KQL Café | October 2024

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/

KQL|Cafe

Show | Agenda

Welcome

What is new/updates for KQL

Our guest: *Koos Goossens*

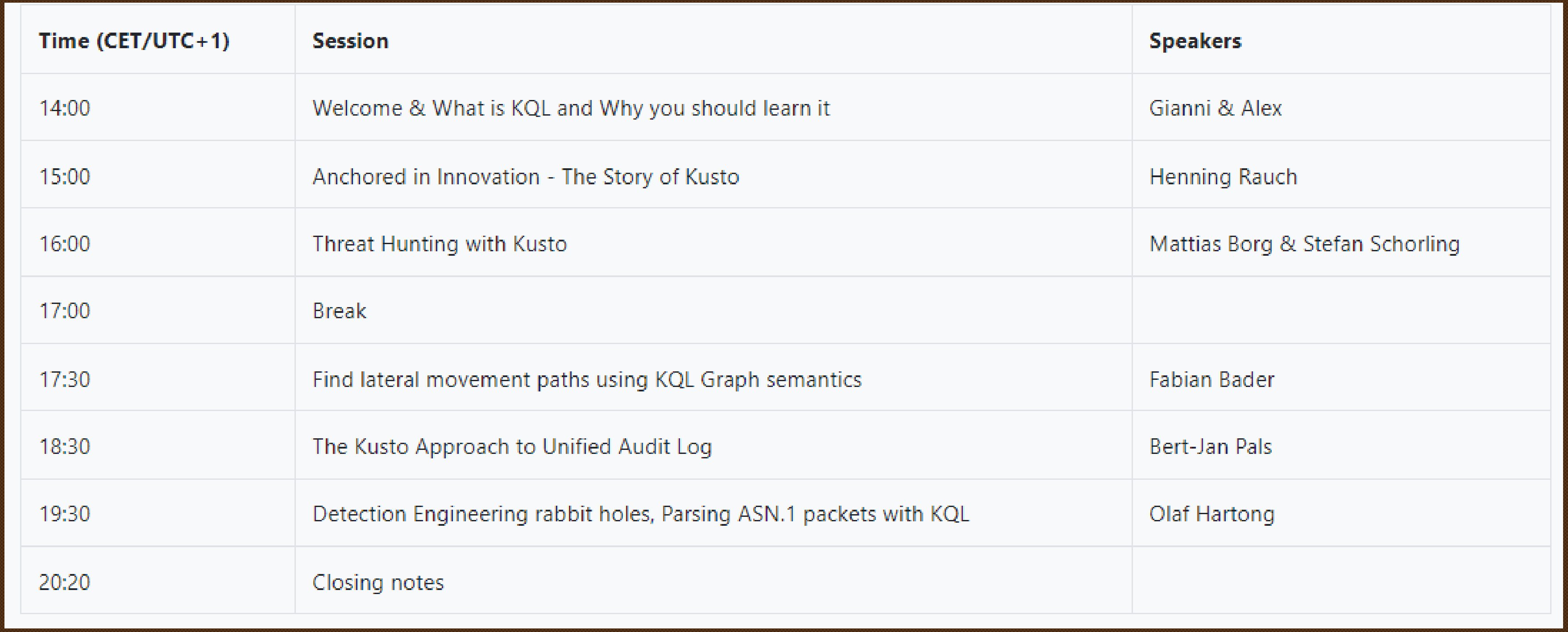
Learning KQL

What did you do with KQL this month?

KustoCon

Learn | Share | Practice

November 8th, 2024



Time (CET/UTC+1)	Session	Speakers
14:00	Welcome & What is KQL and Why you should learn it	Gianni & Alex
15:00	Anchored in Innovation - The Story of Kusto	Henning Rauch
16:00	Threat Hunting with Kusto	Mattias Borg & Stefan Schorling
17:00	Break	
17:30	Find lateral movement paths using KQL Graph semantics	Fabian Bader
18:30	The Kusto Approach to Unified Audit Log	Bert-Jan Pals
19:30	Detection Engineering rabbit holes, Parsing ASN.1 packets with KQL	Olaf Hartong
20:20	Closing notes	

More info's and registration https://kustocon.com/

News

MC906487 - Microsoft Defender XDR: InitiatingProcessFolderPath changes to include file names

https://mc.merill.net/message/MC906487

Microsoft Defender for Endpoint will update the **InitiatingProcessFolderPath** to include file names in all tables, affecting Windows activity. This change will be globally available on November 4, 2024, requiring updates to custom detection rules and queries.

