

# Session 4 | Detections



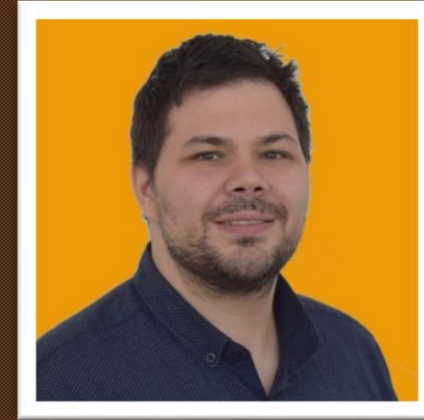
## Session 4 | Detections

# Your | hosts

## Alex Verboon



## Gianni Castaldi



<https://twitter.com/alexverboon>

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

<https://github.com/alexverboon>

<https://www.verboon.info/>

[https://twitter.com/castello\\_johnny](https://twitter.com/castello_johnny)

<https://www.linkedin.com/in/giannicastaldi/>

<https://github.com/KustoKing>

<https://www.kustoking.com/>

Show | Agenda

Welcome / Poll Results

What's new in KQL

Working with IOCs

Learning KQL

Our KQL Guest

What did you do with KQL this month?

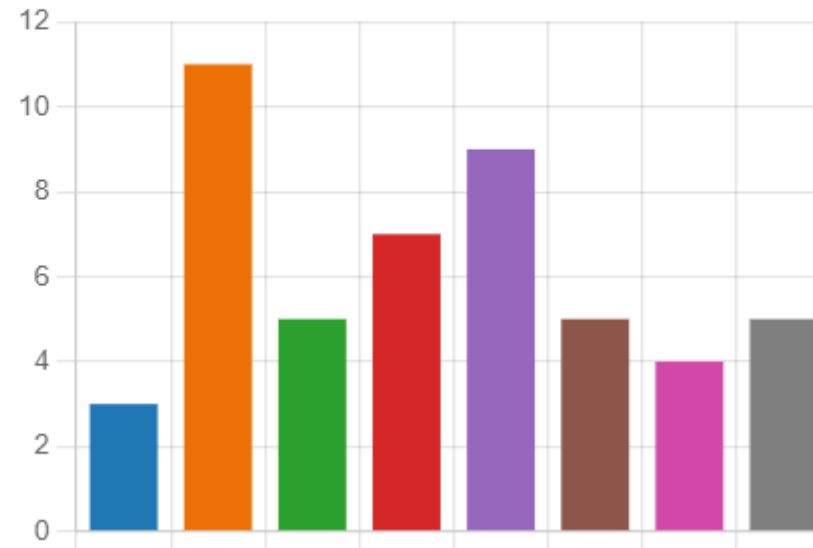
KQL Challenge of the month

# Poll Results

1. When we started we thought Tuesday would be a good day for the KQL Cafe. Which days would you like?

[More Details](#)

Monday	3
Tuesday	11
Wednesday	5
Thursday	7
Friday	9
Saturday	5
Sunday	4
I rather watch the recording	5



We will continue to host KQL Café on Tuesdays

# Poll Results

2. For the time we choose to start at 6:00 PM in western europe. (summer UTC+2, winter UTC+1) What would be a good time for you?

[More Details](#)

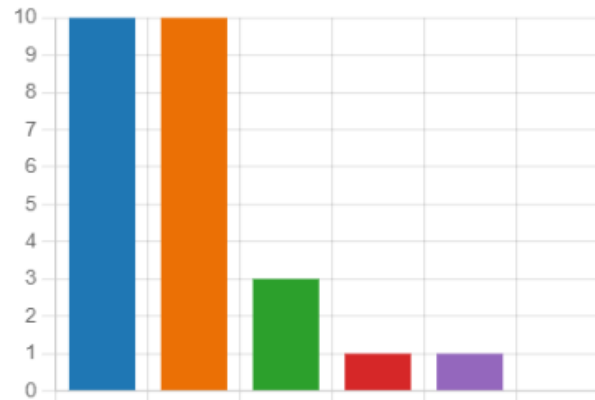
09:00 AM (PDT) 04:00 PM (UTC) ...	9
10:00 AM (PDT) 05:00 PM (UTC) ...	4
11:00 AM (PDT) 06:00 PM(UTC) ...	7
I rather watch the recording	8
Other	2



3. After choosing the date and the time the next question is the duration. We try to aim for two hours of content, and the current average is 1 hour and 49 minutes. What do you think is a good duration?

