KQL Café – January 2024 | 3 Years

Your | hosts

Alex Verboon

https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

Microsoft® MVP Most Valuable Professional

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

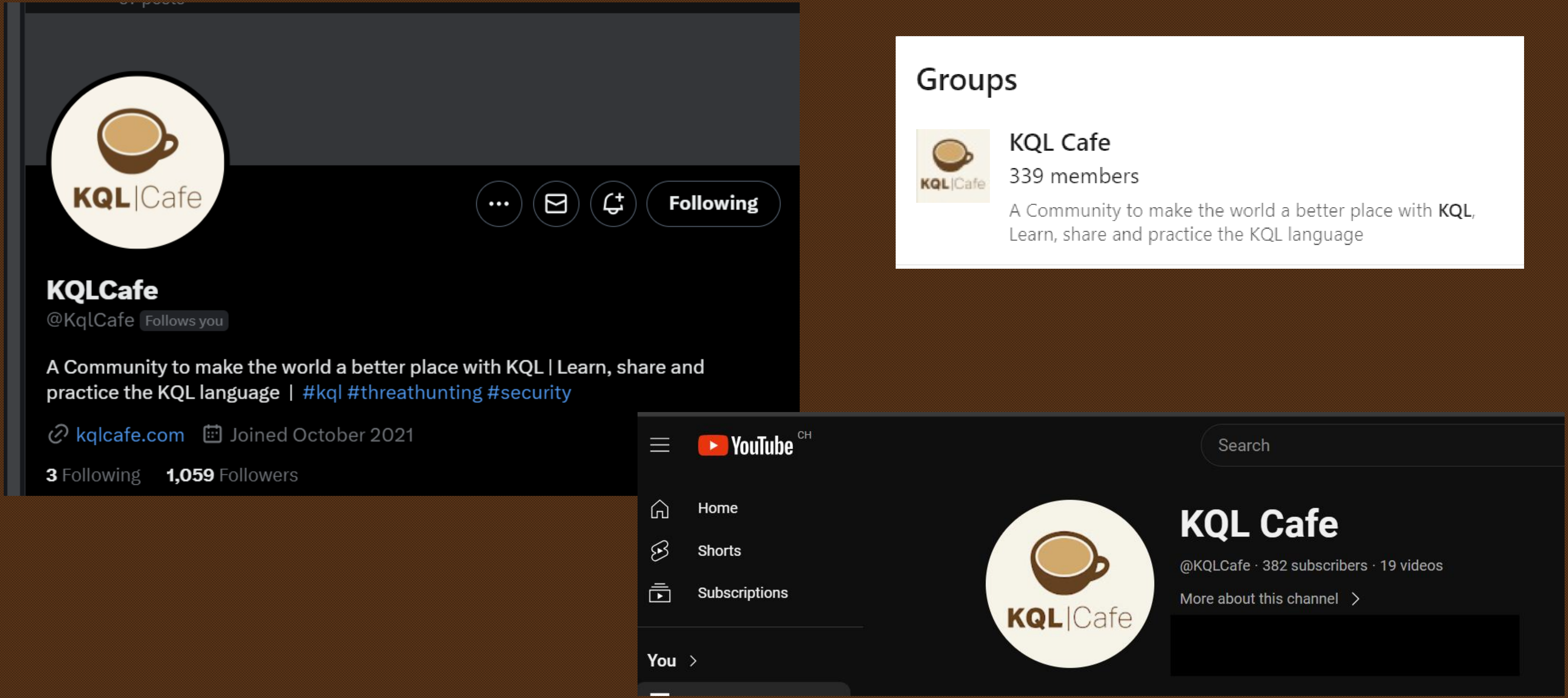
What is new/updates for KQL

Our guest: Ilana Waitser

Learning KQL

What did you do with KQL this month?

Thank you



KQLCafe

@KqlCafe Follows you

A Community to make the world a better place with KQL | Learn, share and practice the KQL language | #kql #threathunting #security

kqlcafe.com Joined October 2021

3 Following 1,059 Followers

Groups

KQL Cafe

339 members

A Community to make the world a better place with **KQL**, Learn, share and practice the KQL language

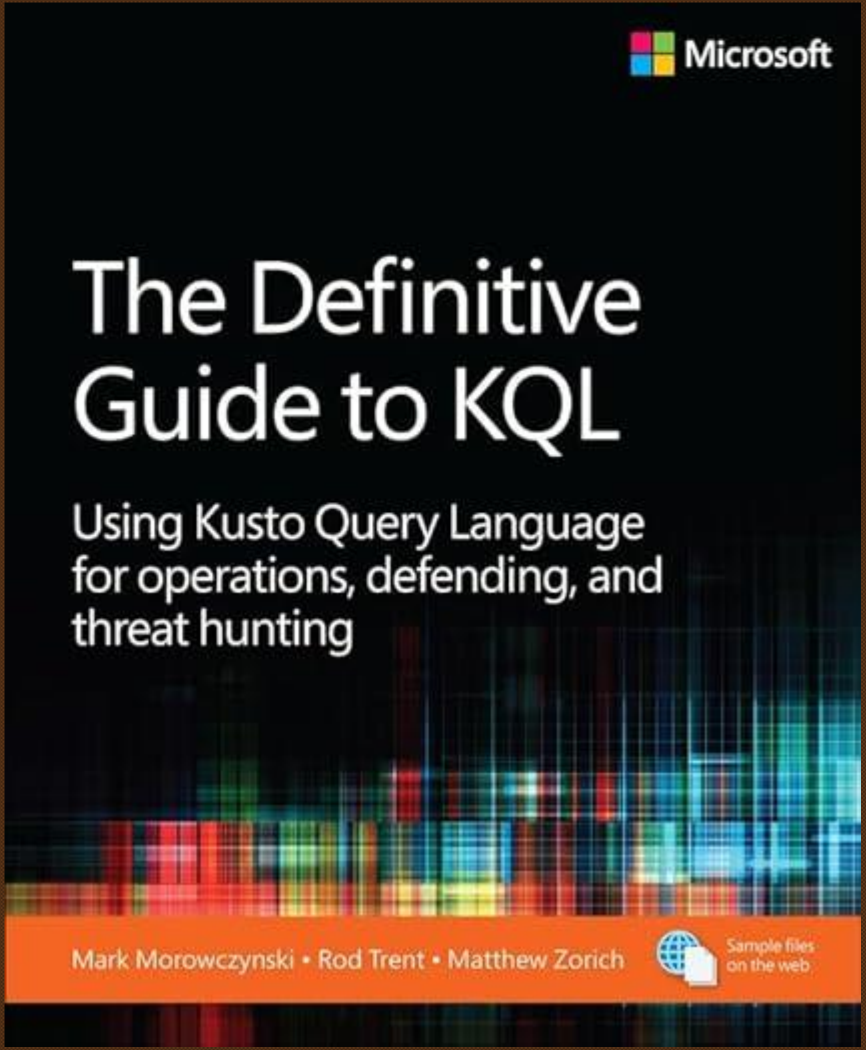
KQL Cafe

@KQLCafe · 382 subscribers · 19 videos

More about this channel >

[redacted]