News

MC906487 - Microsoft Defender XDR: InitiatingProcessFolderPath changes to include file names

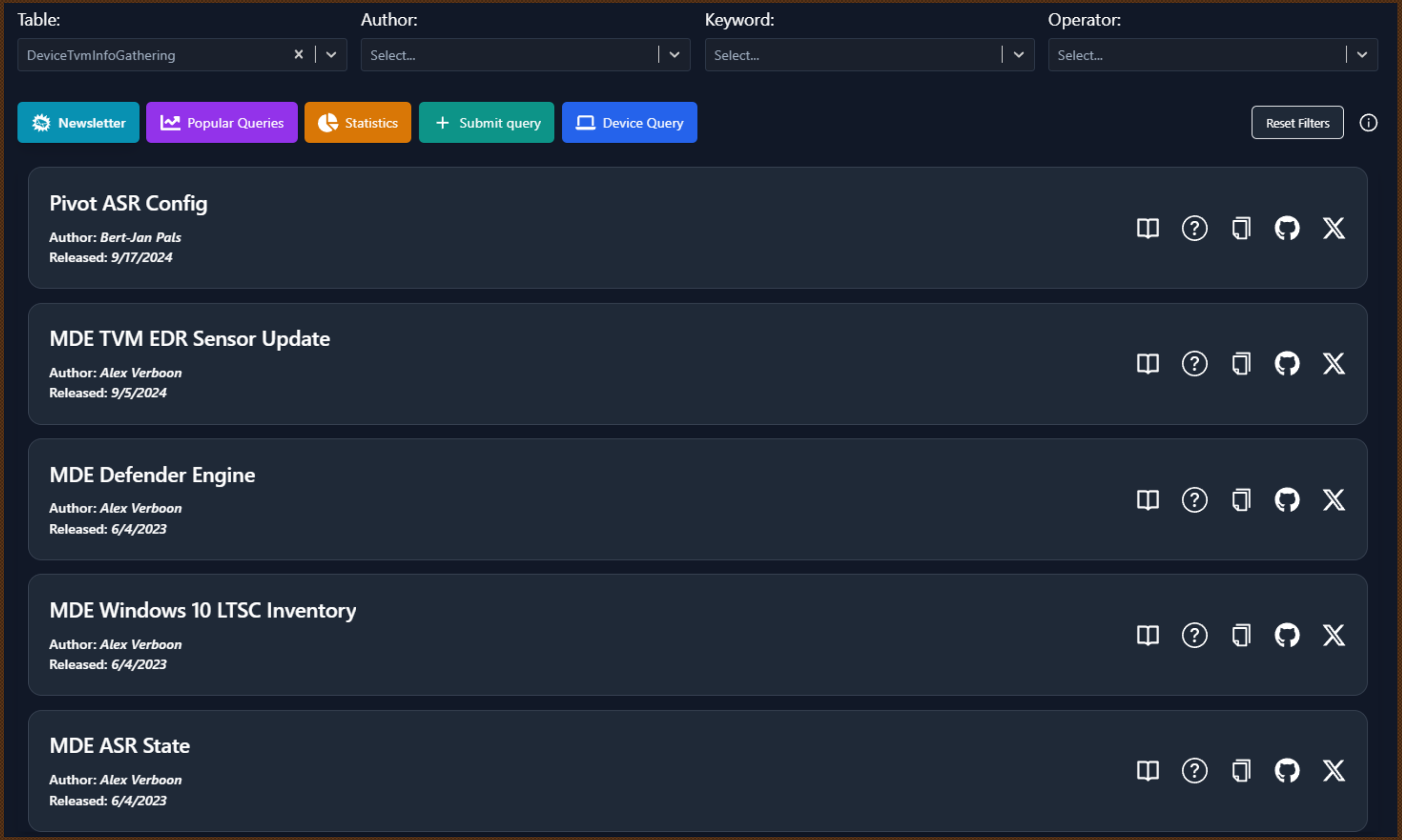
- **Before** this rollout, the **InitiatingProcessFolderPath** column is inconsistent across action types. Some columns include the file name, and other columns do not include the file name.
- **After** the rollout, all Microsoft Defender for Endpoint action types across all tables will report the full path including the file name of the initiating process in the InitiatingProcessFolderPath column.

