Session 6-2023 | Jupyter Notebooks

KQL|Cafe

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/

Show | Agenda

Welcome

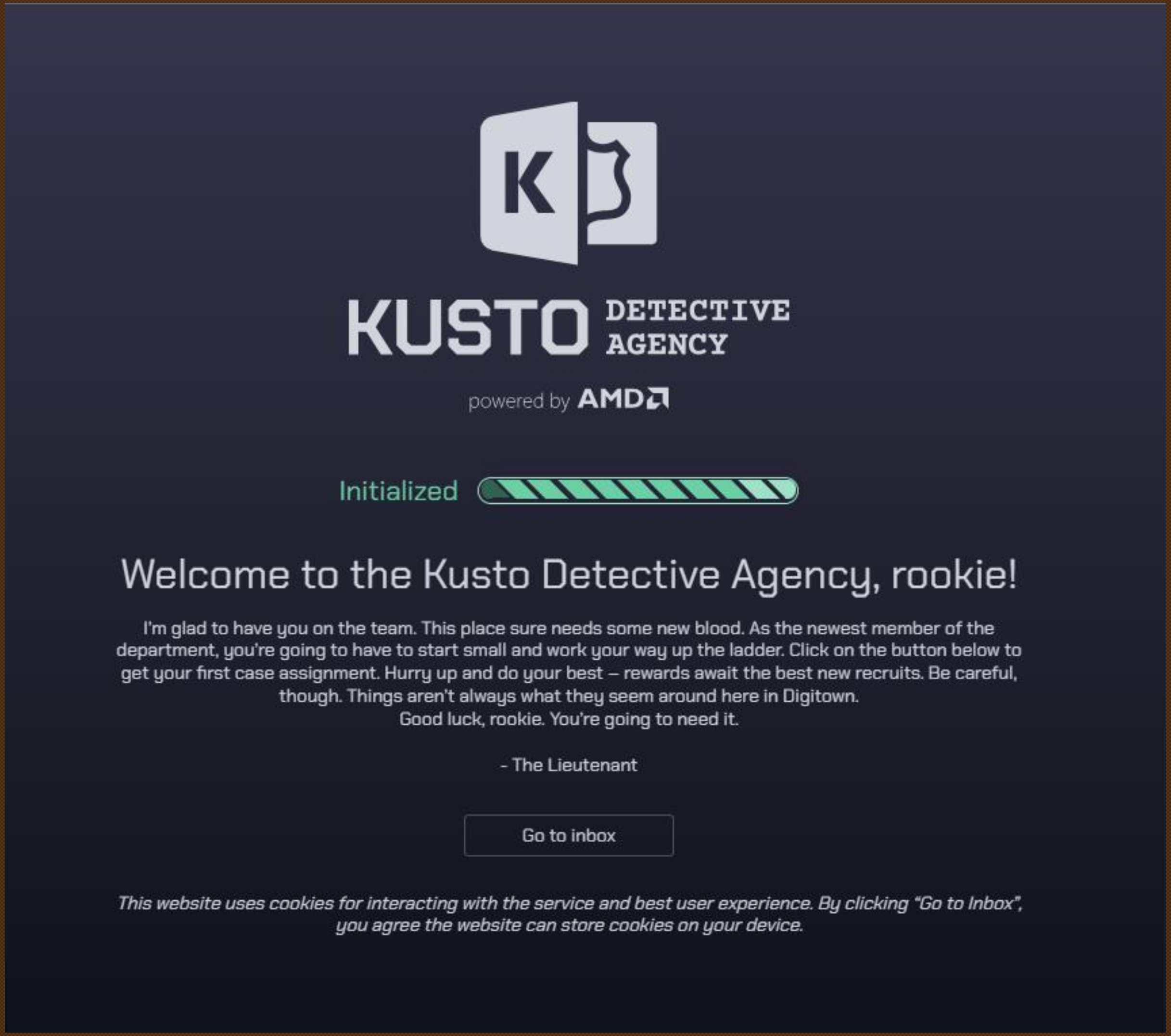
What is new/updates for KQL

Our KQL Guest Brian Bønk Rueløkke

What did you do with KQL this month?

