

BEFORE WE START...

- You'll need a computer/your laptop today
- Make an account for kc7cyber.com

KQL 101

KUSTO QUERY LANGUAGE

GrayHats
Cybersecurity Club
12/1/2023



TODAY'S AGENDA...

01

WHAT IS KQL?

02

WHY KQL?

03

HOW DO WE
USE KQL?

04

USING KQL ON
REAL DATA

WHAT IS KQL?

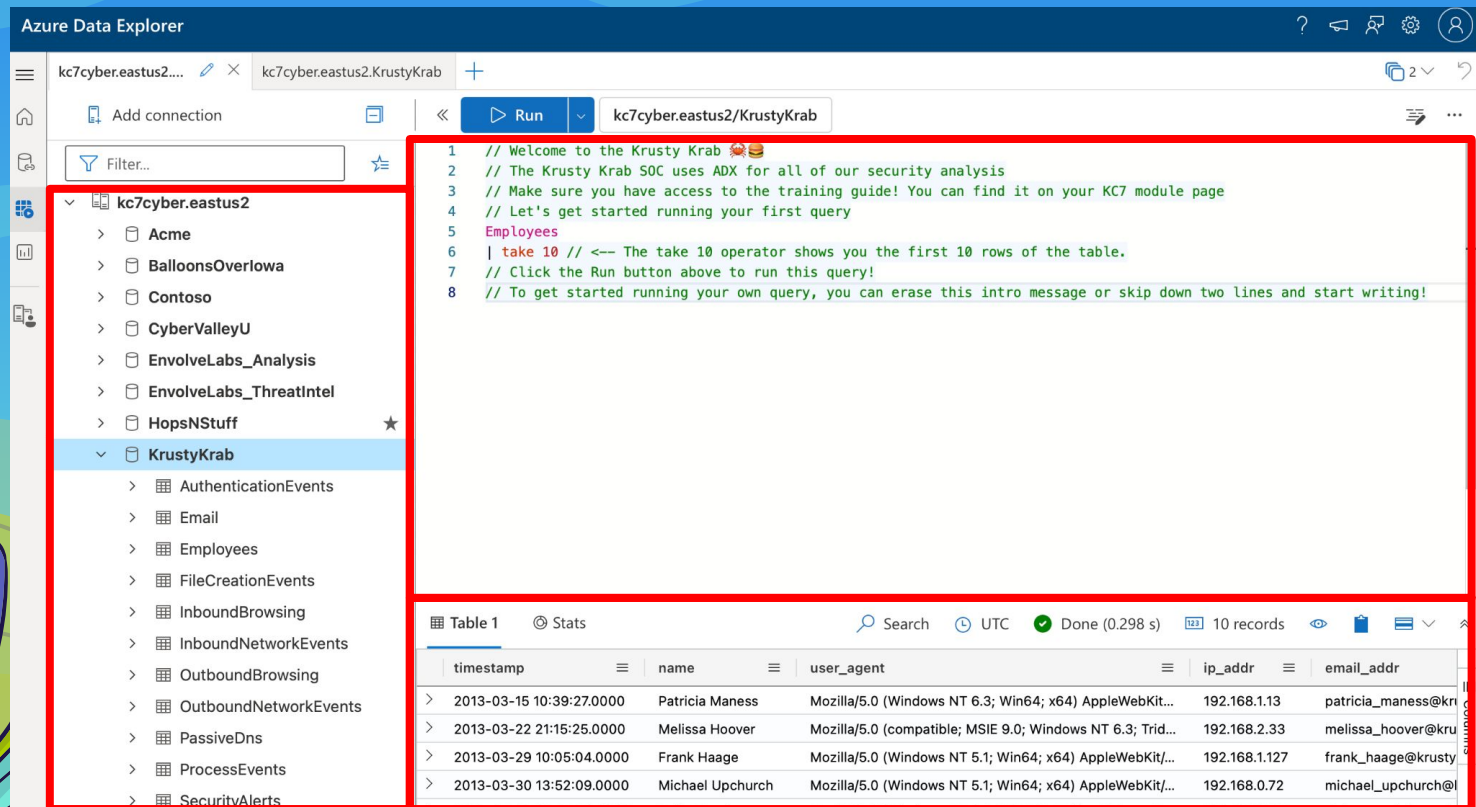
- Kusto Query Language
 - Similar concept to SQL
- Allows us to make a read-only request for data
- Developed for Microsoft's Azure Data Explorer

WHAT'S **AZURE** **DATA EXPLORER?**

- Data analysis tool for Azure
- “end-to-end solution for data ingestion, query, visualization, and management.”
- Uses traditional relational database type structure



AZURE DATA EXPLORER



The screenshot displays the Azure Data Explorer web application. The left sidebar shows a tree view of databases under the connection 'kc7cyber.eastus2'. The 'KrustyKrab' database is selected, revealing a list of tables including AuthenticationEvents, Email, Employees, FileCreationEvents, InboundBrowsing, InboundNetworkEvents, OutboundBrowsing, OutboundNetworkEvents, PassiveDns, ProcessEvents, and SecurityAlerts. The main pane shows a SQL query being executed against the 'KrustyKrab' database. The query is a simple SELECT statement with a comment. The results are displayed in a table format at the bottom of the interface.