Consider the following example to be the new normal, InitiatingProcessFolderPath ==
c:\temp\file.exe
An example of a possible current implementation that will be retired with this change:
InitiatingProcessFolderPath == c:\temp\
Custom detection rules and queries considering the InitiatingProcessFolderPath may be affected.

News

Unleash The Power Of DeviceTvmInfoGathering

https://kqlquery.com/posts/devicetvminfogathering/



Pivot ASR Config
Author: *Bert-Jan Pals*
Released: *9/17/2024*

MDE TVM EDR Sensor Update
Author: *Alex Verboon*
Released: *9/5/2024*

MDE Defender Engine
Author: *Alex Verboon*
Released: *6/4/2023*

MDE Windows 10 LTSC Inventory
Author: *Alex Verboon*
Released: *6/4/2023*

MDE ASR State
Author: *Alex Verboon*
Released: *6/4/2023*

News

Rod Trent shared his session content from the Midwest Management Summit Flamingo Edition 2024

Slides and Demo Query’s

https://github.com/rod-trent/JunkDrawer/tree/main/MMSFlamingo2024

News

KQL Threathunting with JohnDCyber

https://github.com/johdcyber/KQL_threathunting_with_john_d_cyber

Explore a collection of KQL queries crafted for dynamic threat hunting across a diverse range of topics, techniques, and use cases! These queries are designed as your launchpad - ready to be tailored to your unique environment and evolving threat landscape.

News

Azure-MFA-Enforcement

https://github.com/nicolonsky/ITDR/blob/main/Queries/Azure-MFA-Enforcement.md#check-the-current-mfa-requirement-provider-for-portals

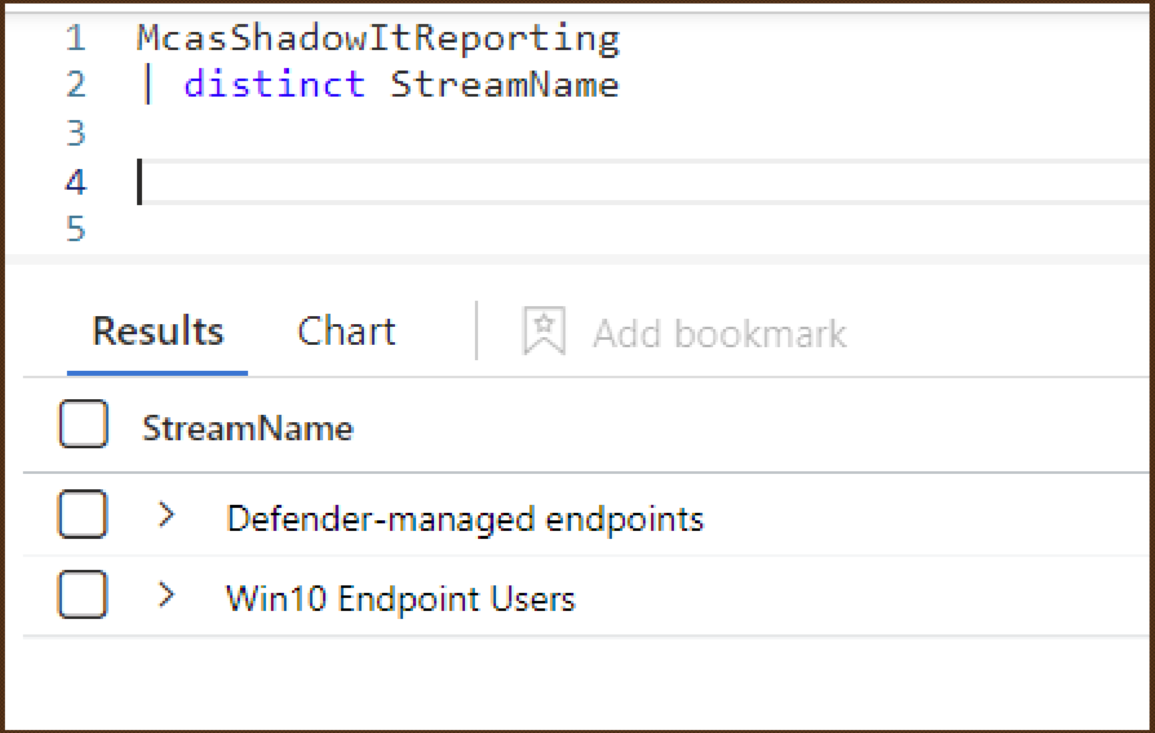
Planning for mandatory multifactor authentication for Azure and other admin portals