[More Details](#)

45~60 minutes	10
60~75 minutes	10
75~90 minutes	3
90~105 minutes	1
105~120 minutes	1
Other	0



We understand 2 hours can be quite lengthy, hence we decided to shorten the show to approx. 1 hr. 15 minutes

# Poll Results

Thanks for all your inputs, you gave us enough ideas for the upcoming shows

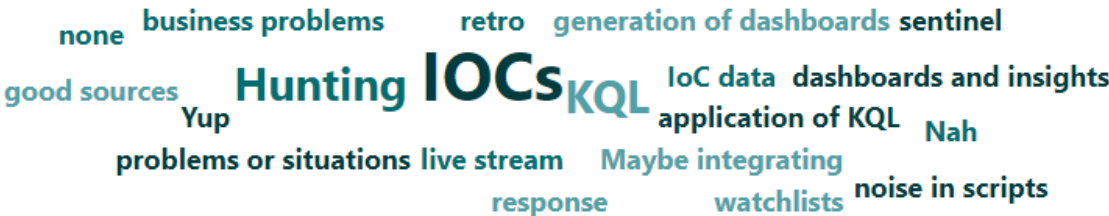
5 respondents (31%) answered **KQL** for this question.



2 respondents (18%) answered **ie** for this question.



3 respondents (25%) answered **IOCs** for this question.



# Microsoft 365 Defender Connector in Microsoft Sentinel

Microsoft Sentinel > Microsoft Sentinel >

Microsoft 365 Defender (Preview) ...

Microsoft 365 Defender (Preview)

Connected Status

Microsoft Provider

5 minutes ago Last Log Received

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence

Last data received

18.04.22, 21:30

Related content

1 Workbooks

4 Queries

39 Analytics rules templates

Data received

25M

Go to log analytics

Incidents

Instructions

Next steps

Connect events

Connect logs from the following Microsoft 365 Defender products to

Microsoft Defender for Endpoint (10/10 connected) ⓘ

Microsoft Defender for Office 365 (4/4 connected)

Microsoft Defender for Cloud Apps (1/1 connected)

Microsoft Defender for Identity (3/3 connected)

Microsoft Defender Alert Evidence (1/1 connected)

Microsoft Defender for Cloud Apps (1/1 connected)

✓ Name

CloudAppEvents

Microsoft Defender for Identity (3/3 connected)

✓ Name

IdentityLogonEvents

IdentityQueryEvents

IdentityDirectoryEvents

Microsoft Defender Alert Evidence (1/1 connected)

✓ Name

AlertEvidence

What's new in KQL

Session 4 | Detections



# Microsoft 365 Defender Connector in Microsoft Sentinel

## Workspace Usage Report - lg-azuresentinel

lg-azuresentinel

Edit Open Save Refresh Share Help Auto refresh: Off

Subscription: Microsoft Azure Enterprise Workspace: LG-AzureSentinel TimeRange: Last 7 days Select the detail level: Basic Advanced Show Help: Yes No Change Log

Workspace Info Latency Cost Analysis Microsoft Sentinel Regular Checks (D/W/M) Azure Data Explorer (ADX)

Log Analytics Workspace Name	Resource Group	location	Data Retention(days)	Last known SKU update
LG-AzureSentinel	rg_azure_sentinel	westeurope	90	✓ Fri, 15 Nov 2019 12:50:27 GMT

Group: Workspace info

LG-AzureSentinel Status for Last 7 days, Billable Tables have an average use of: 29.48 GB per day, Billable Tables have a Total size of 197.06 GB

identity

Table Name	IsBillable	Table Size
IdentityQueryEvents	True	7.03GB
IdentityLogonEvents	True	2.252GB
IdentityDirectoryEvents	True	48.844MB

# Microsoft 365 Defender Connector in Microsoft Sentinel

► Run Time range : Last 7 days Save

```
1 IdentityQueryEvents
2 | summarize count() by ActionType
```

Results Chart Add bookmark

<input type="checkbox"/> ActionType	count_
<input type="checkbox"/> > SAMR query	6'766'907
<input type="checkbox"/> > DNS query	1'095'476
<input type="checkbox"/> > LDAP query	197'359