What's New

Kusto Detective Agency – **Season 2**



Welcome to the Kusto Detective Agency, rookie!

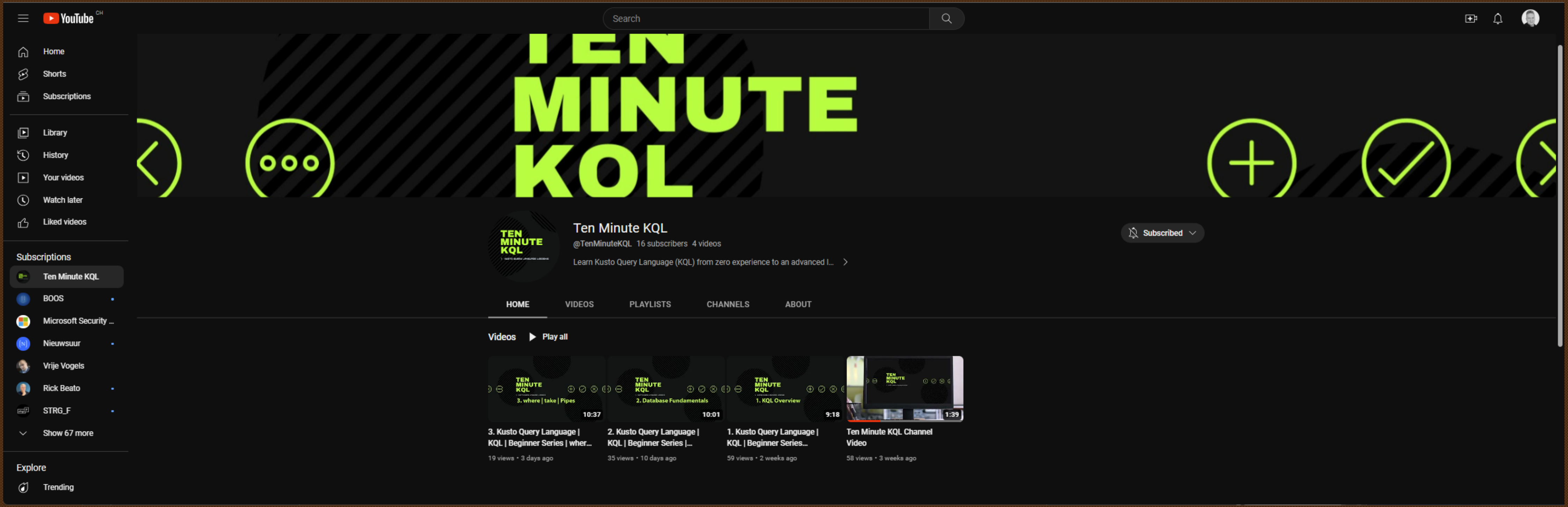
I'm glad to have you on the team. This place sure needs some new blood. As the newest member of the department, you're going to have to start small and work your way up the ladder. Click on the button below to get your first case assignment. Hurry up and do your best – rewards await the best new recruits. Be careful, though. Things aren't always what they seem around here in Digitown.
Good luck, rookie. You're going to need it.

- The Lieutenant

This website uses cookies for interacting with the service and best user experience. By clicking "Go to Inbox", you agree the website can store cookies on your device.

What's New

Ten Minute KQL is dedicated to learning the Kusto Query Language, in short ten-minute sessions. This video provides an overview for upcoming learning Beginner, Intermediate, and Advanced KQL learning paths as well as ideas for future video series. If you have limited experience in tech, or have never learned a language don't hesitate to start with the Beginner series. We will do our best to keep the technical jargon to a minimum in that learning path.



