
AZURE
PLATFORM ENGINEERING
APEN HEUL
MONKEY SEE, MONKEY DETECT

AGENDA

- Good detection logic?
- KQL fundamentals
- From KQL to Detection
- Wrap-up

WHO AM I

GIANNI CASTALDI

SECURITY CONSULTANT @ KUSTOWORKS

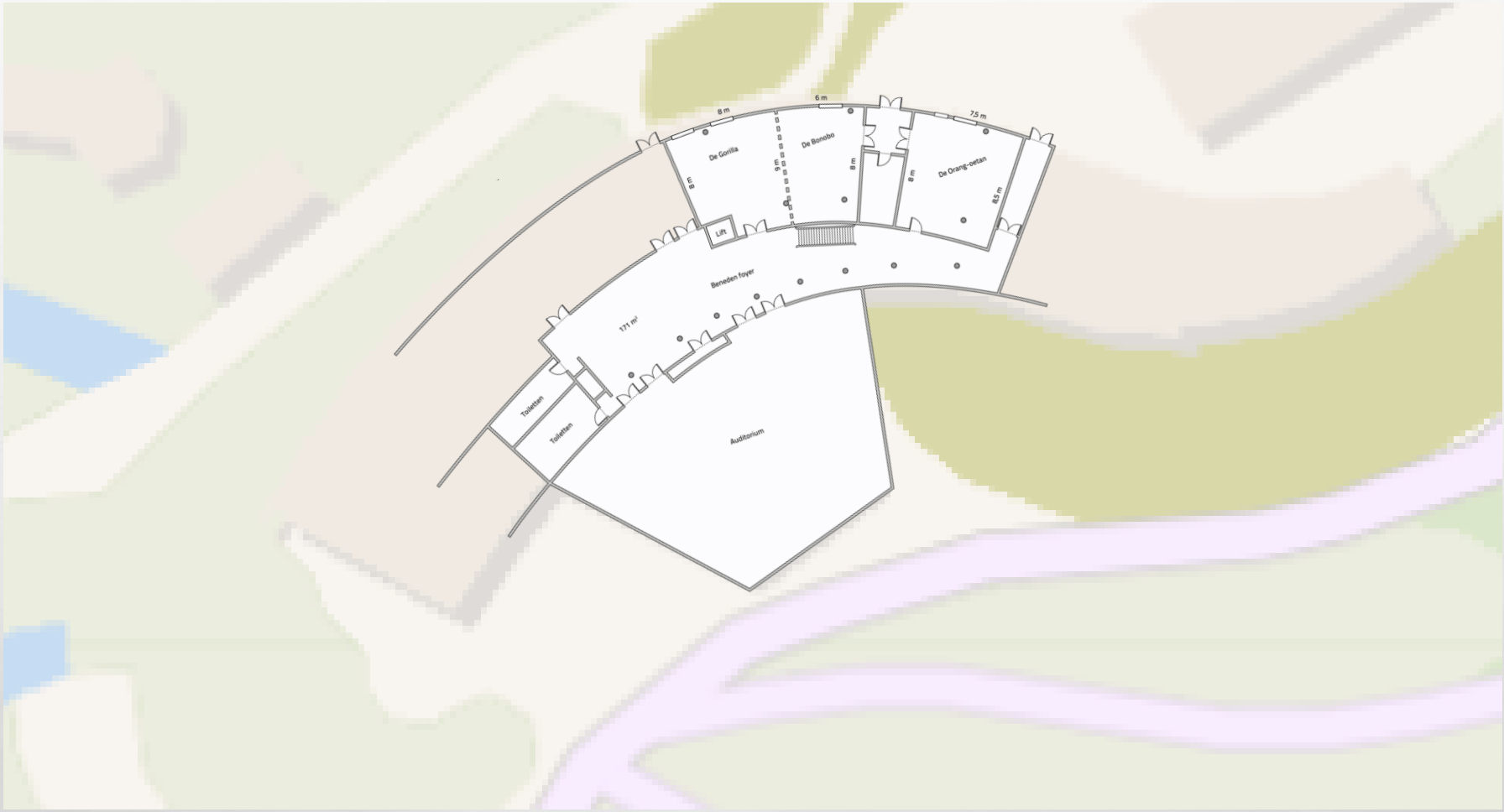
/GIANNICASTALDI

MICROSOFT MVP

GIAC GCFE

CISSP

ANY IDEA WHERE THIS IS?