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication

News

Defender for Cloud Apps – Shadow Reporting

If you have queries on McasShadowItReporting note the value change for the StreamName for MDE data



```
McasShadowItReporting
| distinct StreamName
```

□ StreamName

□ > Defender-managed endpoints

□ > Win10 Endpoint Users

Our Guest:

Koos Goossens

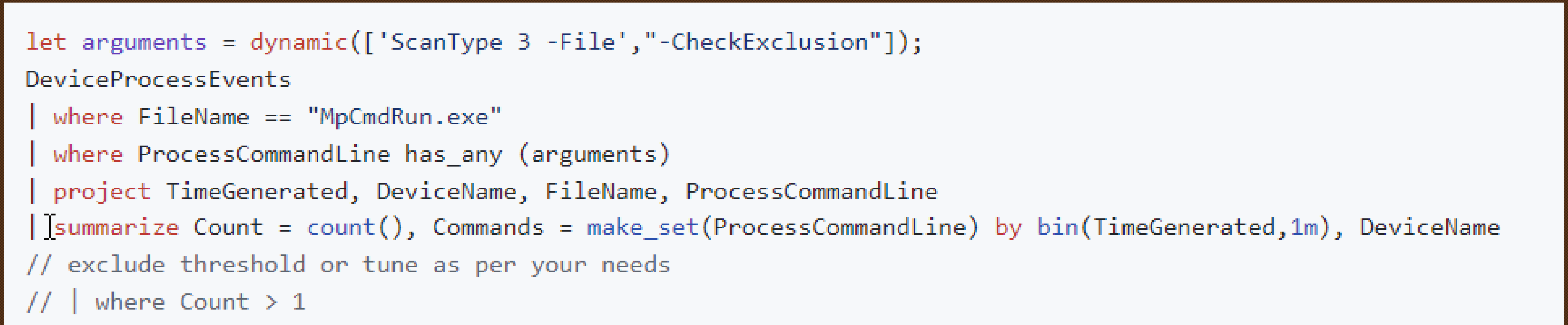
Microsoft Security MVP | Azure | Sentinel | Defender XDR

What did you do with KQL this month?

MDE - Defender Antivirus Exclusion Enumeration activities

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

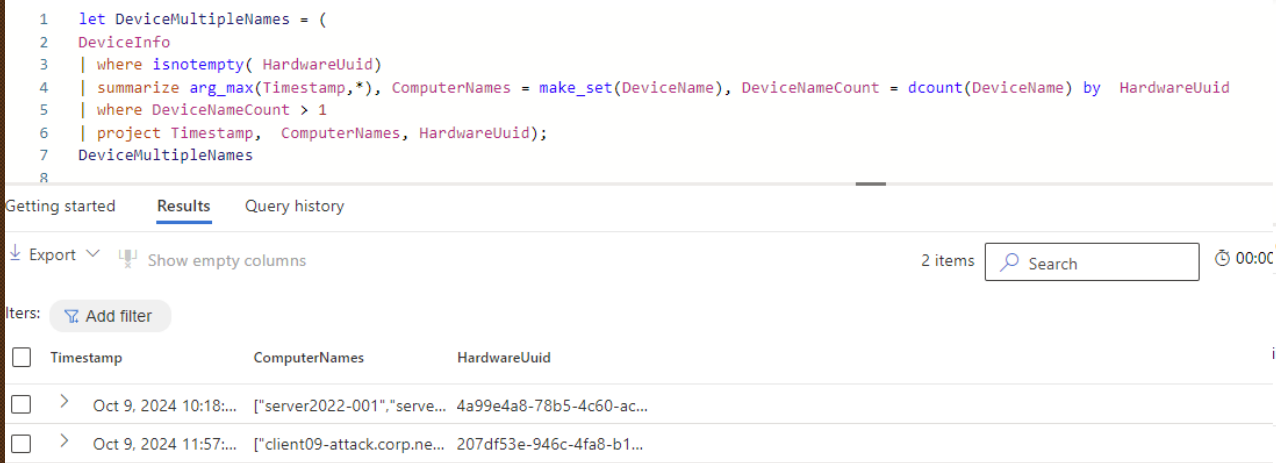
Identify Defender Antivirus Exclusion Path enumeration activities that use the mpcmdrun.exe



```
let arguments = dynamic(['ScanType 3 -File',"-CheckExclusion"]);
DeviceProcessEvents
| where FileName == "MpCmdRun.exe"
| where ProcessCommandLine has_any (arguments)
| project TimeGenerated, DeviceName, FileName, ProcessCommandLine
| summarize Count = count(), Commands = make_set(ProcessCommandLine) by bin(TimeGenerated,1m), DeviceName
// exclude threshold or tune as per your needs
// | where Count > 1
```