► Run Time range : Last 7 days Save

```
1 IdentityQueryEvents
2 | //| summarize count() by ActionType
3 | where ActionType contains "SAMR"
4 | extend ACTOR_DEVICE_ = tostring(AdditionalFi
5 | summarize count() by ACTOR_DEVICE_
```

Results Chart Add bookmark

<input type="checkbox"/> ACTOR_DEVICE_	count_ ↑↓
<input type="checkbox"/> >	1'892'734
<input type="checkbox"/> >	1'790'228
<input type="checkbox"/> >	1'153'254
<input type="checkbox"/> >	317'329
<input type="checkbox"/> >	288'853

```
1 IdentityLogonEvents
2 | distinct ActionType
3
4 IdentityDirectoryEvents
5 | distinct ActionType
```

# Extend Columns in Microsoft Sentinel Log Analytics

Run

Time range : Last 7 days

Save

Share

New alert rule

Export

Pin to

```
1 IdentityQueryEvents
2 //| summarize count() by ActionType
3 | where ActionType contains "SAMR"
4 | extend ACTOR_DEVICE_ = tostring(AdditionalFields["ACTOR.DEVICE"])
5
6
7
8
9
10
11
```

Results

Chart

Add bookmark

Showing the first 30'000 results. [Learn more](#) on how to narrow down the result set.

TimeGenerated [UTC]

ACTOR\_DEVICE\_

ActionType

Application

TargetAccountDisplayName

Wagner Quentin

ReportId

AdditionalFields

{ "TO.DEVICE": "MBOVDCPR783", "ACTOR.DE..."

ACTOR\_DEVICE

Count

1

DeviceName

DeviceId

DeviceType

windows server 2016 standard

DestinationComputerOperatingSystemVersion

10.0 (14393)

Copy

Include "M..."

Exclude "I..."

Extend column

# Black/Cat ALPHV ransomware

## [FBI Releases IOCs Associated with BlackCat/ALPHV Ransomware | CISA](#)

**TLP: WHITE**

Batch Scripts	
Filename	MD5 Hash
CheckVuln.bat	f5ef5142f044b94ac5010fd883c09aa7
Create-share-RunAsAdmin.bat	84e3b5fe3863d25bb72e25b10760e861
LPE-Exploit-RunAsUser.bat	9f2309285e8a8471fce7330fcade8619
RCE-Exploit-RunAsUser.bat	6c6c46bdac6713c94debbd454d34efd9
est.bat	e7ee8ea6fb7530d1d904cdb2d9745899
runav.bat	815bb1b0c5f0f35f064c55a1b640fca5

# Learning MV-EXPAND

- Summarize
- Lists
- Series

# KQL Tools | Generate a KQL query that includes PowerShell cmdlets from a specific Module

The screenshot shows the Windows PowerShell ISE interface with a script named 'Untitled1.ps1' containing a function 'New-KQPSModuleFunctions'. The function has parameters for 'Synopsis', 'New-KQPSModulecmdlets', and 'DESCRIPTION'. Below the script, a table displays the command type and name for the 'Get-MpPreference' cmdlet.

CommandType	Name
Function	Get-MpPreference

Overlaid on the ISE is a Notepad window titled 'ps\_ConfigDefender.kql'. It contains a KQL query that searches for PowerShell commands in the 'ConfigDefender' module. The query uses the 'dynamic' operator to list various cmdlets and filters for 'PowerShellCommand' and 'AdditionalFields'.

```
// Search for PowerShell commands included in the PowerShell module: ConfigDefender Version:1.0)
let pscommands = dynamic ([ "Add-MpPreference", "Get-MpComputerStatus", "Get-MpPreference", "Get-MpThreat", "Get-
MpThreatCatalog", "Get-MpThreatDetection", "Remove-MpPreference", "Remove-MpThreat", "Set-MpPreference", "Start-
MpRollback", "Start-MpScan", "Start-MpWDOScan", "Update-MpSignature" ]);
DeviceEvents
| where ActionType contains "PowerShellCommand"
| where AdditionalFields has_any (pscommands)
```