What's New –Books

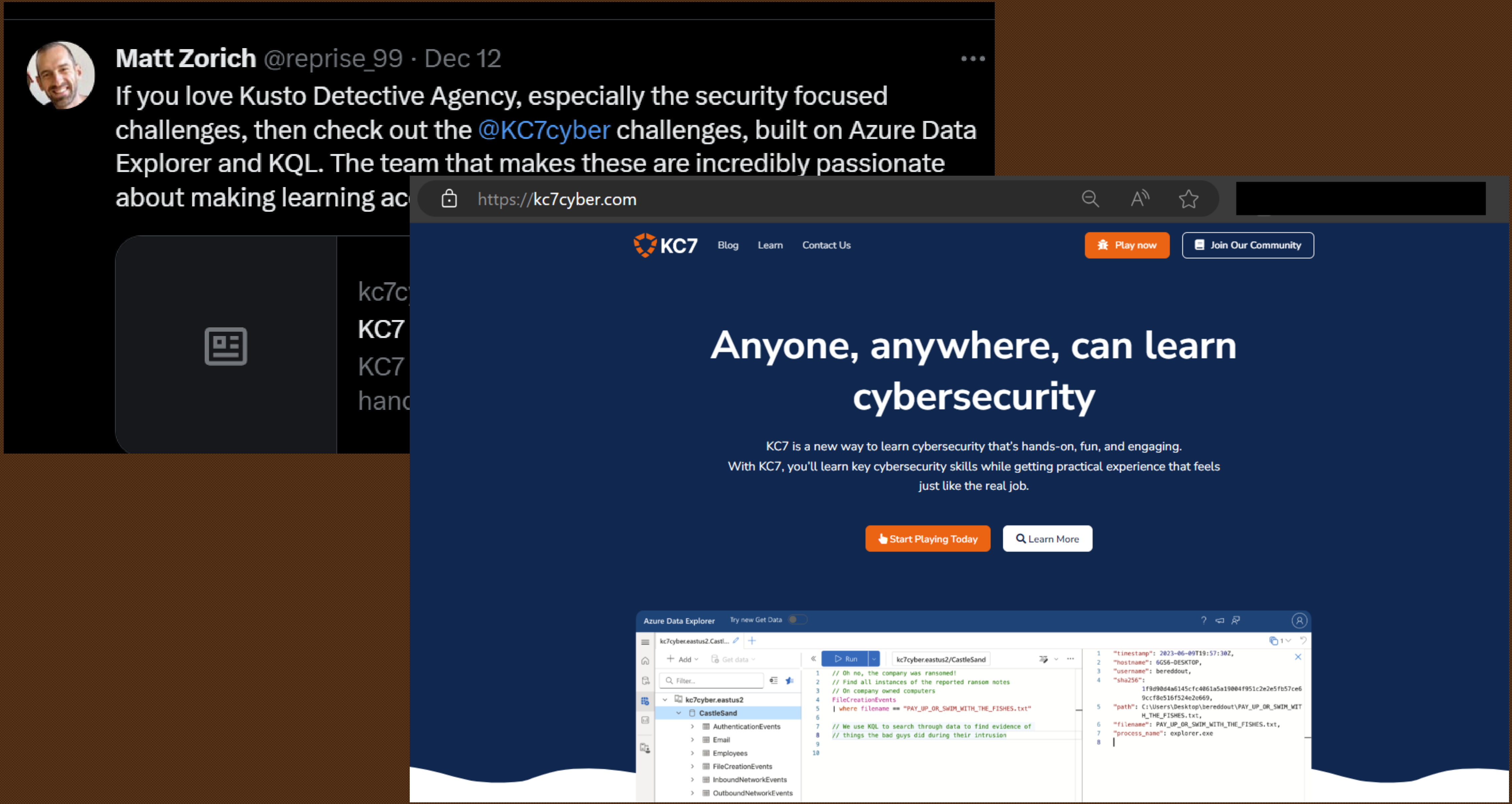

Microsoft
The Definitive Guide to KQL
Using Kusto Query Language for operations, defending, and threat hunting
Mark Morowczynski • Rod Trent • Matthew Zorich
Sample files on the web

The Definitive Guide to KQL: Using Kusto Query Language for Operations, Defending, and Threat Hunting 1

https://www.amazon.com/Definitive-Guide-Kql-Operations-Defending/dp/0138293384

Publishing Date: March 31, 2024

What's New – Training



Matt Zorich @reprise_99 · Dec 12

If you love Kusto Detective Agency, especially the security focused challenges, then check out the @KC7cyber challenges, built on Azure Data Explorer and KQL. The team that makes these are incredibly passionate about making learning ac

kc7c

KC7

KC7

hand

https://kc7cyber.com

[redacted]

Anyone, anywhere, can learn cybersecurity

KC7 is a new way to learn cybersecurity that's hands-on, fun, and engaging.
With KC7, you'll learn key cybersecurity skills while getting practical experience that feels just like the real job.

```
// Oh no, the company was ransomed!
// Find all instances of the reported ransom notes
// On company owned computers
FileCreationEvents
| where filename == "PAY_UP_OR_SWIM_WITH_THE_FISHES.txt"

// We use KQL to search through data to find evidence of
// things the bad guys did during their intrusion
```

```
"timestamp": 2023-06-09T19:57:30Z,
"hostname": 6GS6-DESKTOP,
"username": bereddout,
"sha256":
        1f9d90d4a6145cfc4061a5a19004f951c2e2e5fb57ce6
        9ccf8e516f524e2e669,
"path": C:\Users\Desktop\bereddout\PAY_UP_OR_SWIM_WIT
        H_THE_FISHES.txt,
"filename": PAY_UP_OR_SWIM_WITH_THE_FISHES.txt,
"process_name": explorer.exe
```

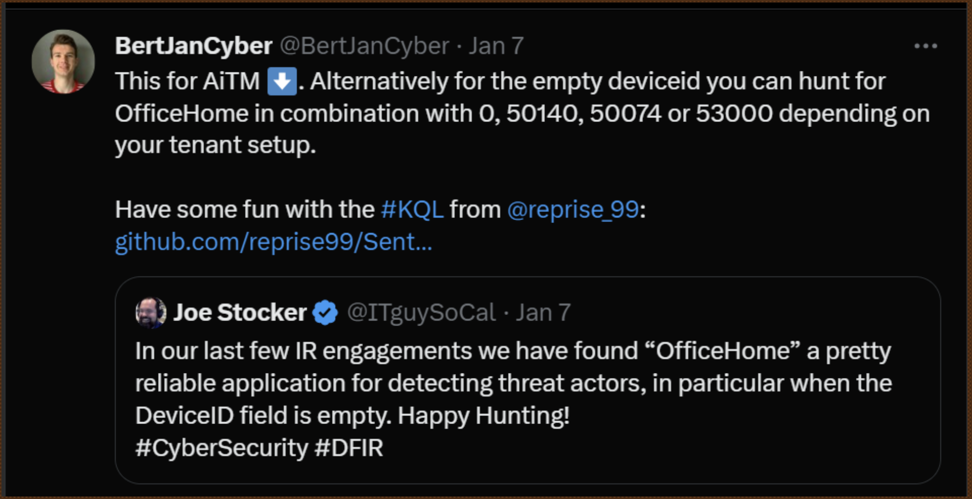
Notable Articles & Queries

KQL Security Sources - 2024 Update
https://kqlquery.com/posts/kql-sources-2024-update/

A Deep Dive into the KQL Union Operator
https://posts.bluraven.io/a-deep-dive-into-the-kql-union-operator-9f16f0ed0a66

Extracting Nested Fields in Kusto
https://www.cloudsma.com/2024/01/extracting-nested-fields-in-kusto-2-0/

Harnessing threat intelligence using externaldata operator
https://www.michalos.net/2024/01/22/harnessing-threat-intelligence-using-externaldata-operator/



BertJanCyber @BertJanCyber · Jan 7

This for AiTM ⬇. Alternatively for the empty deviceid you can hunt for OfficeHome in combination with 0, 50140, 50074 or 53000 depending on your tenant setup.