Ten Minute KQL
@TenMinuteKQL 16 subscribers 4 videos
Learn Kusto Query Language (KQL) from zero experience to an advanced l...

3. Kusto Query Language | KQL | Beginner Series | wher...
19 views • 3 days ago

2. Kusto Query Language | KQL | Beginner Series |...
35 views • 10 days ago

1. Kusto Query Language | KQL | Beginner Series...
59 views • 2 weeks ago

Ten Minute KQL Channel Video
58 views • 3 weeks ago

What's New

new ActionTypes in DeviceNetworkEvents

On July 18, 2023, Microsoft will be ret new ActionTypes in DeviceNetworkEventsiring a subset of signatures found in the "NetworkSignaturesInspected" action type of Advanced Hunting. With the recent integration of Zeek providing advanced protocol parsing capabilities, which result in better visibility into full network sessions compared to the raw packet bytes found in the "NetworkSignaturesInspected" action type of Advanced Hunting today, the effort to consolidate will provide a better overall experience for our customers by reducing the signatures that serve similar functions without the added benefits provided by the new Zeek alternative.

When this will happen:
July 18, 2023

How this affects your organization:

For customers currently using the "NetworkSignaturesInspected" action type, here is a list of signatures that will be deprecated, referenced alongside their alternatives available in Advanced Hunting:

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/enrich-your-advanced-hunting-experience-using-network-layer/ba-p/3794693

What's New

new ActionTypes in DeviceNetworkEvents

Protocol / Signature Name	Old Action Type	New Action Type
SSH	NetworkSignatureInspected	SshConnectionInspected
FTP_Upload	NetworkSignatureInspected	FtpConnectionInspected
FFP_Client	NetworkSignatureInspected	FtpConnectionInspected
HTTP_Client	NetworkSignatureInspected	HttpConnectionInspected
HTTP_Server	NetworkSignatureInspected	HttpConnectionInspected
HTTP_RequestBodyParameters	NetworkSignatureInspected	HttpConnectionInspected
HTTPS_Client	NetworkSignatureInspected	SslConnectionInspected
DNS_Request	NetworkSignatureInspected	DnsConnectionInspected

An example of your old query:

```
DeviceNetworkEvents
| where ActionType == "NetworkSignatureInspected"
| extend AdditionalFields = todynamic(AdditionalFields)
| where AdditionalFields.SignatureName == "SSH"
```

Your new query:

```
DeviceNetworkEvents
| where ActionType == "SshConnectionInspected"
```

What's New

(Updated) Configuration Change - Microsoft Defender for Cloud Apps threat protection policies

Alert Name	Policy name
Activity from infrequent country	Activity from infrequent country
Impossible travel activity	Impossible travel
Mass delete	Unusual file deletion activity (by user)
Mass download	Unusual file download (by user)
Mass share	Unusual file share activity (by user)
Multiple delete VM activities	Multiple delete VM activities
Multiple failed login attempts	Multiple failed login attempts
Multiple Power BI report sharing activities	Multiple Power BI report sharing activities
Multiple VM creation activities	Multiple VM creation activities
Suspicious administrative activity	Unusual administrative activity (by user)
Suspicious impersonated activity	Unusual impersonated activity (by user)
Suspicious OAuth app file download activities	Suspicious OAuth app file download activities
Suspicious Power BI report sharing	Suspicious Power BI report sharing
Unusual addition of credentials to an OAuth app	Unusual addition of credentials to an OAuth app

https://admin.microsoft.com/Adminportal/Home?source=applauncher&ref=MessageCenter/:/messages/MC550086

What's New

(Updated) Configuration Change - Microsoft Defender for Cloud Apps threat protection policies

[Investigate behaviors with advanced hunting (Preview) - Microsoft Defender for Cloud Apps | Microsoft Learn]