8 m
6 m
7,5 m
De Gorilla
De Bonobo
De Orang-oetan
8 m
8 m
8,5 m
Lift
Beneden foyer
171 m²
Toiletten
Toiletten
Auditorium

LET'S VISIT OUR CISO

CHIEF BANANA SECURITY OFFICER

LOG JUNGLE

TOO MUCH DATA

TOO LITTLE DETECTION LOGIC

ALERT FATIGUE

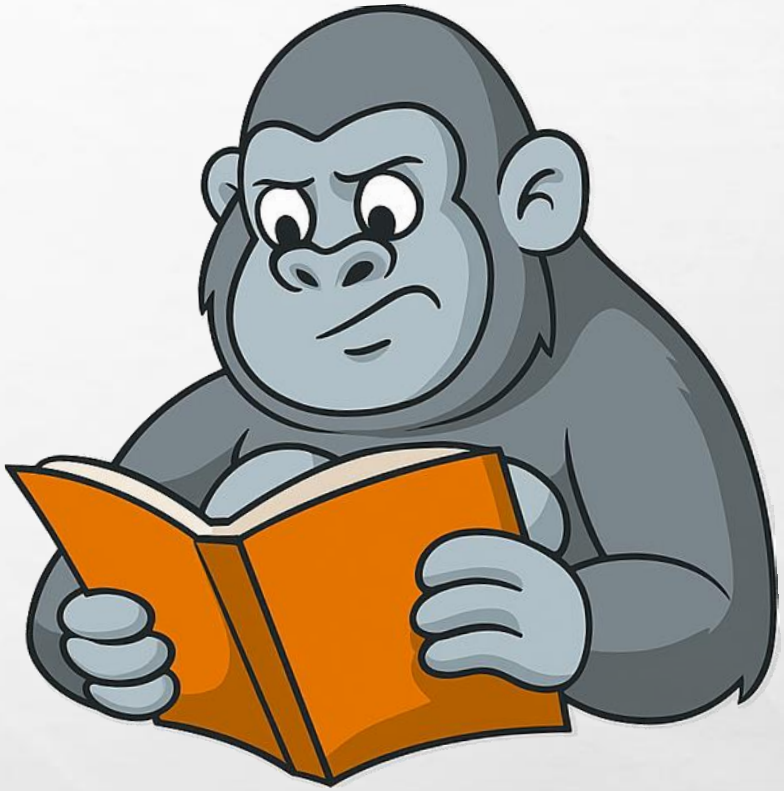
GOOD DETECTION LOGIC

Good signal-to-noise ratio

Hypothesis driven

MITRE-Focused

KQL FOUNDATIONS



