting in Azure subscriptions - Guidance

https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/hunting-in-azure-subscriptions/ba-p/4125875

Microsoft Security Exposure Management (XSPM) Overview

https://samilamppu.com/2024/04/15/microsoft-security-exposure-management-xspm-overview-part-1/

https://samilamppu.com/2024/04/25/microsoft-security-exposure-management-xspm-deep-dive-part-2/

Our Guest: Nicola Suter

la-dev | Run | Time range : Last 24 hours | Save | Share | New alert rule | Export | Pin to

```
// KQL Cafe Mai 2024 (:
IdentityInfo
```

Results | Chart | Add bookmark

Name	Location	Work	TechInterests	LeisureStuff
Nicola Suter	Switzerland	Security Consultant @baseVISION	["Security","Identity","KQL","PowerShell"]	["Skitouring","Cycling","Running","Coffe","Beers"]

Columns

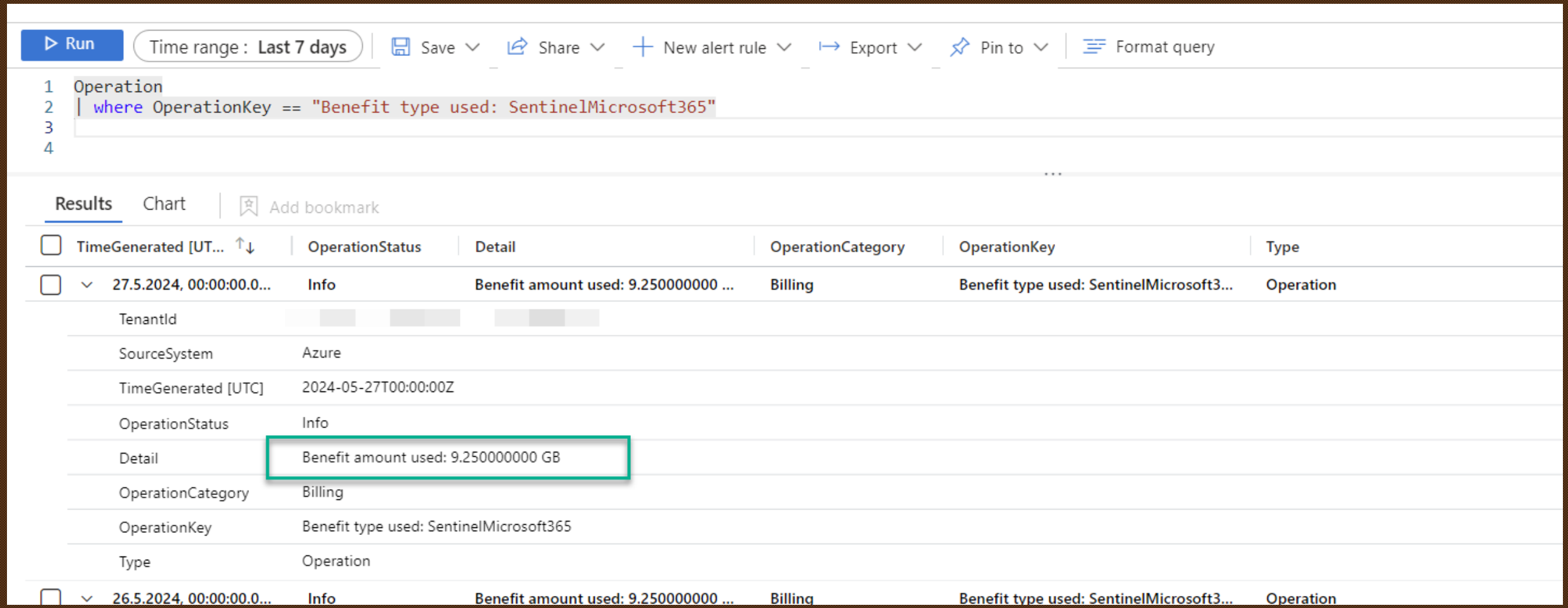
MVP

What did you do with KQL this month?

Journey with Microsoft Security: From CASB to Project Breeze
https://medium.com/@giannicastaldi/journey-with-microsoft-security-from-casb-to-project-breeze-72338c1529ae

What did you do with KQL this month?

Microsoft Sentinel benefit for Microsoft 365 E5, A5, F5, and G5 customers



https://azure.microsoft.com/en-gb/pricing/offers/sentinel-microsoft-365-offer/

What did you do with KQL this month?

EntraID - Group Membership changes - Dynamic Group memberships
https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Azure%20Active%20Directory/EntraID%20-%20GroupMembershipchanges-Dynamic.md

Microsoft Defender for Identity - Attack Disruption
https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Identity/MDI-AttackDisruption.md

Thanks for attending