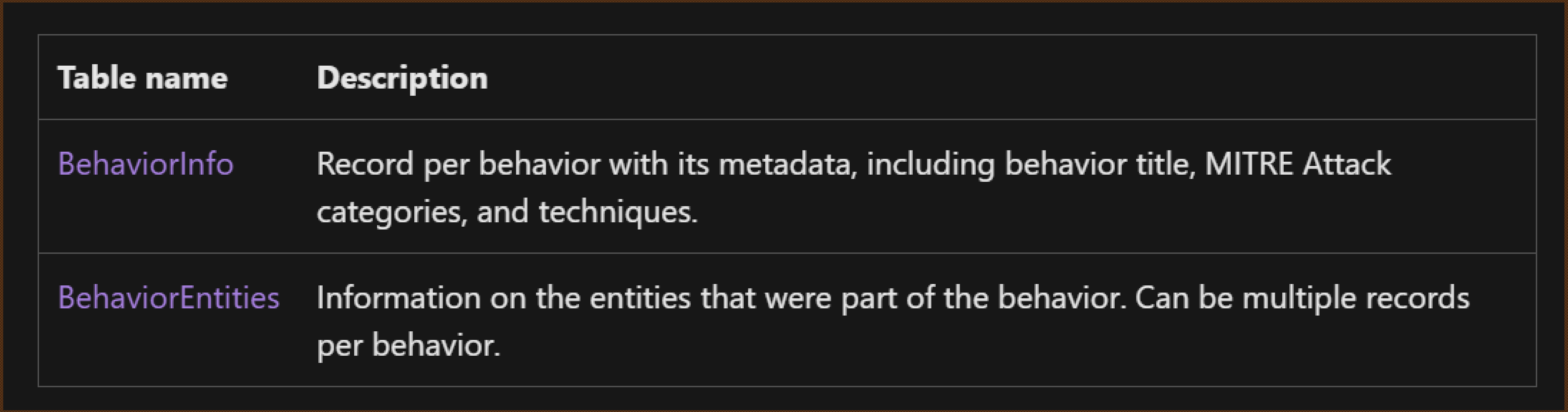
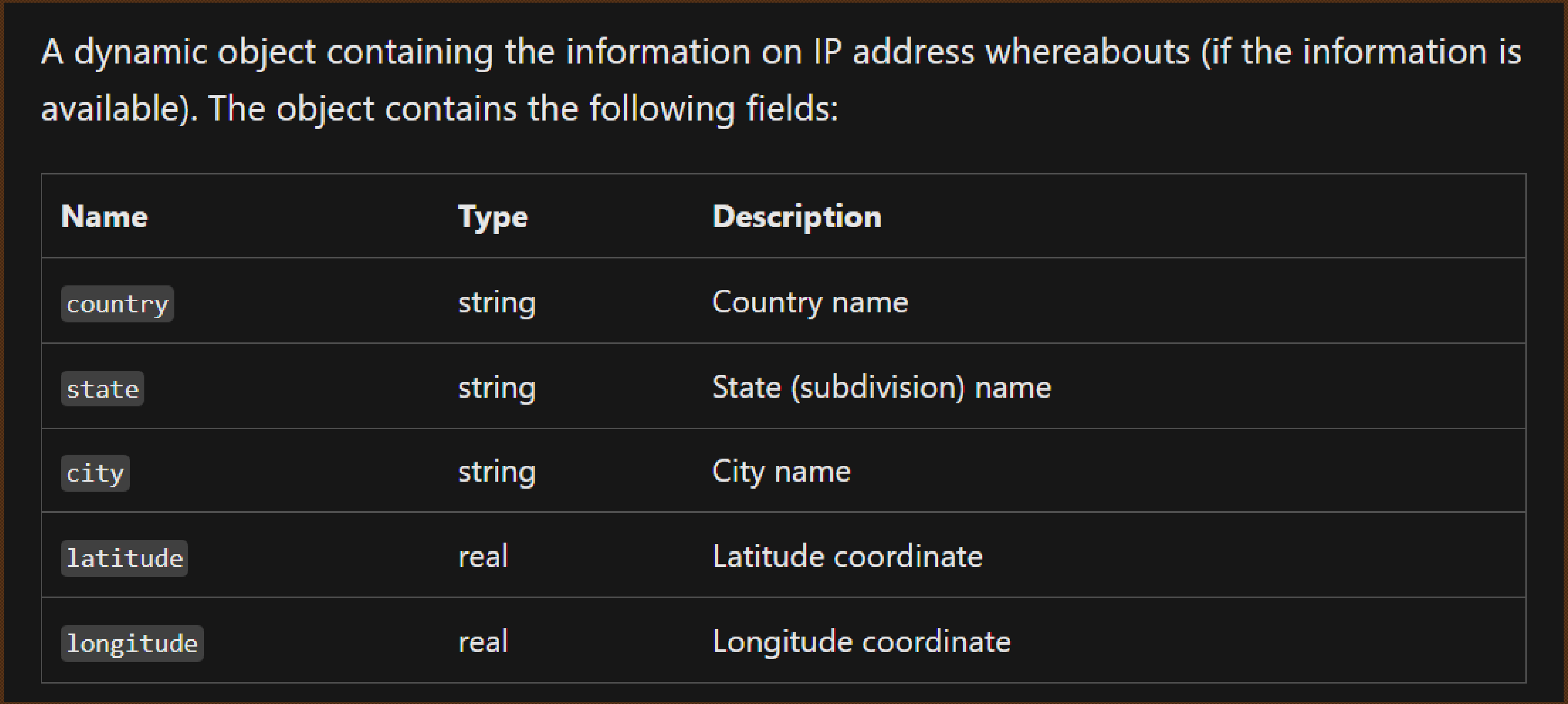