Below the Notepad window, the PowerShell ISE console shows the execution of the 'New-KQPSModuleFunctions' command. It lists the paths for various module files (e.g., 'MSFT\_MpComputerStatus.cdxml') and saves the generated KQL query to 'c:\temp\kql\_ConfigDefender.kql'.

```
PS C:\Users\AlexVerboon> New-KQPSModuleFunctions -ModuleName ConfigDefender -Path c:\temp -Verbose
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpComputerStatus.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpPreference.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreat.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatCatalog.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpThreatDetection.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpScan.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpSignature.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpWDOScan.cdxml'.
VERBOSE: Loading module from path 'C:\WINDOWS\system32\windowsPowerShell\v1.0\Modules\ConfigDefender\MSFT_MpRollback.cdxml'.
Saving KQL query to c:\temp\kql_ConfigDefender.kql
PS C:\Users\AlexVerboon>
```

<https://gist.github.com/alexverboon/9ccf8af7569103397da2b8ba4079529d>

# Today's | Guest

## Olaf Hartong



GitHub: <https://github.com/olafhartong>

Blog: <https://olafhartong.nl>

Company: <https://falconforce.nl>

# This Month – Microsoft Defender for Endpoint – Software Vulnerabilities

Inventories

Applications  
926

Export

Filters: Product Code (CPE): Available

Name	OS platform	Vendor	Weaknesses ↓	Threats	Exposed devices	Impact
Windows 10	Windows	Microsoft	1.91k			
Windows Server 2016	Windows	Microsoft	1.59k			
Acrobat Reader Dc	Windows	Adobe	1.47k			
Windows Server 2012 R2	Windows	Microsoft	1.18k			
Firefox	Windows	Mozilla	1.06k			
Windows Server 2019	Windows	Microsoft	1.02k			
Windows 7	Windows	Microsoft	971			
Flash Player	Windows	Adobe	965			
Windows Server 2008 R2	Windows	Microsoft	836			
Jre	Windows	Oracle	699			
Jdk	Windows	Oracle	682			

Run query

Save

Share link

Query

```
1 // Software Vulnerability Overview
2 DeviceTvmSoftwareVulnerabilities
3 | summarize make_list(VulnerabilitySeverityLevel), make_set(DeviceId), make_set(CveId), make_set(SoftwareVersion)
4   , Critical = make_set_if(CveId, VulnerabilitySeverityLevel == 'Critical'),
5   High = make_set_if(CveId, VulnerabilitySeverityLevel == 'High'),
6   Medium = make_set_if(CveId, VulnerabilitySeverityLevel == 'Medium'),
7   Low = make_set_if(CveId, VulnerabilitySeverityLevel == 'Low')
8   by SoftwareName, SoftwareVendor
9 | extend ExposedDevices = array_length(set_DeviceId)
10 | extend TotalVulnerabilities = array_length(set_CveId)
11 | extend VersionDistribution = array_length(set_SoftwareVersion)
12 | extend Critical = array_length(Critical)
13 | extend High = array_length(High)
14 | extend Medium = array_length(Medium)
15 | extend Low = array_length(Low)
16 | project SoftwareVendor, SoftwareName, ExposedDevices, TotalVulnerabilities, Critical, High, Medium, Low
17
```