Have some fun with the #KQL from @reprise_99: github.com/reprise99/Sent...

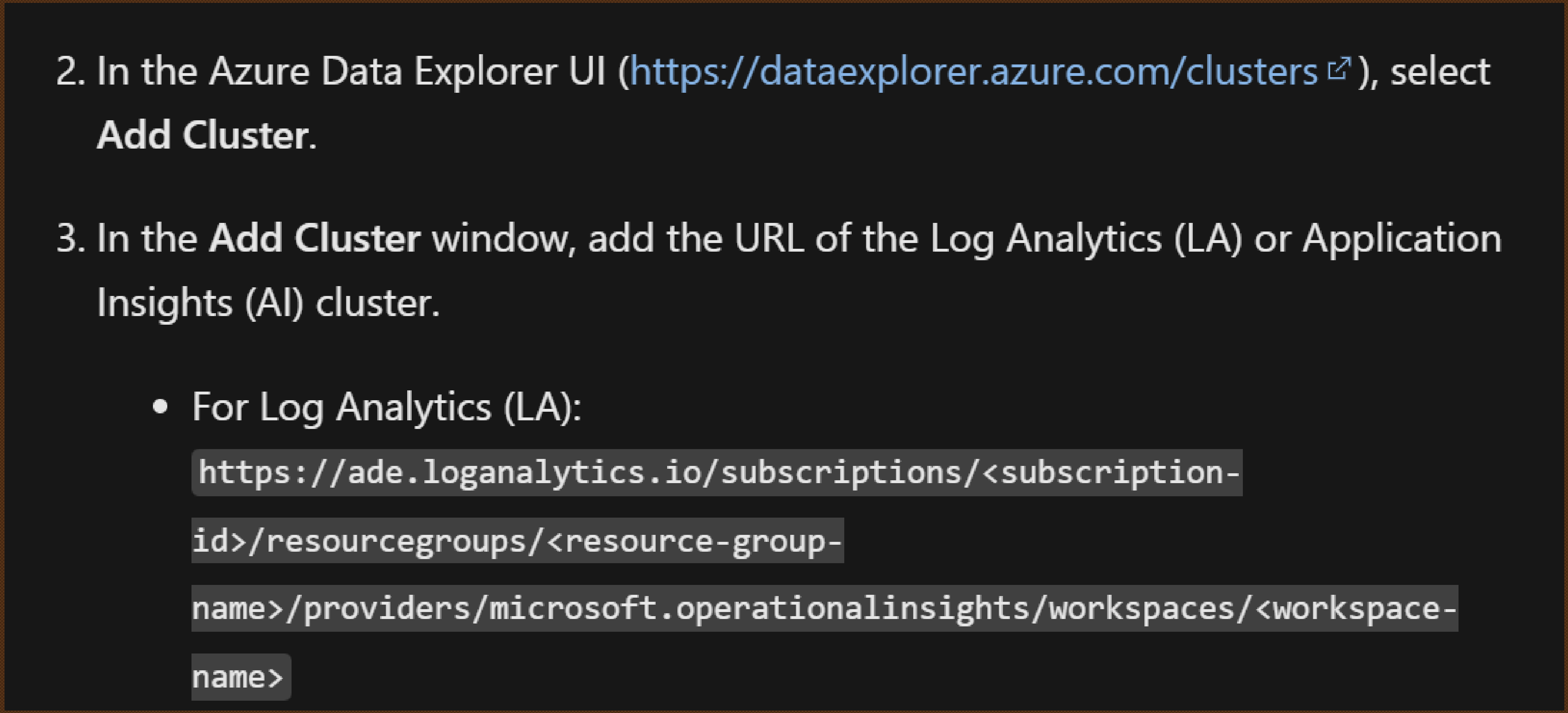
Joe Stocker @ITguySoCal · Jan 7

In our last few IR engagements we have found “OfficeHome” a pretty reliable application for detecting threat actors, in particular when the DeviceID field is empty. Happy Hunting! #CyberSecurity #DFIR

https://github.com/reprise99/Sentinel-Queries/blob/main/Azure%20Active%20Directory/Identity-PotentialAiTM.kql

Tip – Connect Kusto Explorer to Log Analytics Workspace

Query data in Azure Monitor using Azure Data Explorer
https://learn.microsoft.com/en-us/azure/data-explorer/query-monitor-data