Table name	Description
BehaviorInfo	Record per behavior with its metadata, including behavior title, MITRE Attack categories, and techniques.
BehaviorEntities	Information on the entities that were part of the behavior. Can be multiple records per behavior.

https://admin.microsoft.com/Adminportal/Home?source=applauncher&ref=MessageCenter/:/messages/MC550086

What's New

geo_info_from_ip_address()



A dynamic object containing the information on IP address whereabouts (if the information is available). The object contains the following fields:

Name	Type	Description
`country`	string	Country name
`state`	string	State (subdivision) name
`city`	string	City name
`latitude`	real	Latitude coordinate
`longitude`	real	Longitude coordinate

Works with IPV4 and IPv6

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/geo-info-from-ip-address-function

https://rodtrent.substack.com/p/getting-geo-information-for-ip-addresses

What's New

geo_info_from_ip_address()

```
// old way to get additional geo info, but in Sign-in logs there is no added value because the location info is already in the logs by default
let geoData =
externaldata(network:string,geoname_id:string,continent_code:string,continent_name:string,country_iso_code:string,country_name:string,is_anonymous_proxy:string,is_satellite_provider:string) [@"https://raw.githubusercontent.com/datasets/geoip2-ipv4/master/data/geoip2-ipv4.csv"] with (ignoreFirstRecord=true, format="csv");
SigninLogs
| where isnotempty( IPAddress)
| where TimeGenerated > ago(90d)
| project TimeGenerated, IPAddress, Location, LocationDetails
| evaluate ipv4_lookup (geoData, IPAddress, network, true)
```

```
// old way to get additional geo info, here there's added value to do so since the location info is NOT included in the logs
let geoData =
externaldata(network:string,geoname_id:string,continent_code:string,continent_name:string,country_iso_code:string,country_name:string,is_anonymous_proxy:string,is_satellite_provider:string) [@"https://raw.githubusercontent.com/datasets/geoip2-ipv4/master/data/geoip2-ipv4.csv"] with (ignoreFirstRecord=true, format="csv");
OfficeActivity
| where isnotempty( ClientIP)
| where TimeGenerated > ago(90d)
| project TimeGenerated, ClientIP, Operation, OfficeWorkload
| evaluate ipv4_lookup (geoData, ClientIP, network, true)
```

