One Kusto to rule them all

NinjaCat

KustoKing

KQL Cafe

KustoWorks

- Security Consultant
- Detection Engineer
  - Microsoft Sentinel
  - Microsoft 365 Defender
- KQL Trainer

Wat is KQL

Wat is KQL

Query taal

Read only

Veel toepassingen

Waar is KQL

Waar is KQL

Intern bij Microsoft

Microsoft Sentinel

Microsoft 365 Defender

Azure Data Explorer

CM Pivot

Hoe gebruik je KQL

Hoe gebruik je KQL

Portals

Jupyter Notebooks

LogicApps

Scripts


DEMO
Hoe gebruik je KQL

KQL Basics

KQL Basics

Waar is de data

Hoe begin je

Performance


DEMO
KQL Basics

KQL Usecases

KQL Usecases

Hunting

Nieuws

Andere security oplossingen

Hunting

Combining information from your security stack to identify if an adversary was successful in compromising your network, identity, systems or data sources while staying unnoticed

Nieuws

Feedly

Podcasts

Twitter

Andere security oplossingen

https://docs.logpoint.com/docs/alert-rules/en/latest/MITRE.html

https://github.com/elastic/detection-rules/tree/main/rules/windows

https://github.com/SigmaHQ/sigma/tree/master/rules/windows

https://github.com/MdTauheedAlam/CBR-Queries/blob/master/process.md

https://github.com/reprise99/Sentinel-Queries

Vragen?


giannicastaldi


@castallo_johnny


gianni@kustoworks.com

KQL Cafe


www.kustoking.com

Pro tips: [1/7]

- Appregistration for JupyterNotebooks

https://docs.microsoft.com/microsoft-365/security/defender-endpoint/exposed-apis-create-app-webapp

- Feedly is een goede RSS lezer, maak hier een gratis account aan en importeer de feed

KustoKing Feedly Feed.opml

Ross Hamish heft een 3-tal VS Code extensies voor Kusto gemaakt, deze verbeteren de leesbaarheid van Kusto in VS Code

- Wat is Hunting

Combining information from your security stack to identify if an adversary was successful in compromising your network, identity, systems or data sources while staying unnoticed

Pro tips: [2/7]

- Appregistration for JupyterNotebooks

https://docs.microsoft.com/microsoft-365/security/defender-endpoint/exposed-apis-create-app-webapp

- Feedly is een goede RSS lezer, maak hier een gratis account aan en importeer de feed

KustoKing Feedly Feed.opml

Ross Hamish heft een 3-tal VS Code extensies voor Kusto gemaakt, deze verbeteren de leesbaarheid van Kusto in VS Code

- Wat is Hunting

Combining information from your security stack to identify if an adversary was successful in compromising your network, identity, systems or data sources while staying unnoticed

Pro tips: [3/7]

- Azure Data Explorer Demo:

https://dataexplorer.azure.com/clusters/help/databases/SampleIoTData

- Log Analytics Demo

https://aka.ms/lademo

Pro tips: [4/7]

```
// Search
search "kusto"

search "*kusto*"

// has <> contains
AADNonInteractiveUserSignInLogs
| where * has "Kusto"

AADNonInteractiveUserSignInLogs
| where * contains "Kusto"
```

Pro tips: [5/7]

```
// Project
AADNonInteractiveUserSignInLogs
| where * contains "Kusto"
| project TimeGenerated, Category

// Distinct
AADNonInteractiveUserSignInLogs
| where * contains "Kusto"
| distinct AppDisplayName
```

Pro tips: [6/7]

```
// Summarize
AADNonInteractiveUserSignInLogs
| where * contains "Kusto"
| summarize count() by AppDisplayName


// Extend
AADNonInteractiveUserSignInLogs
| where * contains "Kusto"
| extend AppClient = strcat(ClientAppUsed, " - ", AppDisplayName)
| distinct AppClient
```

Pro tips: [7/7]

```
// Take <> Top
AADNonInteractiveUserSignInLogs
| where * contains "Kusto"
| extend AppClient = strcat(ClientAppUsed, " - ", AppDisplayName)
| take 10

AADNonInteractiveUserSignInLogs
| where * contains "Kusto"
| extend AppClient = strcat(ClientAppUsed, " - ", AppDisplayName)
| top 10 by TimeGenerated
```