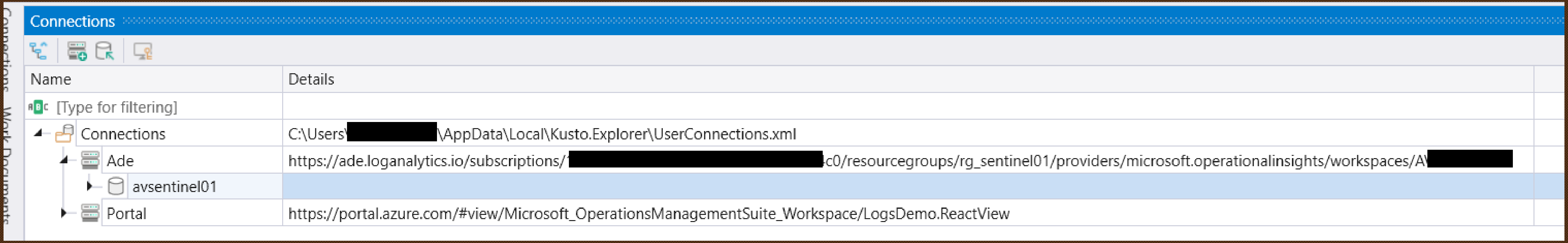


2. In the Azure Data Explorer UI (https://dataexplorer.azure.com/clusters), select **Add Cluster**.

3. In the **Add Cluster** window, add the URL of the Log Analytics (LA) or Application Insights (AI) cluster.

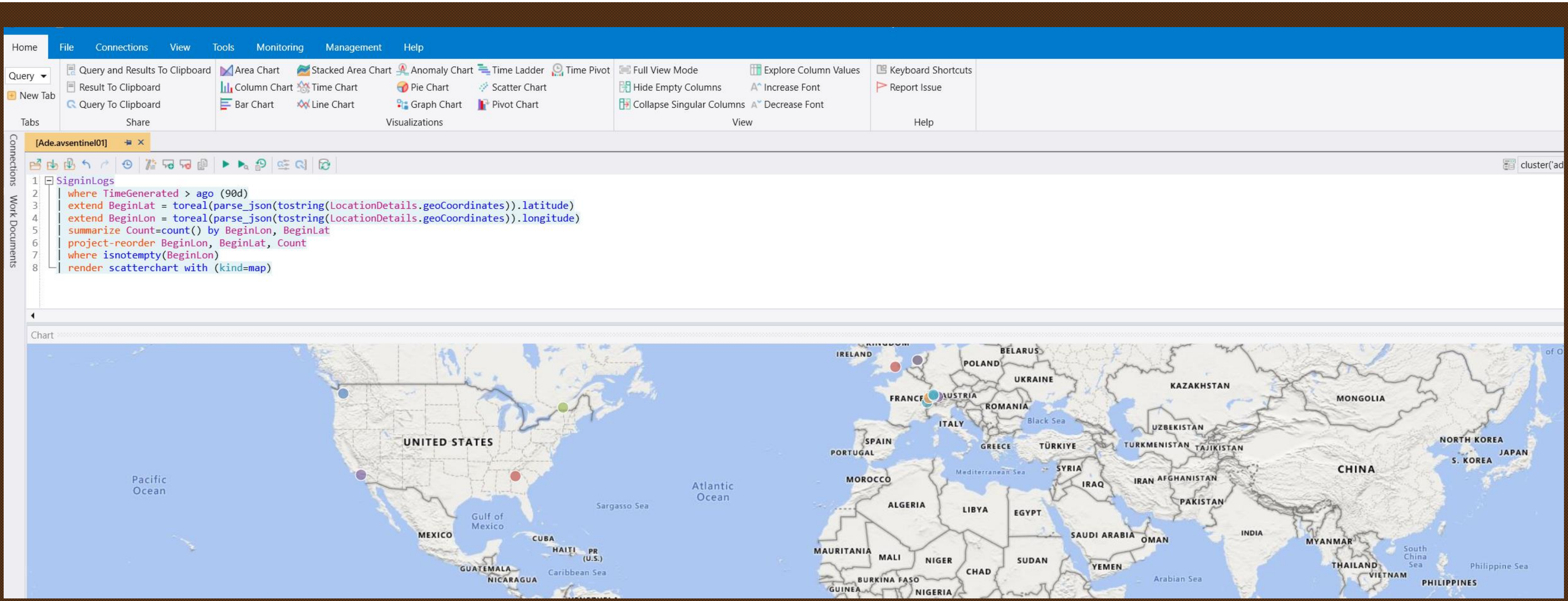
   - For Log Analytics (LA): `https://ade.loganalytics.io/subscriptions/<subscription-id>/resourcegroups/<resource-group-name>/providers/microsoft.operationalinsights/workspaces/<workspace-name>`

Tip – Connect Kusto Explorer to Log Analytics Workspace



Connections

Name	Details
[Type for filtering]	
Connections	C:\Users\[redacted]\AppData\Local\Kusto.Explorer\UserConnections.xml
Ade	https://ade.loganalytics.io/subscriptions/[redacted]c0/resourcegroups/rg_sentinel01/providers/microsoft.operationalinsights/workspaces/A[redacted]
avsentinel01	
Portal	https://portal.azure.com/#view/Microsoft_OperationsManagementSuite_Workspace/LogsDemo.ReactView



```
SigninLogs
| where TimeGenerated > ago (90d)
| extend BeginLat = toreal(parse_json(tostring(LocationDetails.geoCoordinates)).latitude)
| extend BeginLon = toreal(parse_json(tostring(LocationDetails.geoCoordinates)).longitude)
| summarize Count=count() by BeginLon, BeginLat
| project-reorder BeginLon, BeginLat, Count
| where isnotempty(BeginLon)
| render scatterchart with (kind=map)
```

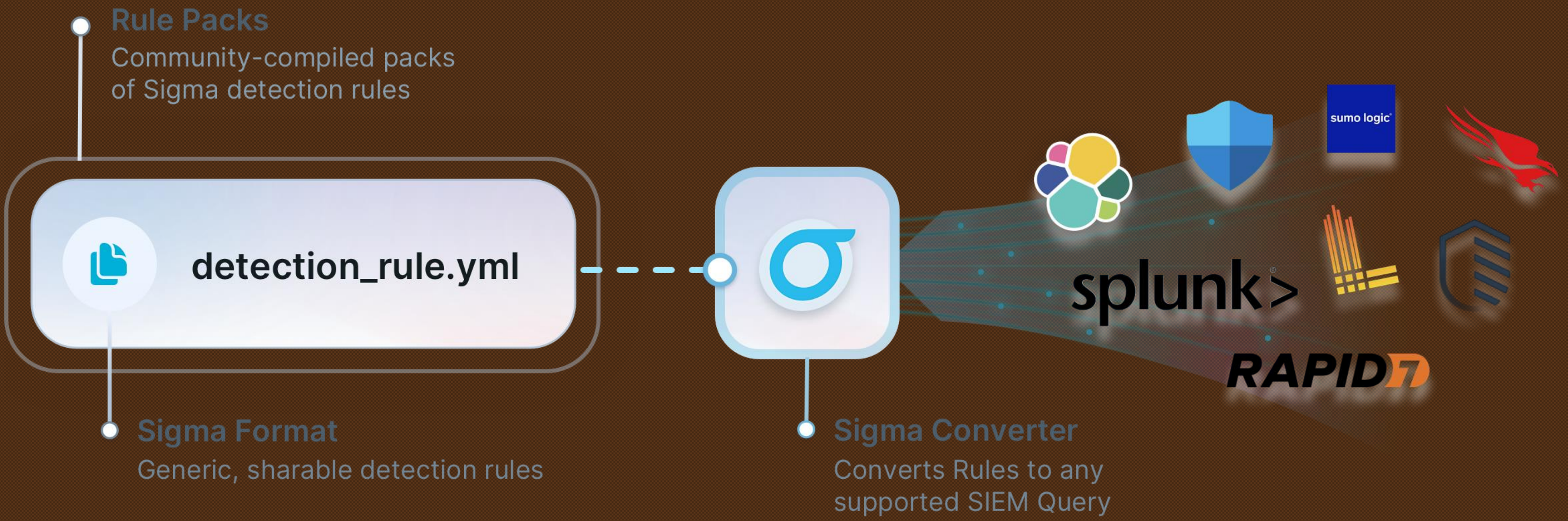
Our Guest:

Ilana Waitser

Senior PM (Program & Product Manager) - Azure Monitor / Log Analytics

Learning KQL

What is Sigma


Rule Packs
Community-compiled packs of Sigma detection rules
detection_rule.yml
Sigma Format
Generic, sharable detection rules
Sigma Converter
Converts Rules to any supported SIEM Query
sumo logic
splunk>
RAPID7