What's New

geo_info_from_ip_address()

```
//  // the new way
OfficeActivity
| where isnotempty( ClientIP)
| where TimeGenerated > ago(90d)
| project TimeGenerated, ClientIP, Operation, OfficeWorkload
| extend geoinfo =  geo_info_from_ip_address(ClientIP)
| extend country = tostring(geoinfo.country)
| extend city = tostring(geoinfo.city)
| extend state = tostring(geoinfo.state)
| extend latitude = tostring(geoinfo.latitude)
| extend longitude = tostring(geoinfo.longitude)
// | where ClientIP contains "::ffff:52.112.120.202"
```

Brian Bønk Rueløkke

Principal & Enterprise arkitekt, Data & Analytics

Fellowmind

https://linkedin.com/in/brianbonk

https://brianbonk.dk

MVP
Microsoft
Most Valuable Professional

Microsoft

FastTrack Recognized
Solution Architect
Power BI
2022 >>

Microsoft

Certified Trainer
Data Platform

2018 >>

What did you do with KQL this month?

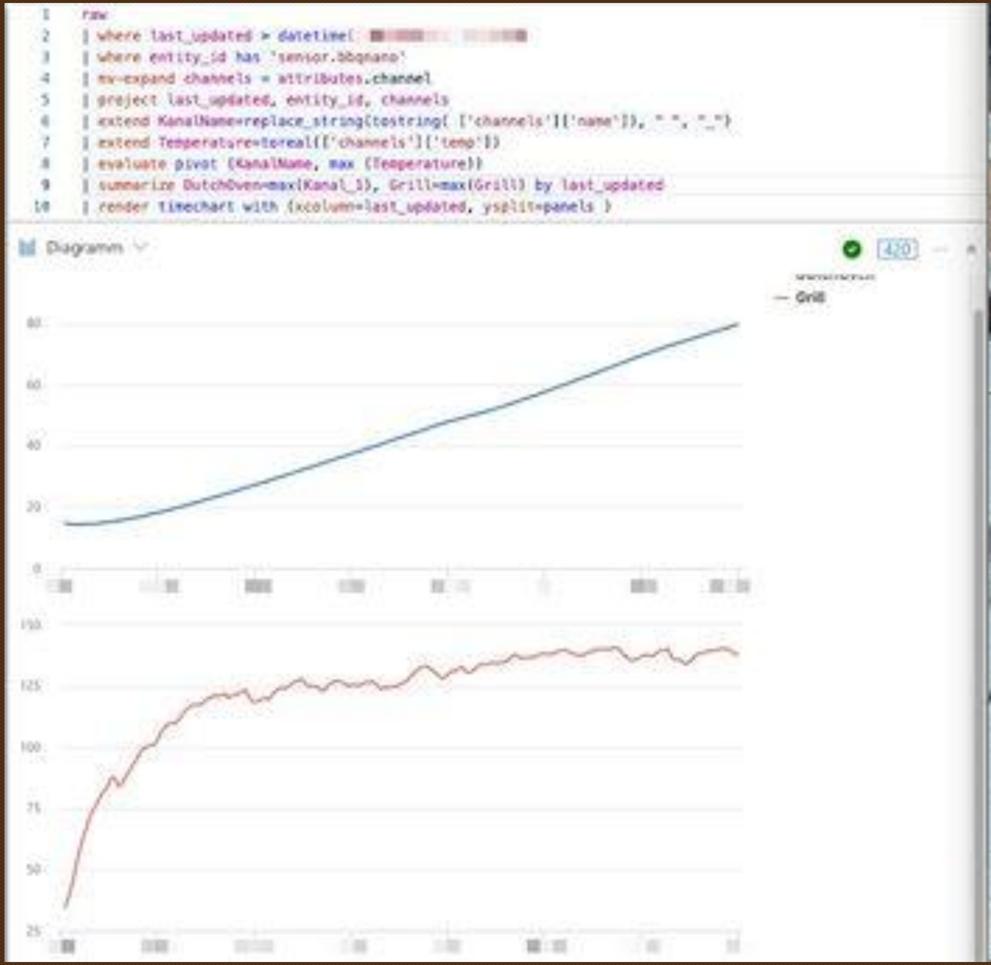
TI Sign-In Logs

Get all Incidents - expand entities and then join the entities with the Sign-in logs again

```
let ioc_lookBack = 90d;
let lookback = 90d;
let IncTitle = dynamic(["(Preview) TI map IP entity to SigninLogs","TI map IP entity to SigninLogs"]);
SecurityIncident
| where TimeGenerated > ago(lookback)
| where Title has_any (IncTitle)
| summarize arg_max(TimeGenerated,*) by IncidentNumber
| mv-expand AlertIds
| extend AlertId = tostring(AlertIds)
| join  (SecurityAlert)
on $left. AlertId == $right. SystemAlertId
| mv-expand parse_json(Entities)
| extend EType = tostring((Entities.Type))
| where EType == 'ip'
| extend IPAddress = tostring(Entities.Address)
// Count the # of alerts per IP address
| summarize Alertcount = dcount(SystemAlertId) by IPAddress
| join kind=innerunique  (ThreatIntelligenceIndicator
   | where TimeGenerated >= ago(ioc_lookBack) and ExpirationDateTime > now()
   | summarize LatestIndicatorTime = arg_max(TimeGenerated, *) by IndicatorId
   | where Active == true
   // Picking up only IOC's that contain the entities we want
   | where isnotempty(NetworkIP)