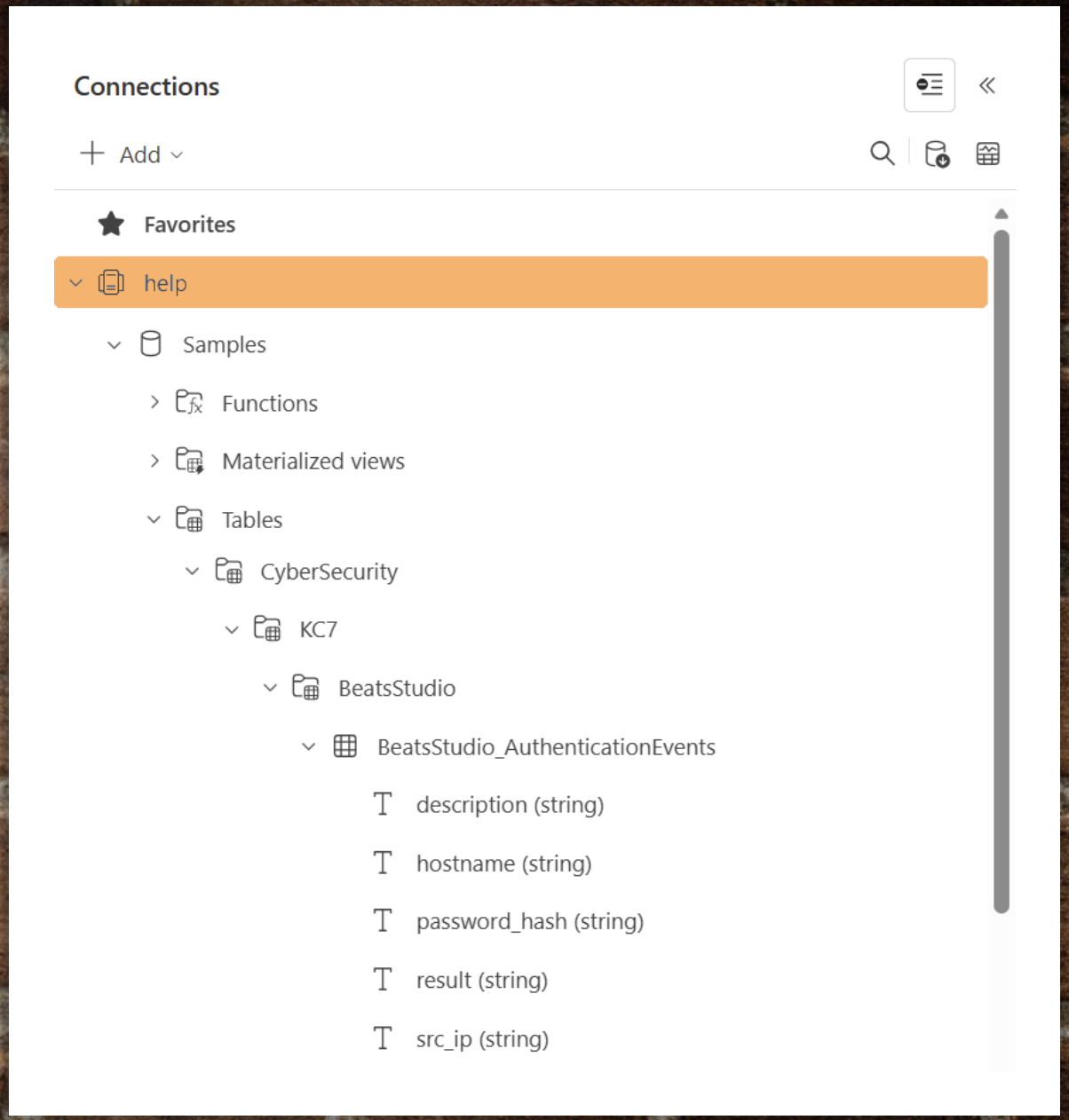
WHAT IS KQL

- A KUSTO QUERY IS A READ-ONLY WAY TO PROCESS DATA AND GET RESULTS IN A SIMPLE, DATA-FLOW STYLE.

OBJECTS IN KUSTO

- Cluster
- Database
- Tables
- Columns
- Rows
- Function
- Views
- External Data

COMPONENTS IN THE EXPLORER



KQL BEGINNER

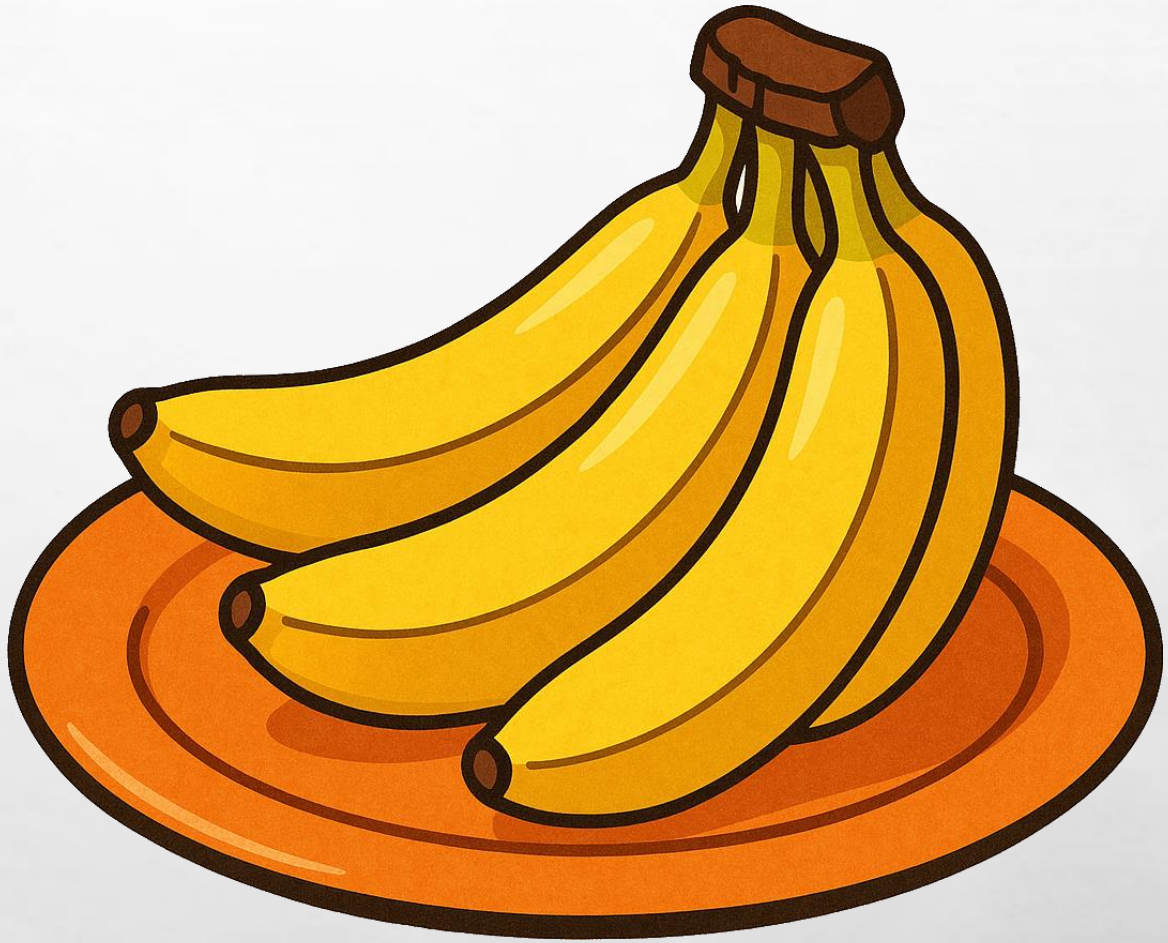
- take
- where
- extend
- project
- summarize
- sort by