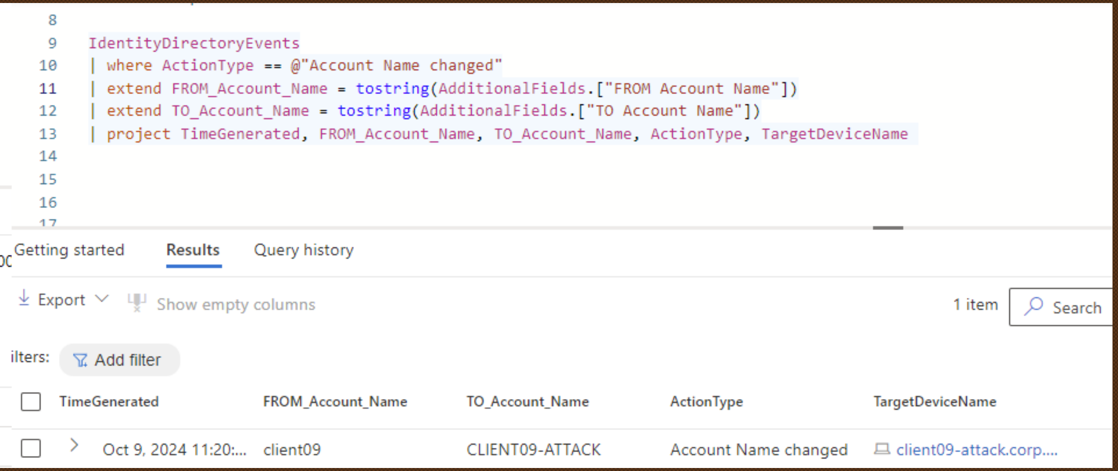
What did you do with KQL this month?
Mitigations for CVE-2024-38124 - Implement monitoring for any suspicious renaming activities of computers within the network

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



```
let DeviceMultipleNames = (
DeviceInfo
| where isnotempty( HardwareUuid)
| summarize arg_max(Timestamp,*), ComputerNames = make_set(DeviceName), DeviceNameCount = dcount(DeviceName) by  HardwareUuid
| where DeviceNameCount > 1
| project Timestamp,  ComputerNames, HardwareUuid);
DeviceMultipleNames
```

Timestamp	ComputerNames	HardwareUuid
Oct 9, 2024 10:18:...	["server2022-001","serve...	4a99e4a8-78b5-4c60-ac...
Oct 9, 2024 11:57:...	["client09-attack.corp.ne...	207df53e-946c-4fa8-b1...



```
IdentityDirectoryEvents
| where ActionType == @"Account Name changed"
| extend FROM_Account_Name = tostring(AdditionalFields.["FROM Account Name"])
| extend TO_Account_Name = tostring(AdditionalFields.["TO Account Name"])
| project TimeGenerated, FROM_Account_Name, TO_Account_Name, ActionType, TargetDeviceName
```

TimeGenerated	FROM_Account_Name	TO_Account_Name	ActionType	TargetDeviceName
Oct 9, 2024 11:20:...	client09	CLIENT09-ATTACK	Account Name changed	client09-attack.corp....

What did you do with KQL this month?
Contribution from: Loris Ambrozzo (@LorisAmbrozzo)