      or isnotempty(EmailSourceIpAddress)
      or isnotempty(NetworkDestinationIP)
      or isnotempty(NetworkSourceIP)
   // As there is potentially more than 1 indicator type for matching IP, taking NetworkIP first, then others if that is empty.
   // Taking the first non-empty value based on potential IOC match availability
   | extend TI_ipEntity = iff(isnotempty(NetworkIP), NetworkIP, NetworkDestinationIP)
   | extend TI_ipEntity = iff(isempty(TI_ipEntity) and isnotempty(NetworkSourceIP), NetworkSourceIP, TI_ipEntity)
   | extend TI_ipEntity = iff(isempty(TI_ipEntity) and isnotempty(EmailSourceIpAddress), EmailSourceIpAddress, TI_ipEntity)
) on $left. IPAddress ==  $right.TI_ipEntity
| project IPAddress, Alertcount, LatestIndicatorTime, SourceSystem, ConfidenceScore, Description, ThreatType, Tags
// find the successfull sign-ins
| join SigninLogs
on $left. IPAddress == $right. IPAddress
| summarize TotalSignIns = dcount(CorrelationId), Failed = dcountif(CorrelationId, ResultType != 0), Success = dcountif(CorrelationId,ResultType == 0) , TotalUsers = dcount(UserPrincipalName)
by IPAddress, Alertcount, Description, ThreatType, Tags, AutonomousSystemNumber, Location
```

KQL and BBQ

If you don´t know what todo until the next Kusto Detective Case?
Hookup your WiFi Thermometer to ADX and check if your BBQ is going well :D



```
raw
| where last_updated > datetime( [redacted]
| where entity_id has 'sensor.bbqnano'
| mv-expand channels = attributes.channel
| project last_updated, entity_id, channels
| extend KanalName=replace_string(tostring( ['channels']['name']), " ", "_")
| extend Temperature=toreal(['channels']['temp'])
| evaluate pivot (KanalName, max (Temperature))
| summarize DutchOven=max(Kanal_1), Grill=max(Grill) by last_updated
| render timechart with (xcolumn=last_updated, ysplit=panels )
```

https://www.linkedin.com/posts/christian-kohmann-88720310a_adx-kql-kusto-activity-7074053783516835840-sv-n?utm_source=share&utm_medium=member_desktop

Thanks for attending

KQL|Cafe