Learning KQL

Converting Sigma to KQL Online

https://sigconverter.io/

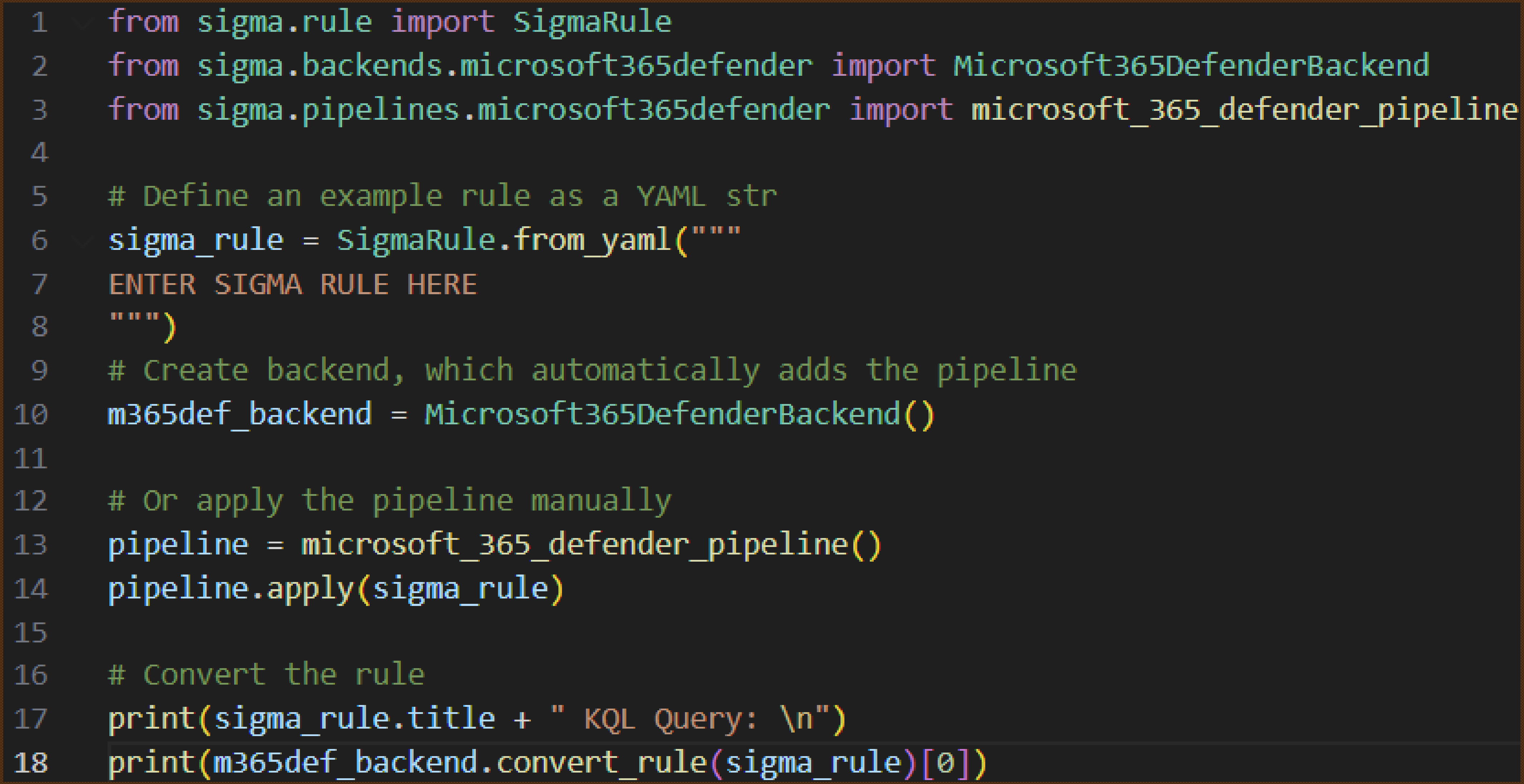
Learning KQL

Sigma to KQL Backend

https://github.com/AttackIQ/pySigma-backend-microsoft365defender/

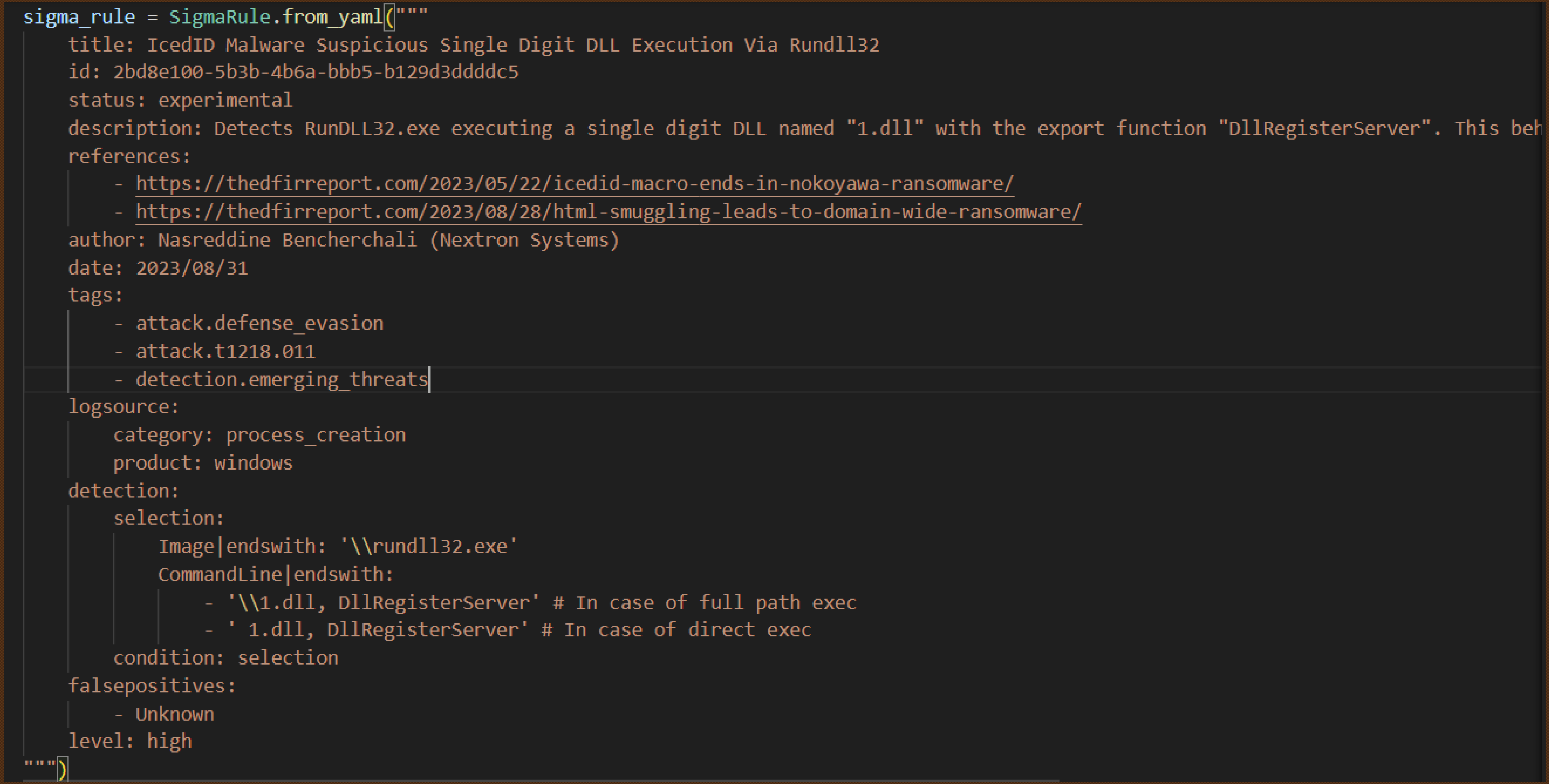
Thanks AttackIQ and Stephen Lincoln

Learning KQL

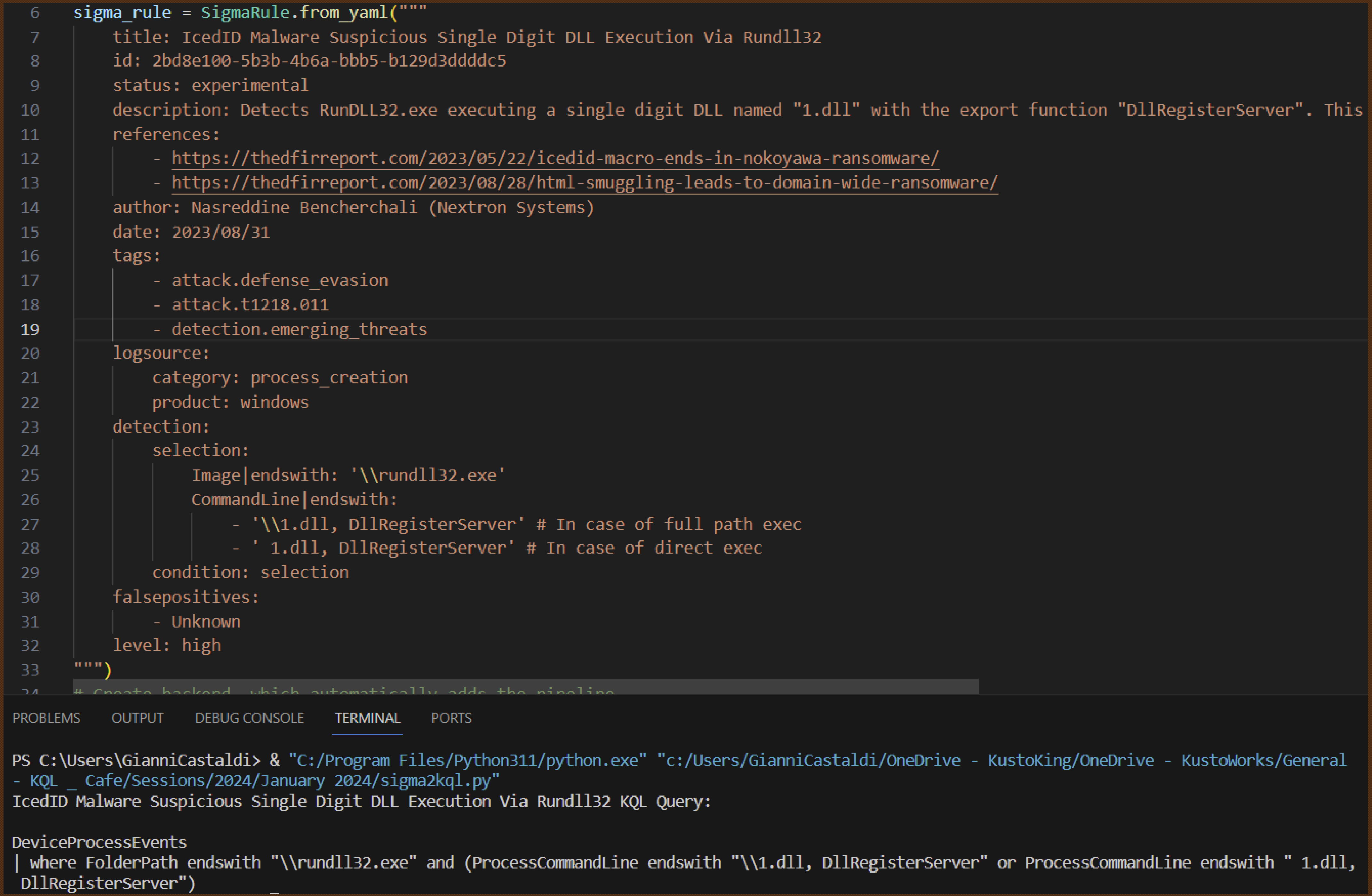


```python
from sigma.rule import SigmaRule
from sigma.backends.microsoft365defender import Microsoft365DefenderBackend
from sigma.pipelines.microsoft365defender import microsoft_365_defender_pipeline

# Define an example rule as a YAML str
sigma_rule = SigmaRule.from_yaml("""
ENTER SIGMA RULE HERE
""")
# Create backend, which automatically adds the pipeline
m365def_backend = Microsoft365DefenderBackend()

# Or apply the pipeline manually
pipeline = microsoft_365_defender_pipeline()
pipeline.apply(sigma_rule)

# Convert the rule
print(sigma_rule.title + " KQL Query: \n")
print(m365def_backend.convert_rule(sigma_rule)[0])
```

Learning KQL



```
sigma_rule = SigmaRule.from_yaml("""
    title: IcedID Malware Suspicious Single Digit DLL Execution Via Rundll32
    id: 2bd8e100-5b3b-4b6a-bbb5-b129d3ddddc5
    status: experimental
    description: Detects RunDLL32.exe executing a single digit DLL named "1.dll" with the export function "DllRegisterServer". This beh
    references:
        - https://thedfirreport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/
        - https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/
    author: Nasreddine Bencherchali (Nextron Systems)
    date: 2023/08/31
    tags:
        - attack.defense_evasion
        - attack.t1218.011
        - detection.emerging_threats
    logsource:
        category: process_creation
        product: windows
    detection:
        selection:
            Image|endswith: '\\rundll32.exe'
            CommandLine|endswith:
                - '\\1.dll, DllRegisterServer' # In case of full path exec
                - ' 1.dll, DllRegisterServer' # In case of direct exec
        condition: selection
    falsepositives:
        - Unknown
    level: high
""")
```