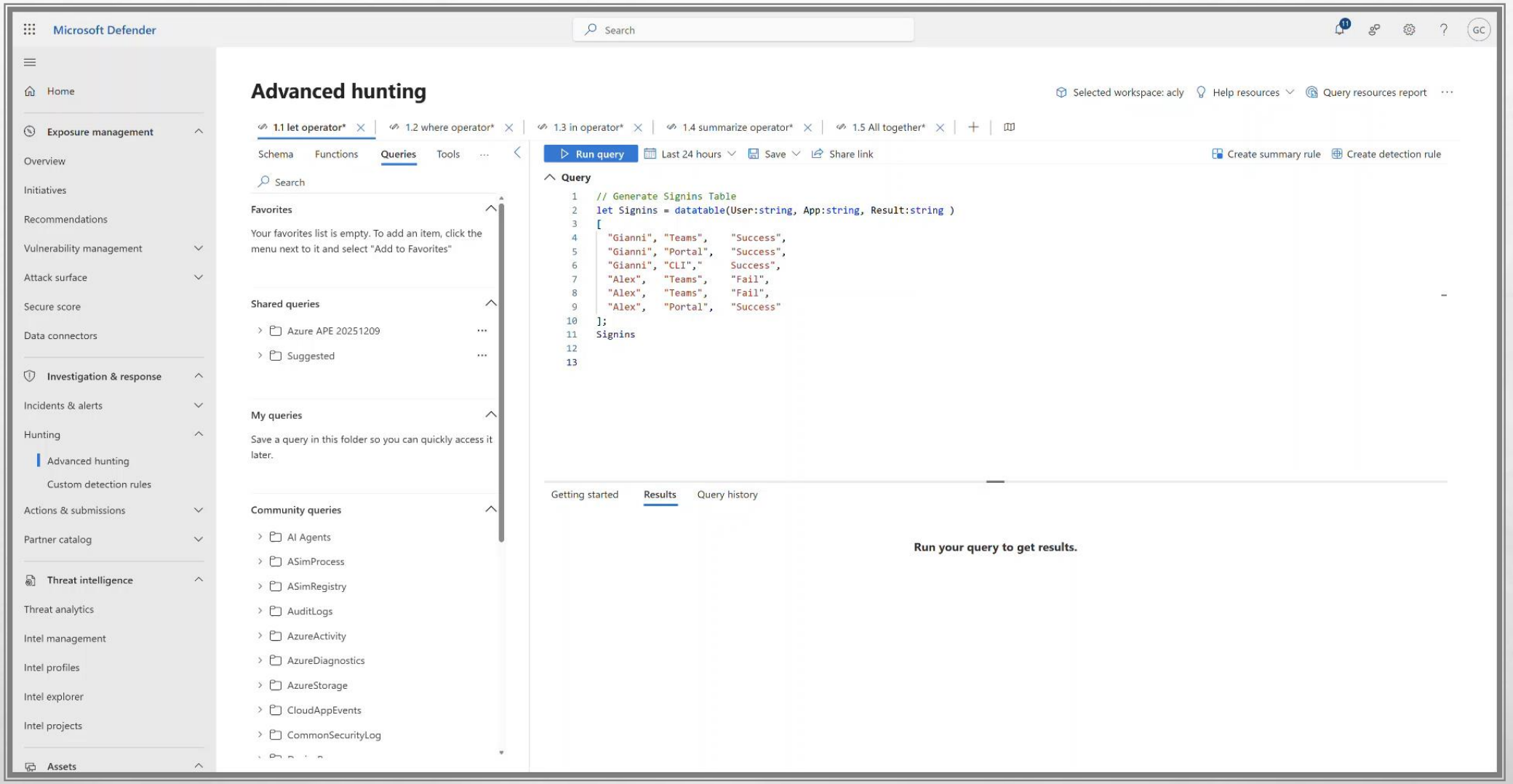
KQL MODERATE

- let
- dynamic
- in()
- case()
- isnotempty()