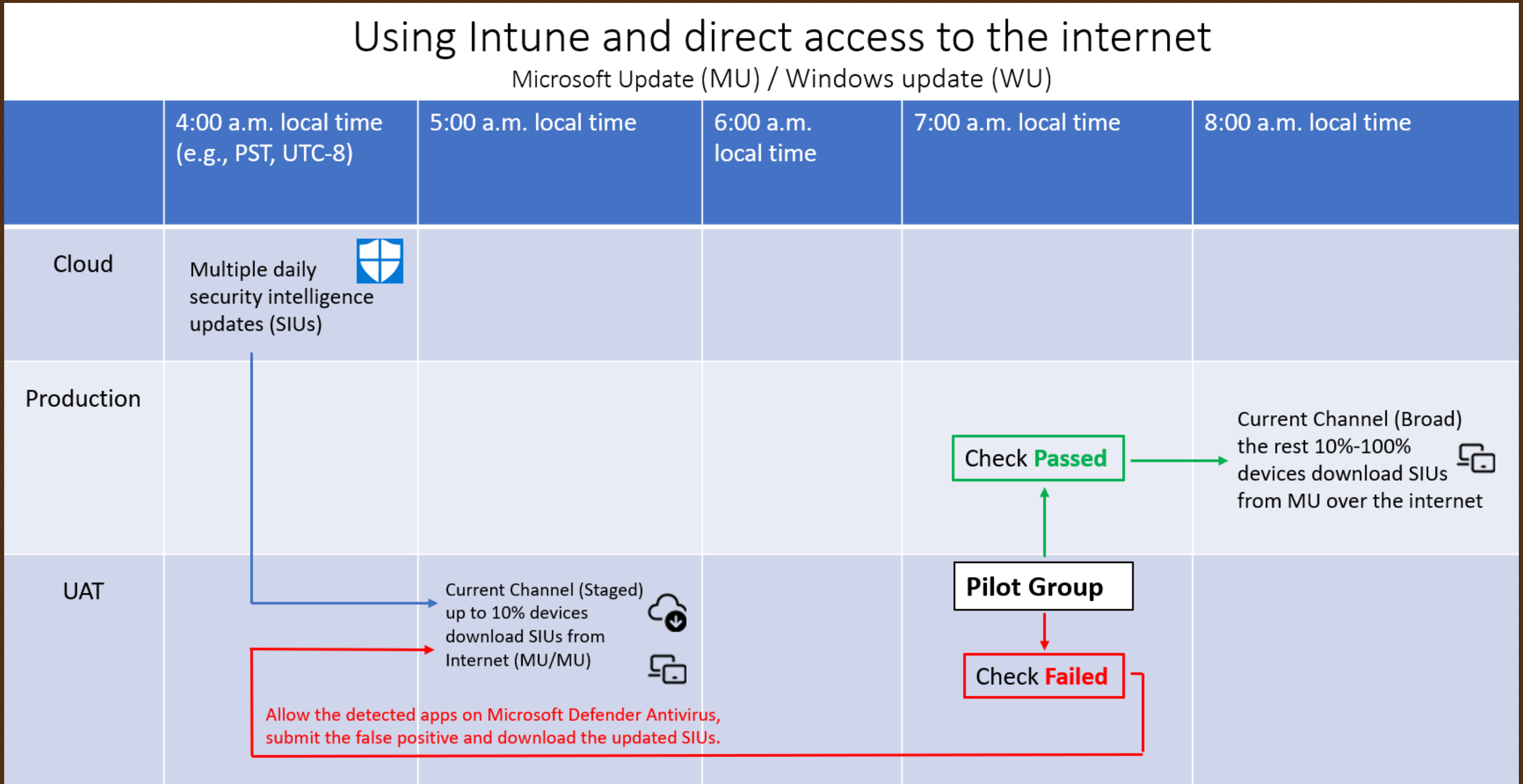
MDE-DefaultLocalAdmin-Logon

This KQL query identifies logon events for the default local administrator (.\Administrator) with SID starting with S-1-5 and ending with 500 (according well-know SIDs). As the default domain administrator also starts with S-1-5 and ends with -500, the query includes a table containing the default domain administrator's SID of the domain to exclude these logons.

https://github.com/lorisAmbrozzo/KQL-Queries/blob/main/Defender%20For%20Endpoint/MDE-DefaultLocalAdmin-Logon.md

What did you do with KQL this month?

What about the Defender Rings?



Using Intune and direct access to the internet

Microsoft Update (MU) / Windows update (WU)

	4:00 a.m. local time (e.g., PST, UTC-8)	5:00 a.m. local time	6:00 a.m. local time	7:00 a.m. local time	8:00 a.m. local time
Cloud	Multiple daily security intelligence updates (SIUs)				
Production				Check **Passed**	Current Channel (Broad) the rest 10%-100% devices download SIUs from MU over the internet
UAT	Allow the detected apps on Microsoft Defender Antivirus, submit the false positive and download the updated SIUs.	Current Channel (Staged) up to 10% devices download SIUs from Internet (MU/MU)		**Pilot Group** Check **Failed**	

Thanks for attending

KQL|Cafe