Query:

```
1 // Welcome to the Krusty Krab 🍷🍷
2 // The Krusty Krab SOC uses ADX for all of our security analysis
3 // Make sure you have access to the training guide! You can find it on your KC7 module page
4 // Let's get started running your first query
5 Employees
6 | take 10 // <-- The take 10 operator shows you the first 10 rows of the table.
7 // Click the Run button above to run this query!
8 // To get started running your own query, you can erase this intro message or skip down two lines and start writing!
```

Results Table:

timestamp	name	user_agent	ip_addr	email_addr
2013-03-15 10:39:27.0000	Patricia Maness	Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit...	192.168.1.13	patricia_maness@kru...
2013-03-22 21:15:25.0000	Melissa Hoover	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.3; Trid...	192.168.2.33	melissa_hoover@kru...
2013-03-29 10:05:04.0000	Frank Haage	Mozilla/5.0 (Windows NT 5.1; Win64; x64) AppleWebKit/...	192.168.1.127	frank_haage@krusty...
2013-03-30 13:52:09.0000	Michael Upchurch	Mozilla/5.0 (Windows NT 5.1; Win64; x64) AppleWebKit/...	192.168.0.72	michael_upchurch@i...

WHY KNOW KQL?



SENTINEL

Cloud based system
that provides SIEM
and SOAR
functionalities



INCIDENT RESP

Microsoft's
cybersecurity tools
send data to Kusto
clusters



FASTER?

KQL can parse data
and convert the
data into something
meaningful

BUILT IN FUNCTIONALITIES

```
1 let SuspiciousPowerShell = datatable(command: string)[ '%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -encodedcommand H4sIAJktWAA/wWAMQ0AAAIAGtnJMT4DGJ+xx/gGM0rsYwgAAAA=' ];
2 SuspiciousPowerShell
3 | extend parsedCommandLine = parse_command_line(command, 'windows')
4 | extend suspiciousBase64 = toString(parsedCommandLine[-1])
5 | extend gunzipSuspiciousBase64 = gzip_decompress_from_base64_string(suspiciousBase64)
```

Table 1 Stats

command	parsedCommandLine	suspiciousBase64	gunzipSuspiciousBase64
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -encodedcommand H4sIAJktWAA/wWAMQ0AAAIAGtnJMT4DGJ+xx/gGM0rsYwgAAAA=	["%COMSPEC%", "/b", "/c", "start", "/b", "/min", "powershell.exe", "-nop", "-w", "hidden", "-encodedcommand", "H4sIAJktWAA/wWAMQ0AAAIAGtnJMT4DGJ+xx/gGM0rsYwgAAAA="]	H4sIAJktWAA/wWAMQ0AAAIAGtnJMT4DGJ+xx/gGM0rsYwgAAAA=	calc.exe

```
1 let data = datatable(SuspiciousPath: string)[@'C:\Windows\System32\evil.exe'];
2 data
3 | extend parsedPath = parse_path(SuspiciousPath)
4 | extend fileName = parsedPath.FileName
5 | extend Directory = parsedPath['DirectoryPath']
```

Table 1 Stats

SuspiciousPath	parsedPath	fileName	Directory
C:\Windows\System32\evil.exe	{'Scheme':"", 'RootPath': 'C:\\', 'DirectoryPath': 'C:\\Windows\\System32', 'DirectoryName': 'System32', 'Filename': 'evil.exe', 'Extension': '.exe', 'AlternateDataStreamName': ''}	evil.exe	C:\Windows\System32

```
1 let suspiciousUrl = (@'http://www.contoso.com:4444/c2/?ver=1.3.3.7&file=C:\Windows\temp\evil.exe');
2 print Results = parse_url(suspiciousUrl)
3 | extend Host = Results.Host
4 | extend Parameter1 = Results['Query Parameters']['ver']
5 | extend Parameter2 = Results['Query Parameters']['file']
```