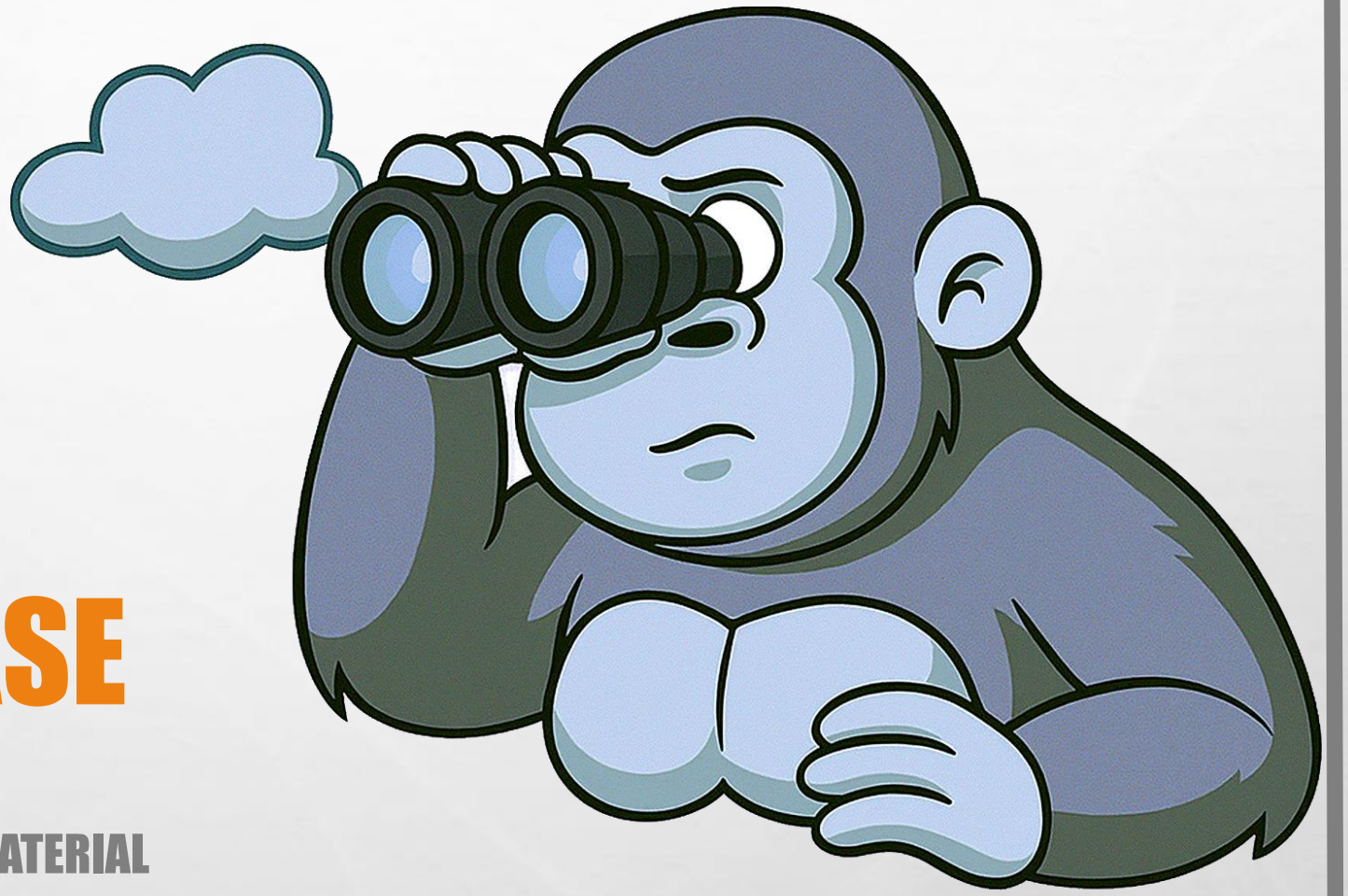
KQL BASICS

DEMO




Microsoft Defender
Search
Home
Exposure management
Overview
Initiatives
Recommendations
Vulnerability management
Attack surface
Secure score
Data connectors
Investigation & response
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Partner catalog
Threat intelligence
Threat analytics
Intel management
Intel profiles
Intel explorer
Intel projects
Assets
Advanced hunting
Selected workspace: acly
Help resources
Query resources report
1.1 let operator*
1.2 where operator*
1.3 in operator*
1.4 summarize operator*
1.5 All together*
Schema
Functions
Queries
Tools
Search
Favorites
Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"
Shared queries
Azure APE 20251209
Suggested
My queries
Save a query in this folder so you can quickly access it later.
Community queries
AI Agents
ASimProcess
ASimRegistry
AuditLogs
AzureActivity
AzureDiagnostics
AzureStorage
CloudAppEvents
CommonSecurityLog
Run query
Last 24 hours
Save
Share link
Create summary rule
Create detection rule
Query
// Generate Signins Table
let Signins = datatable(User:string, App:string, Result:string)
[
"Gianni", "Teams", "Success",
"Gianni", "Portal", "Success",
"Gianni", "CLI", Success",
"Alex", "Teams", "Fail",
"Alex", "Teams", "Fail",
"Alex", "Portal", "Success"
];
Signins
Getting started
Results
Query history
Run your query to get results.