Getting Started

Results

Export

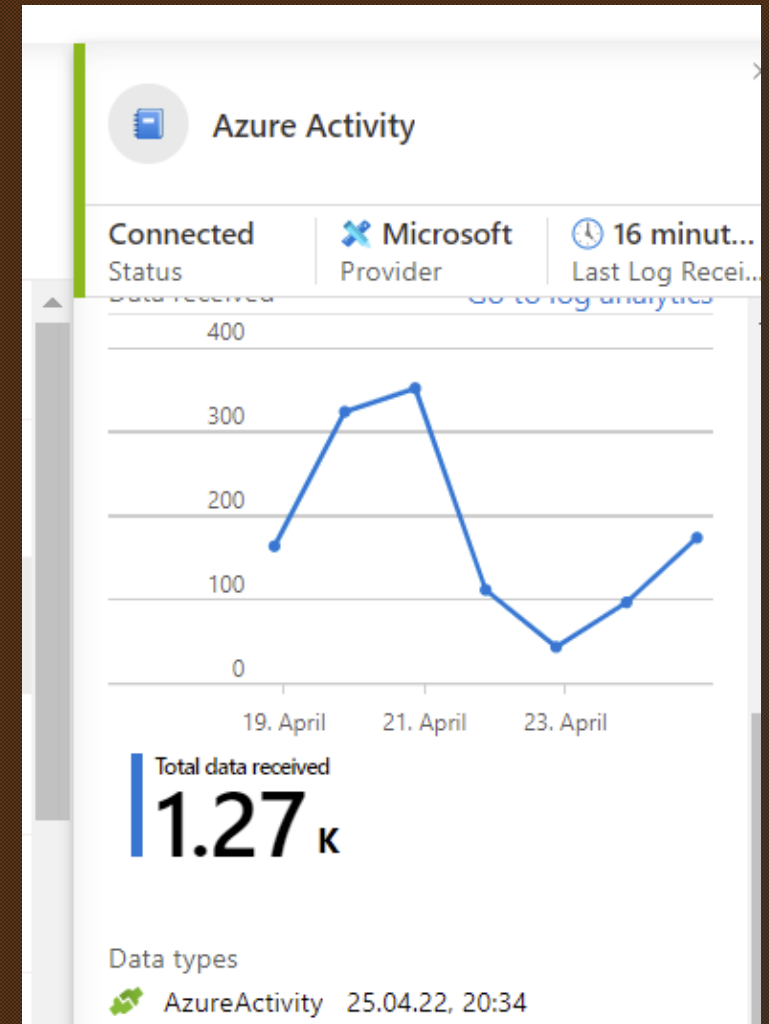
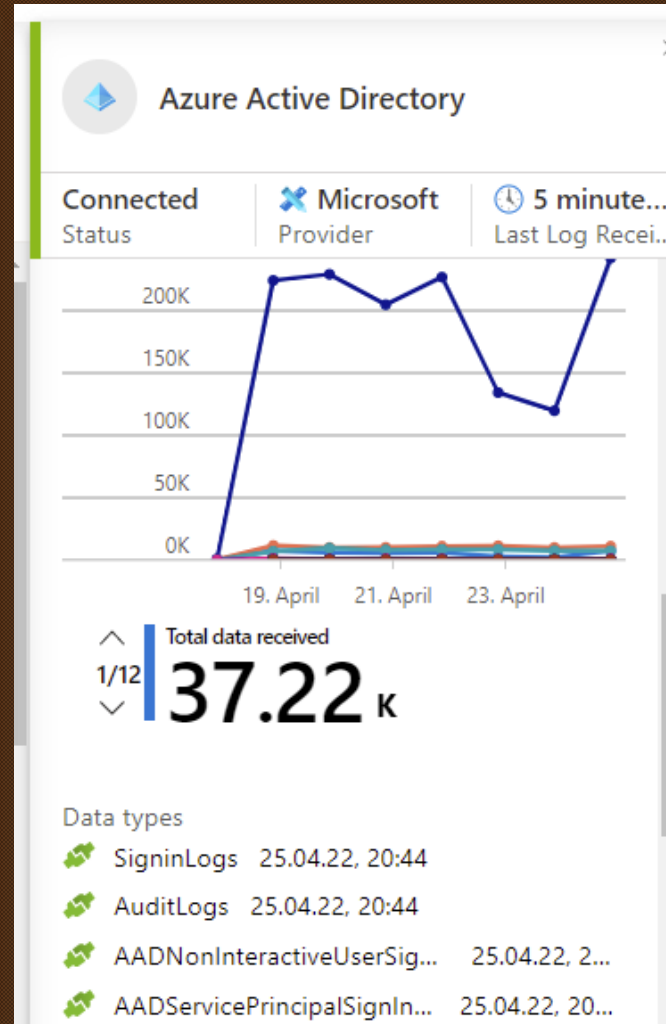
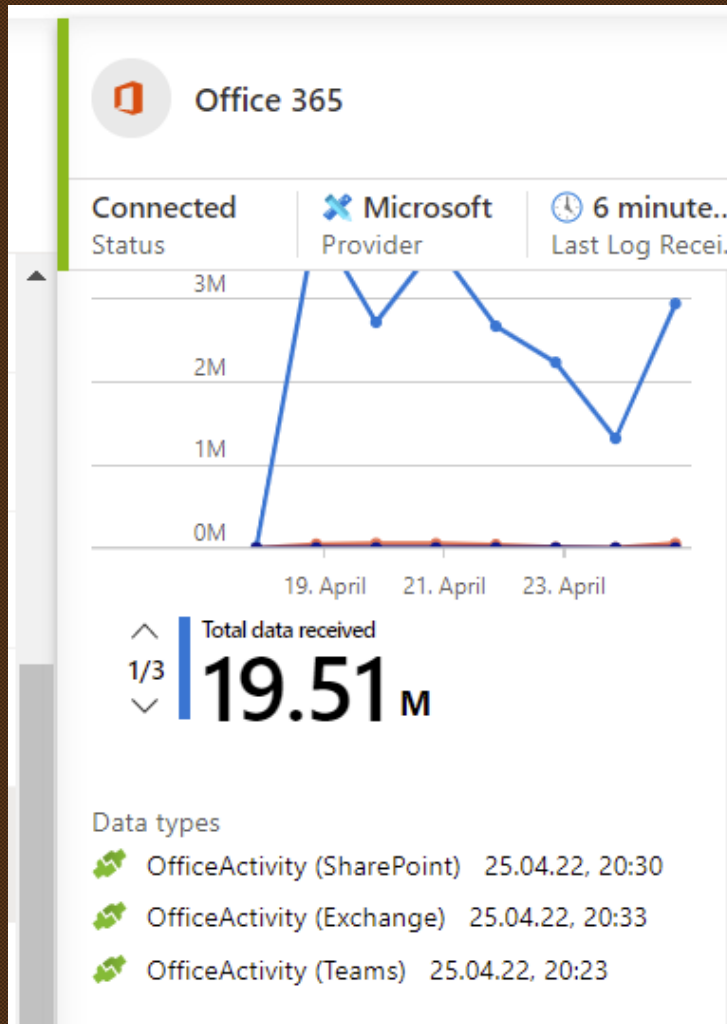
SoftwareVendor	SoftwareName	ExposedDevices	TotalVulnerabilities ↓	Critical	High	Medium	Low
microsoft	windows_10	1281	1911	26	1344	524	17
microsoft	windows_server_2016	13	1592	22	1103	454	13
adobe	acrobat_reader_dc	69	1465	2	1005	443	15
microsoft	windows_server_2012_r2	29	1179	20	811	342	6
mozilla	firefox	17	1059	5	511	538	5