Table 1 Stats

Results	Host	Parameter1	Parameter2
{'Scheme': 'http', 'Host': 'www.contoso.com', 'Port': '4444', 'Path': '/c2/', 'Username': '', 'Password': '', 'Query Parameters': {'ver': '1.3.3.7', 'file': 'C:\\Windows\\temp\\evil.exe'}, 'Fragment': ''}	www.contoso.com	1.3.3.7	C:\Windows\temp\evil.exe

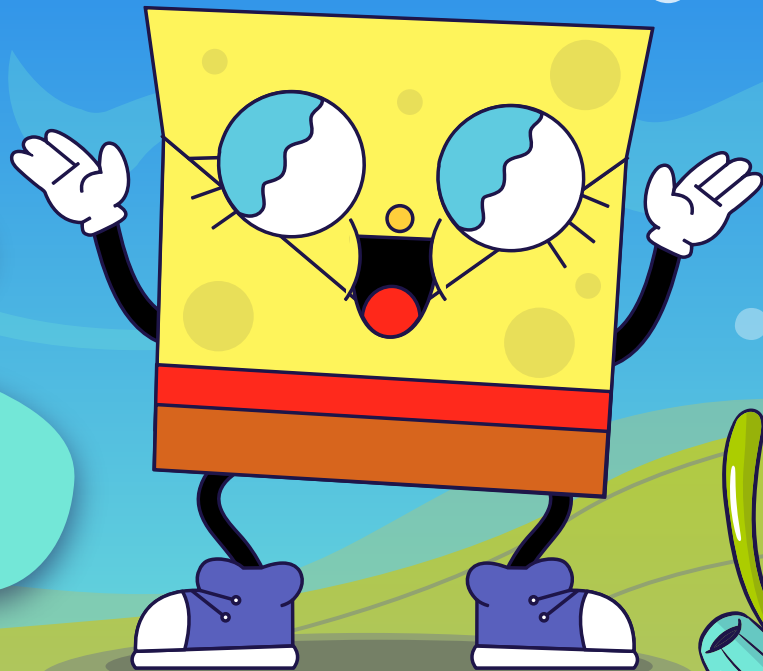
RECREATING POWERSHELL SCRIPTS

```
1 .create-or-alter function with (docstring = "Reconstruct PowerShell script from script block logging. The required ScriptBlockId parameter takes a GUID as a string") RecreateScriptFromScriptBlocks(ScriptBlockId:string) {  
2     EventLogs  
3     | where LogName == "Microsoft-Windows-PowerShell/Operational" and EventId == 4104  
4     | where Message contains ScriptBlockId  
5     | distinct *  
6     | extend Blocks = toint(extract(@"Creating Scriptblock text \\\d+ of \d+):\s+", 1, Message))  
7     | extend TotalBlocks = toint(extract(@"Creating Scriptblock text \\\d+ of \d+):\s+", 1, Message))  
8     | order by Blocks asc  
9     | extend trimStart = trim(@"Creating Scriptblock text \\\d+ of \d+):\s+", Message)  
10    | extend ScriptBlock = replace(@"\s+(ScriptBlock ID[Path]\[UserId]:.+)", "", trimStart)  
11    | extend Script = ''  
12    | evaluate python(  
13        //  
14        typeof(*),  
15        //  
16        'result = df\\n'  
17        'finalScript = []\\n'  
18        'for i in range(df.shape[0]):\\n'  
19        '    block = result.loc[i, "ScriptBlock"]\\n'  
20        '    finalScript.append(block)\\n'  
21        'sb = "".join(finalScript)\\n'  
22        'for i in range(df.shape[0]):\\n'  
23        '    result.loc[i, "Script"] = sb\\n'  
24    )  
25    | project SystemName, TimeCreated, Script, ScriptBlockId  
26    | distinct *  
27 }
```

Table 1

SystemName	TimeCreated	Script
system.contoso.com	2021-02-05 14:39:48.0000	#requires -version 3.0 try { [Microsoft.PowerShell.Core\Set-StrictMode -Off] catch {} } \$script:MyModule = \$MyInvocation.MyCommand.ScriptBlock.Module \$script:ClassName = 'ROOT/Microsoft/Windows/Storage/MSFT_Volume' \$s

KQL SYNTAX



KQL SYNTAX

1 Employees ← Table Name

2 | take 10

! "Pipe" Character

↑
Operator

COMMONLY USED OPERATORS

TAKE

Returns # amount of records from DB

COUNT

Returns the number of records from prev operation

WHERE

Filters the records by field

DISTINCT

Returns only unique records

LET

Used to create variables

- has
- contains
- ==
- in