TODAY'S USE CASE



TA0005: DEFENSE EVASION

T1550: USE ALTERNATE AUTHENTICATION MATERIAL

T1550.004: WEB SESSION COOKIE

HYPOTHESIS

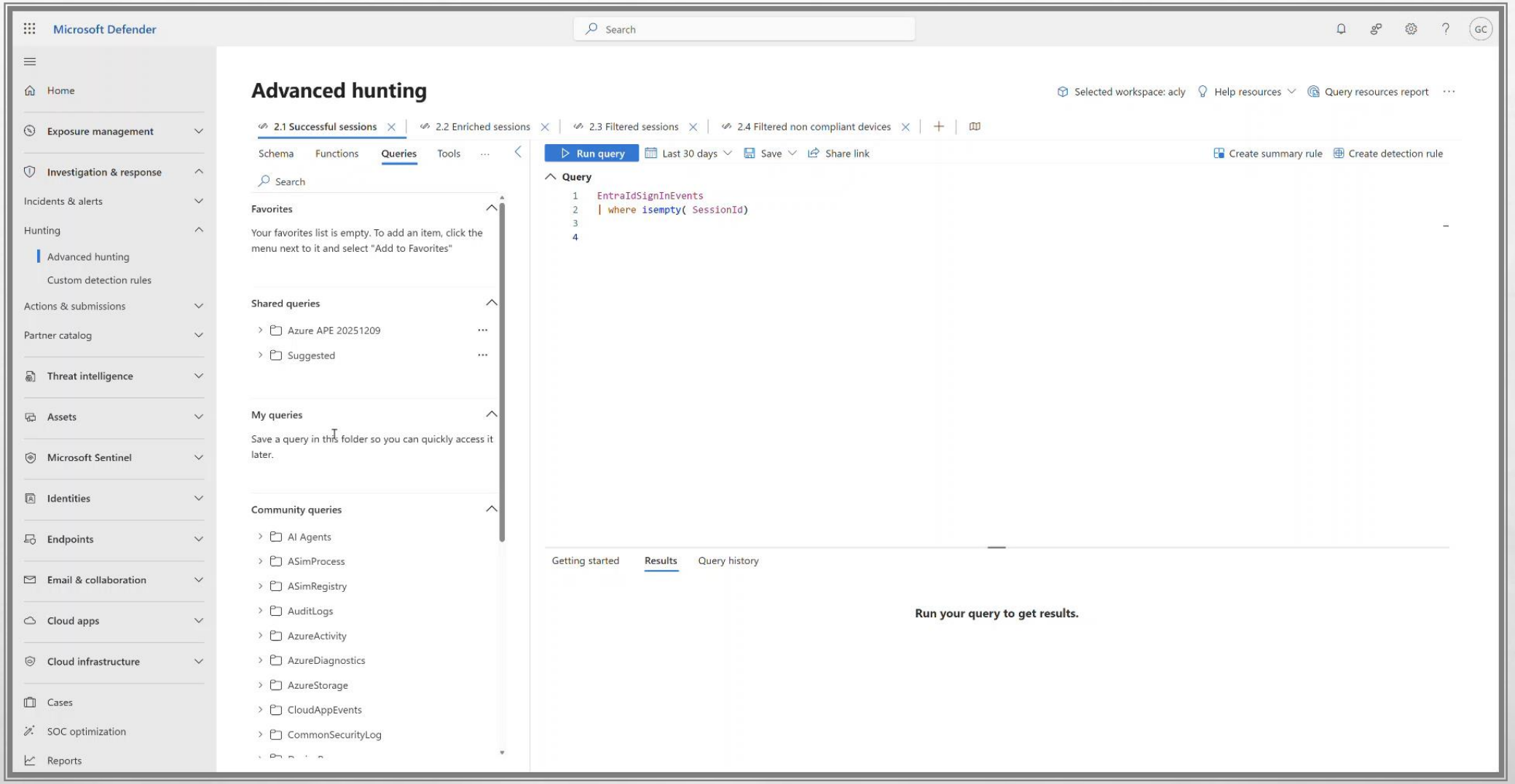
A successful login creates a SessionId

A Regular user session does not interact with administrative applications

Admin Behavior only happens from Compliant Devices

BUILDING THE QUERY

DEMO


Microsoft Defender
Search
GC
Home
Exposure management
Investigation & response
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Cases
SOC optimization
Reports
Advanced hunting
Selected workspace: acly
Help resources
Query resources report
2.1 Successful sessions
2.2 Enriched sessions
2.3 Filtered sessions
2.4 Filtered non compliant devices
Schema
Functions
Queries
Tools
Search
Favorites
Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"
Shared queries
Azure APE 20251209
Suggested
My queries
Save a query in this folder so you can quickly access it later.
Community queries
AI Agents
ASimProcess
ASimRegistry
AuditLogs
AzureActivity
AzureDiagnostics
AzureStorage
CloudAppEvents
CommonSecurityLog
Run query
Last 30 days
Save
Share link
Create summary rule
Create detection rule
Query
1 EntraIdSignInEvents
2 | where isempty(SessionId)
3
4
Getting started
Results
Query history
Run your query to get results.

KQL TO DETECTION

MICROSOFT SENTINEL

- Analytic Rules
- Frequency NRT or 5M to 14D
- Short Lookback (<1h) 5M to 2879M
- Long LookBack (>1h) 5M TO 14D