# This Month – Microsoft Defender for Endpoint – Software Vulnerabilities

```
// Software Vulnerability Overview
DeviceTvmSoftwareVulnerabilities
| summarize make_list(VulnerabilitySeverityLevel), make_set(DeviceId), make_set(CvId),
make_set(SoftwareVersion)
, Critical = make_set_if(CvId, VulnerabilitySeverityLevel == 'Critical'),
High = make_set_if(CvId, VulnerabilitySeverityLevel == 'High'),
Medium = make_set_if(CvId, VulnerabilitySeverityLevel == 'Medium'),
Low = make_set_if(CvId, VulnerabilitySeverityLevel == 'Low')
by SoftwareName, SoftwareVendor
| extend ExposedDevices = array_length(set_DeviceId)
| extend TotalVulnerabilities = array_length(set_CvId)
| extend VersionDistribution = array_length(set_SoftwareVersion)
| extend Critical = array_length(Critical)
| extend High = array_length(High)
| extend Medium = array_length(Medium)
| extend Low = array_length(Low)
| project SoftwareVendor, SoftwareName, ExposedDevices, TotalVulnerabilities, Critical, High, Medium, Low
```

# This Month – Microsoft Sentinel – Connector Health



# This Month – Microsoft Sentinel – Connector Health

```
New Query 1*
EG-AzureSentinel
Run Time range: Last 3 days Save Share New alert rule Export Pin to Format query

1 let connectortable = datatable (Connector: string, LogTable: string) [
2   "Azure Active Directory", "SignInLogs",
3   "Azure Active Directory", "AuditLogs",
4   "Azure Active Directory", "ADManagedIdentitySignInLogs",
5   "Azure Active Directory", "ADServicePrincipalSignInLogs",
6   "Azure Active Directory", "ADNonInteractiveUserSignInLogs",
7   "Azure Active Directory", "ADProvisioningLogs",
8   "Sentinel", "ThreatIntelligenceIndicator",
9   "Office 365", "OfficeActivity",
10  "Azure", "AzureActivity",
11  "Microsoft Defender for Endpoint", "DeviceLogonEvents",
12  "Microsoft Defender for Endpoint", "DeviceProcessEvents",
13  "Microsoft Defender for Endpoint", "DeviceRegistryEvents",
14  "Microsoft Defender for Endpoint", "DeviceInfo",
15  "Microsoft Defender for Endpoint", "DeviceFileEvents",
16  "Microsoft Defender for Endpoint", "DeviceNetworkEvents",
17  "Microsoft Defender for Endpoint", "DeviceNetworkInfo",
18  "Microsoft Defender for Endpoint", "DeviceImageLoadEvents",
19  "Microsoft Defender for Endpoint", "DeviceEvents",
20  "Microsoft Defender for Endpoint", "DeviceFileCertificateInfo",
21  "Microsoft Defender for Cloud Apps", "CloudAppEvents",
22  "Microsoft Defender for Cloud Apps", "McanShadowReporting",
23  "Microsoft Defender for Office 365", "EmailEvents",
24  "Microsoft Defender for Office 365", "EmailAttachmentInfo",
25  "Microsoft Defender for Office 365", "EmailUrlInfo",
26  "Microsoft Defender for Office 365", "EmailPostDeliveryEvents",
27  "Microsoft Defender for Identity", "IdentityLogonEvents",
28  "Microsoft Defender for Identity", "IdentityQueryEvents",
29  "Microsoft Defender for Identity", "IdentityDirectoryEvents",
30  "Microsoft Defender for Identity", "Azure Advanced Threat Protection",
31  "Azure Firewall", "AZFWFWLIS",
32  "Azure Key Vault", "WULTS",
33  "Azure Web Application Firewall (WAF)", "APPLICATIONGATEWAYS"
34 ];
35
36 union
37 // Defender for Endpoint
38 DeviceEvents, DeviceFileEvents, DeviceProcessEvents, DeviceRegistryEvents, DeviceImageLoadEvents, DeviceNetworkEvents, DeviceNetworkInfo, DeviceLogonEvents, DeviceInfo, DeviceFileCertificateInfo,
39 // Azure AD
40 SignInLogs, AuditLogs, ADNonInteractiveUserSignInLogs, ADServicePrincipalSignInLogs, ADManagedIdentitySignInLogs,
41 // Azure
42 AzureActivity,
43 // Defender for Identity
44 IdentityDirectoryEvents, IdentityLogonEvents, IdentityQueryEvents,
45 // Microsoft Defender for Cloud Apps
46 CloudAppEvents, // McanShadowReporting
47 // Defender for Office 365
48 EmailEvents, EmailAttachmentInfo, EmailUrlInfo, EmailPostDeliveryEvents,
49 // Office 365
50 OfficeActivity,
51 // Sentinel
52 ThreatIntelligenceIndicator,
53 // Azure Firewall
54 AzureDiagnostics
55
56 summarize
57   Entries = count(),
58   last log minute = datetime diff('minute', now(), max(TimeGenerated)),
59   last log hours = datetime diff('hour', now(), max(TimeGenerated)),
60   last log days = datetime diff('day', now(), max(TimeGenerated)),
61   last logdate = max(TimeGenerated)
62 by Type, ResourceType
63
64 project ['TableName'] = Type,
65 ['Table Entries'] = Entries,
66 ['Last Record Minutes'] = last log minute,
67 ['Last Record Hours'] = last log hours,
68 ['Last Record Days'] = last log days,
69 last logdate, ResourceType
70 order by ['Last Record Minutes'] desc
71 join kind=leftouter connectortable
72 on SLeft['TableName'] == SRight.LogTable
73 join kind=leftouter connectortable
74 on SLeft.ResourceType == SRight.LogTable
75 extend Connector = strcat(Connector, Connector1)
76 where isnotempty(Connector)
77
78 project
79   last logdate,
80   Connector,
81   ['TableName'],
82   ['Table Entries'],
83   ['Last Record Minutes'],
84   ['Last Record Hours'],
85   ['Last Record Days'], //, ResourceType
86 where ['Last Record Days'] > 0
87 // where ['Last Record Hours'] > 4
```