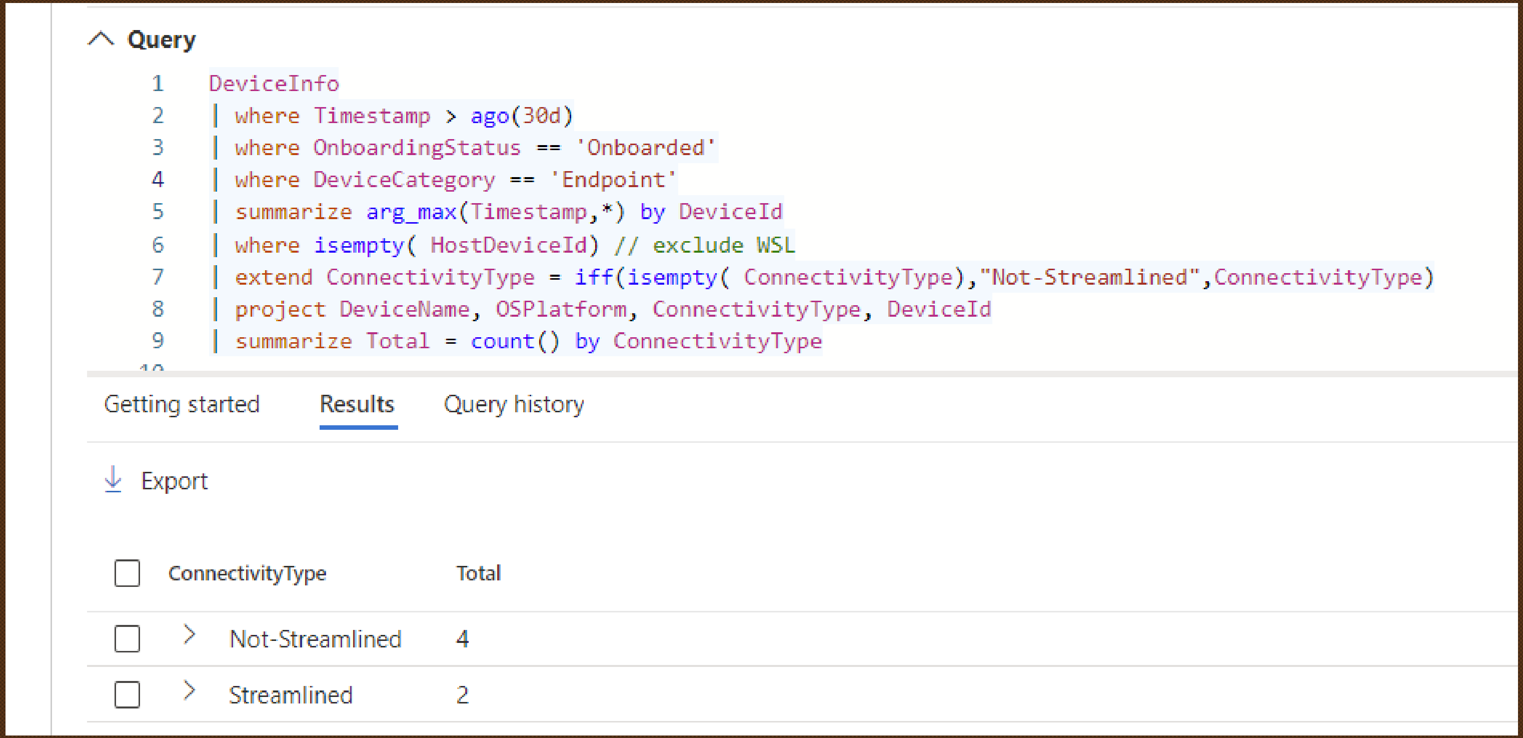


```
sigma_rule = SigmaRule.from_yaml("""
    title: IcedID Malware Suspicious Single Digit DLL Execution Via Rundll32
    id: 2bd8e100-5b3b-4b6a-bbb5-b129d3ddddc5
    status: experimental
    description: Detects RunDLL32.exe executing a single digit DLL named "1.dll" with the export function "DllRegisterServer". This
    references:
        - https://thedfirreport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/
        - https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/
    author: Nasreddine Bencherchali (Nextron Systems)
    date: 2023/08/31
    tags:
        - attack.defense_evasion
        - attack.t1218.011
        - detection.emerging_threats
    logsource:
        category: process_creation
        product: windows
    detection:
        selection:
            Image|endswith: '\\rundll32.exe'
            CommandLine|endswith:
                - '\\1.dll, DllRegisterServer' # In case of full path exec
                - ' 1.dll, DllRegisterServer' # In case of direct exec
        condition: selection
    falsepositives:
        - Unknown
    level: high
""")
# Create backend, which automatically adds the pipeline
```

```
PS C:\Users\GianniCastaldi> & "C:/Program Files/Python311/python.exe" "c:/Users/GianniCastaldi/OneDrive - KustoKing/OneDrive - KustoWorks/General
- KQL _ Cafe/Sessions/2024/January 2024/sigma2kql.py"
IcedID Malware Suspicious Single Digit DLL Execution Via Rundll32 KQL Query:

DeviceProcessEvents
| where FolderPath endswith "\\rundll32.exe" and (ProcessCommandLine endswith "\\1.dll, DllRegisterServer" or ProcessCommandLine endswith " 1.dll,
 DllRegisterServer")
```

What did you do with KQL this month?

Microsoft Defender for Endpoint – Streamlined Connectivity Monitoring



```
DeviceInfo
| where Timestamp > ago(30d)
| where OnboardingStatus == 'Onboarded'
| where DeviceCategory == 'Endpoint'
| summarize arg_max(Timestamp,*) by DeviceId
| where isempty( HostDeviceId) // exclude WSL
| extend ConnectivityType = iff(isempty( ConnectivityType),"Not-Streamlined",ConnectivityType)
| project DeviceName, OSPlatform, ConnectivityType, DeviceId
| summarize Total = count() by ConnectivityType
```

ConnectivityType	Total
Not-Streamlined	4
Streamlined	2

https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Endpoint/MDE-ConnectivityType.md

Or just use www.kqlsearch.com

What did you do with KQL this month?

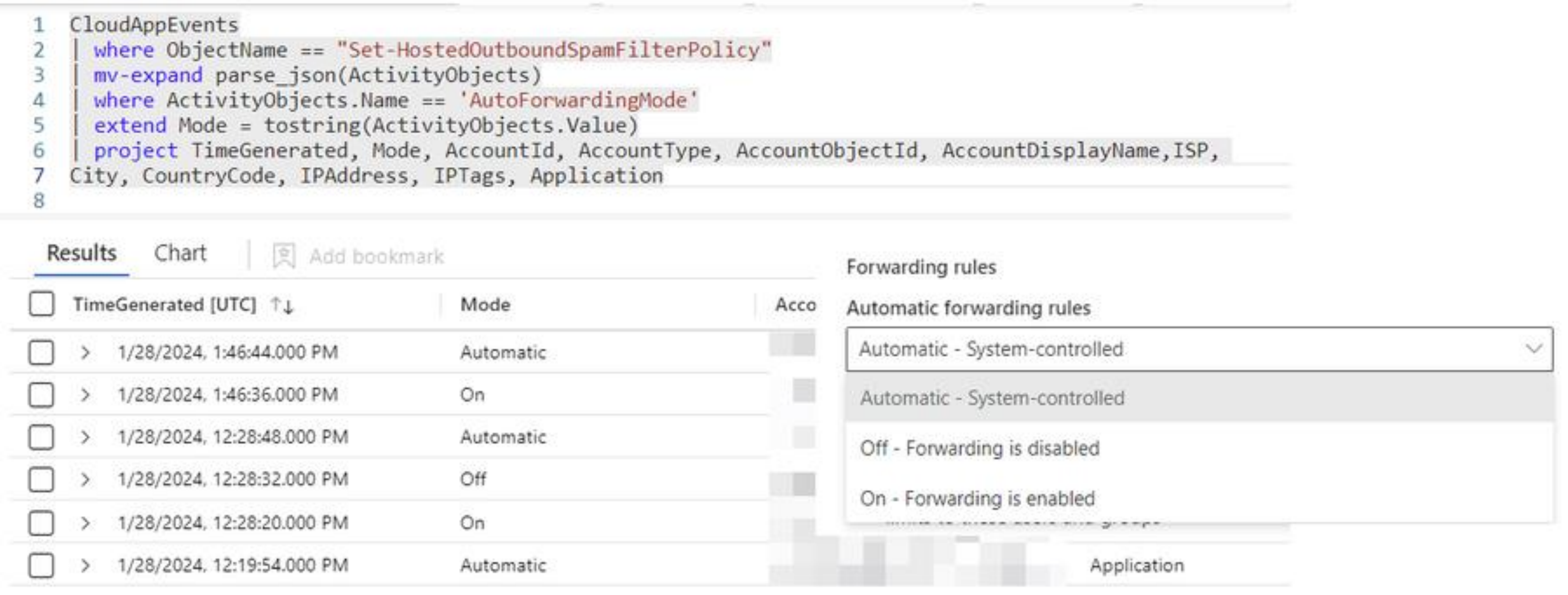
Microsoft Defender XDR – Threat Protection Reporting