MICROSOFT DEFENDER XDR

Custom Detections

Frequency NRT or 5M to 14D

Short Lookback (<1D) 4 Times FREQENCY

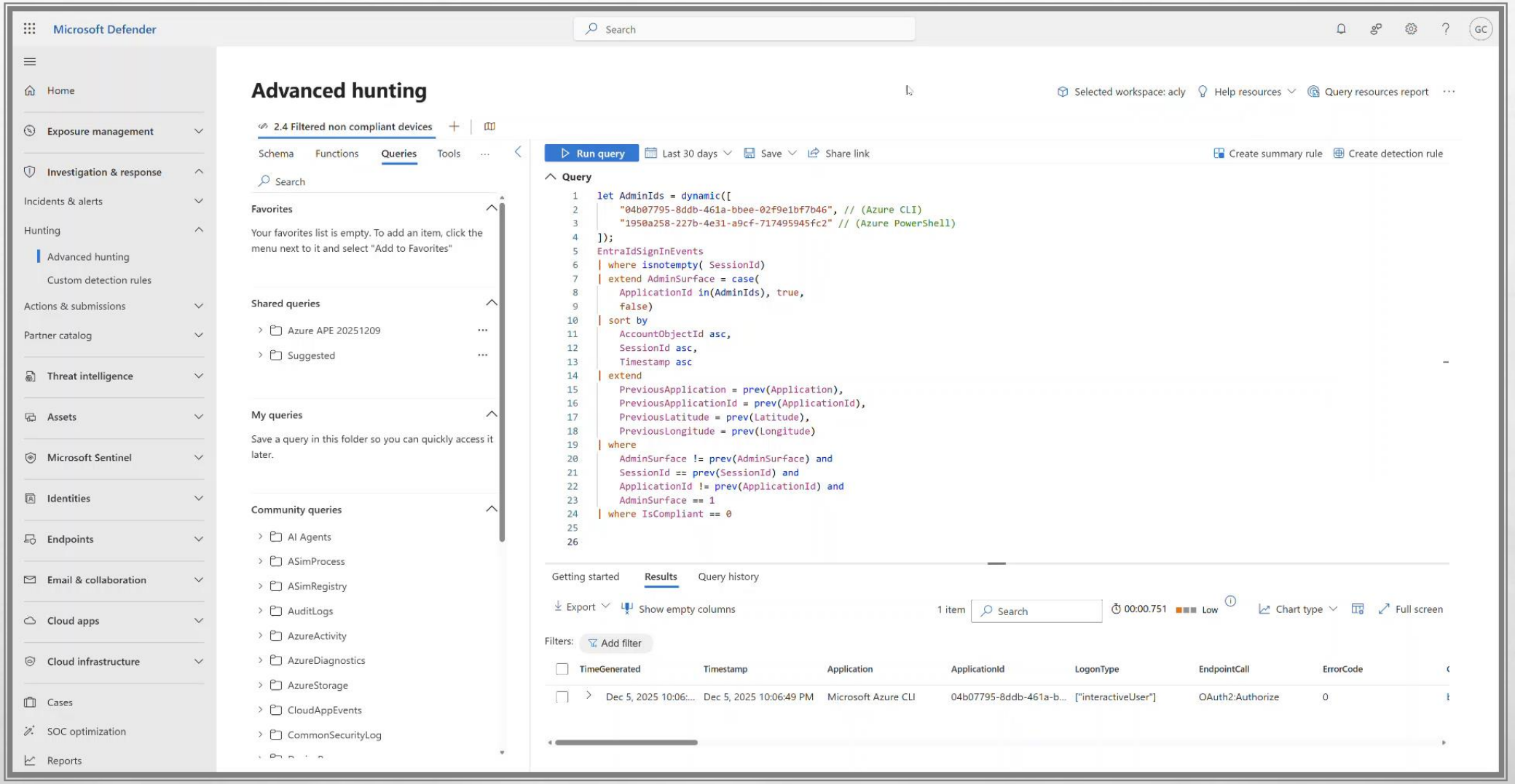
LONG Lookback (>1d) 30DAYS

Automated actions

- Device
- Files
- User
- Email

CREATING DETECTION

DEMO


Microsoft Defender
Search
GC
Home
Exposure management
Investigation & response
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Cases
SOC optimization
Reports
Advanced hunting
Selected workspace: acly
Help resources
Query resources report
2.4 Filtered non compliant devices
Schema
Functions
Queries
Tools
Search
Favorites
Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"
Shared queries
Azure APE 20251209
Suggested
My queries
Save a query in this folder so you can quickly access it later.
Community queries
AI Agents
ASimProcess
ASimRegistry
AuditLogs
AzureActivity
AzureDiagnostics
AzureStorage
CloudAppEvents
CommonSecurityLog
Run query
Last 30 days
Save
Share link
Create summary rule
Create detection rule
Query
let AdminIds = dynamic([
"04b07795-8ddb-461a-bbee-02f9e1bf7b46", // (Azure CLI)
"1950a258-227b-4e31-a9cf-717495945fc2" // (Azure PowerShell)
]);
EntraIdSignInEvents
| where isnotempty(SessionId)
| extend AdminSurface = case(
ApplicationId in(AdminIds), true,
false)
| sort by
AccountObjectId asc,
SessionId asc,
Timestamp asc
| extend
PreviousApplication = prev(Application),
PreviousApplicationId = prev(ApplicationId),