# This Month – Microsoft Sentinel – Connector Health

<input type="checkbox"/> last_logdate [UTC]	Connector ↑↓	TableName	Table Entries	Last Record Minutes	Last Record Hours	Last Record Days
<input type="checkbox"/> > 25.4.2022, 18:34:59.965	Azure	AzureActivity	174	20	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:58.179	Azure Active Directory	AADNonInteractiveUse...	242'579	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:46:06.340	Azure Active Directory	AADServicePrincipalSig...	7'228	8	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:20.738	Azure Active Directory	SigninLogs	7'336	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:34.939	Azure Active Diretory	AuditLogs	10'958	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:02.000	Microsoft Defender for Cloud Apps	CloudAppEvents	1'849'503	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:12.548	Microsoft Defender for Endpoint	DeviceFileCertificateInfo	1'450'759	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:53:18.485	Microsoft Defender for Endpoint	DeviceEvents	4'701'218	1	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:57.838	Microsoft Defender for Endpoint	DeviceImageLoadEvents	1'462'322	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:53:03.361	Microsoft Defender for Endpoint	DeviceNetworkInfo	226'271	1	0	0
<input type="checkbox"/> > 25.4.2022, 18:52:27.443	Microsoft Defender for Endpoint	DeviceNetworkEvents	2'805'723	2	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:56.174	Microsoft Defender for Endpoint	DeviceFileEvents	2'949'054	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:53:03.361	Microsoft Defender for Endpoint	DeviceInfo	82'410	1	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:43.292	Microsoft Defender for Endpoint	DeviceRegistryEvents	5'848'468	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:54:07.133	Microsoft Defender for Endpoint	DeviceProcessEvents	1'770'371	0	0	0
<input type="checkbox"/> > 25.4.2022, 18:51:05.589	Microsoft Defender for Endpoint	DeviceLogonEvents	221'473	3	0	0
<input type="checkbox"/> > 25.4.2022, 18:53:40.822	Microsoft Defender for Identity	IdentityDirectoryEvents	6'007	1	0	0
<input type="checkbox"/> > 25.4.2022, 18:53:49.470	Microsoft Defender for Identity	IdentityQueryEvents	902'156	1	0	0
<input type="checkbox"/> > 25.4.2022, 18:53:48.738	Microsoft Defender for Identity	IdentityLogonEvents	214'467	1	0	0

# This Month – Microsoft Sentinel – Connector Health

**General** Set rule logic Incident settings Automated response Review and update

Create an analytics rule that will run on your data to detect threats.

### Analytics rule details

Name \*

Sentinel Connector Health

Id

c2336f69-4c0a-4693-be93-d9bc5f18d2da

Description

Sentinel Connector Health

Tactics and techniques

0 selected

Severity

Medium

Status

Enabled Disabled

**General** **Set rule logic** Incident settings Automated response Review and update

Define the logic for your new analytics rule.

### Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
let connectortable = datatable (Connector: string, LogTable: string) [  
    "Azure Active Directory", "SignInLogs",  
    "Azure Active Directory", "AuditLogs",  
    "Azure Active Directory", "AADManagedIdentitySignInLogs",  
    "Azure Active Directory", "AADServicePrincipalSignInLogs",  
    "Azure Active Directory", "AADNonInteractiveUserSignInLogs",  
    "Azure Active Directory", "AADServicePrincipalLogs"  
]
```

[View query results >](#)

### Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

ⓘ Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. [Learn more >](#)

Cloud application

Name Connector + Add identifier

# This Month – Microsoft Sentinel – Connector Health

## ^ Custom details

Here you can surface particular event parameters and their values in alerts that comprise those events, by adding key-value pairs below. In the Key field, enter a name of your choosing that will appear as the field name in alerts. In the Value field, choose the event parameter you wish to surface in the alerts from the drop-down list. [Learn more >](#)

+ Add new

## ∨ Alert details

### Query scheduling

Run query every \*

Lookup data from the last \* ⓘ

### Alert threshold

Generate alert when number of query results

\*

# This Month – Microsoft Sentinel – Connector Health

**Incident** ...  
Incident ID 17491

Refresh

**Sentinel Connector Health**  
Incident ID: 17491

Unassigned Owner | New Status | Medium Severity

Description  
Sentinel Connector Health

Alert product names  
• Microsoft Sentinel

Evidence  
1 Events | 1 Alerts | 0 Bookmarks

Last update time: 25.04.22, 20:33 | Creation time: 25.04.22, 20:33

Entities (1)  
Sentinel  
[View full details >](#)

Incident workbook  
[Incident Overview](#)

Analytics rule  
[Sentinel Connector Health](#)

Tags  
+

Incident link  
[https://portal.azure.com/#asset/Microsoft\\_Azure\\_Security\\_Insights/...](https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/...)

Last comment (Total: 0)  
Write a comment...

Connector  
Sentinel

Table  
ThreatIntelligenceIndicator

Entities (1)  
Sentinel  
[View full details >](#)

Connector  
Sentinel

Table  
ThreatIntelligenceIndicator

# Questions?



Thanks for attending