Microsoft announced that they will be retiring the Threat Protection report page - https://security.microsoft.com/mde-reports/threatProtection (accessed through Reports > Endpoints > Threat protection). Instead, they recommend the utilization of Advanced hunting queries and Alert queue filter in Defender XDR.

https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20365/MDXDR-ThreatProtectionReport.md

What did you do with KQL this month?

Detecting Defender 365 Forwarding Rules policy changes



```
CloudAppEvents
| where ObjectName == "Set-HostedOutboundSpamFilterPolicy"
| mv-expand parse_json(ActivityObjects)
| where ActivityObjects.Name == 'AutoForwardingMode'
| extend Mode = tostring(ActivityObjects.Value)
| project TimeGenerated, Mode, AccountId, AccountType, AccountObjectId, AccountDisplayName,ISP,
City, CountryCode, IPAddress, IPTags, Application
```

□	TimeGenerated [UTC] ↑↓	Mode	Acco
□	1/28/2024, 1:46:44.000 PM	Automatic	[redacted]
□	1/28/2024, 1:46:36.000 PM	On	[redacted]
□	1/28/2024, 12:28:48.000 PM	Automatic	[redacted]
□	1/28/2024, 12:28:32.000 PM	Off	[redacted]
□	1/28/2024, 12:28:20.000 PM	On	[redacted]
□	1/28/2024, 12:19:54.000 PM	Automatic	[redacted]

Forwarding rules

Automatic forwarding rules

Automatic - System-controlled

- Automatic - System-controlled
- Off - Forwarding is disabled
- On - Forwarding is enabled

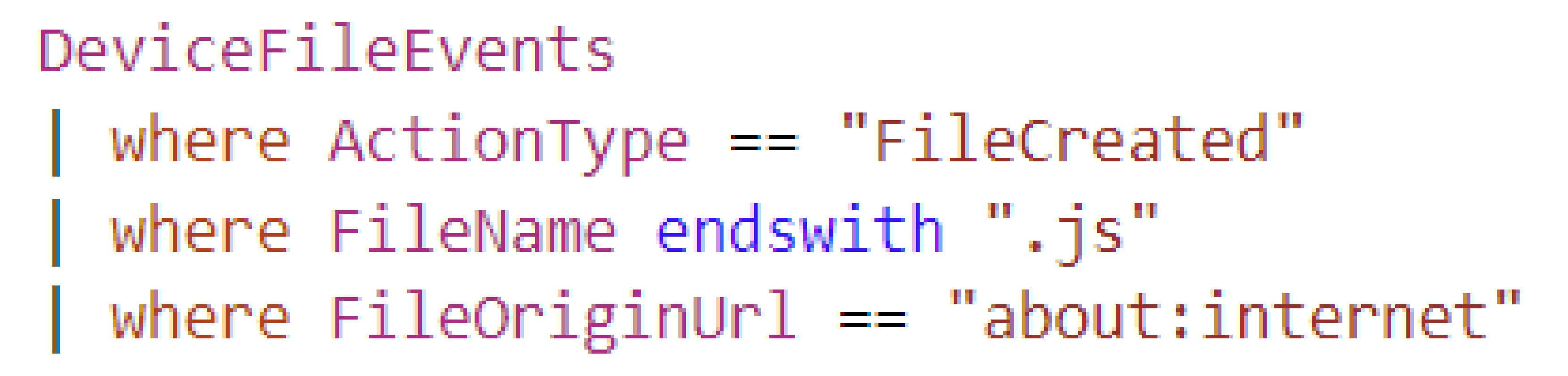
https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Office%20365/MDO-InboxForwarding.md

What did you do with KQL this month?

HTML smuggling detecting Socgolish

What did you do with KQL this month?

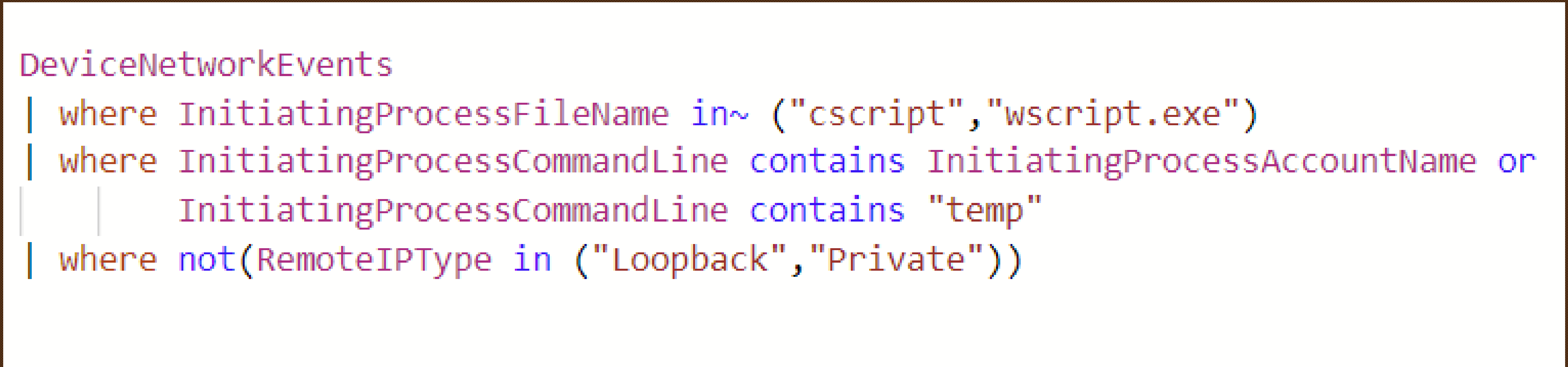
HTML smuggling detecting Socgolish



```
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName endswith ".js"
| where FileOriginUrl == "about:internet"
```

https://www.microsoft.com/en-us/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/

What did you do with KQL this month?



```
DeviceNetworkEvents
| where InitiatingProcessFileName in~ ("cscript","wscript.exe")
| where InitiatingProcessCommandLine contains InitiatingProcessAccountName or
        InitiatingProcessCommandLine contains "temp"
| where not(RemoteIPType in ("Loopback","Private"))
```

Thanks for attending

KQL|Cafe