PreviousLatitude = prev(Latitude),
PreviousLongitude = prev(Longitude)
| where
AdminSurface != prev(AdminSurface) and
SessionId == prev(SessionId) and
ApplicationId != prev(ApplicationId) and
AdminSurface == 1
| where IsCompliant == 0
Getting started
Results
Query history
Export
Show empty columns
1 item
Search
00:00.751
Low
Chart type
Full screen
Filters:
Add filter
TimeGenerated
Timestamp
Application
ApplicationId
LogonType
EndpointCall
ErrorCode
Dec 5, 2025 10:06:...
Dec 5, 2025 10:06:49 PM
Microsoft Azure CLI
04b07795-8ddb-461a-b...
["interactiveUser"]
OAuth2:Authorize
0

WRAPPING THINGS UP

WRAP UP

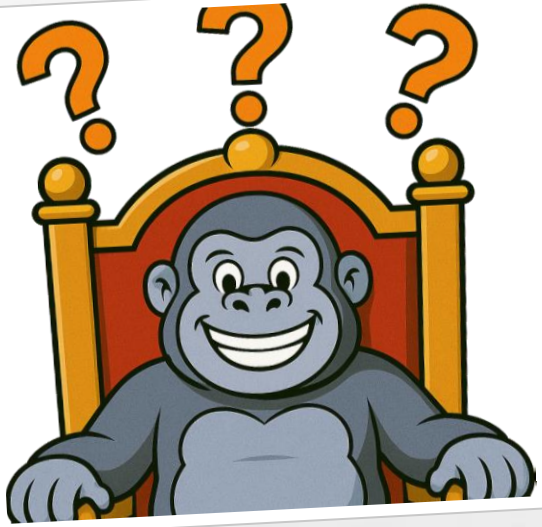
PREVENT LOG JUNGLE

USE GOOD DETECTION LOGIC

KNOW YOUR DATA

DEMO KQL

```
let AdminIds = dynamic([
"04b07795-8ddb-461a-bbee-02f9e1bf7b46", // (Azure CLI)
"1950a258-227b-4e31-a9cf-717495945fc2" // (Azure PowerShell)
]);
EntraIdSignInEvents
| where isnotempty( SessionId)
| extend AdminSurface = case(ApplicationId in(AdminIds), true, false)
| sort by AccountObjectId asc, SessionId asc, Timestamp asc
| extend PreviousApplication = prev(Application), PreviousApplicationId = prev(ApplicationId), PreviousLatitude = prev(Latitude), PreviousLongitude = prev(Longitude)
| where
AdminSurface != prev(AdminSurface) and SessionId == prev(SessionId) and ApplicationId != prev(ApplicationId) and AdminSurface == 1
| where IsCompliant == 0
```



ANY QUESTIONS