Session 4 | Detections

Session 4 | Detections

Your | hosts

Alex Verboon

https://twitter.com/alexverboon

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

https://github.com/alexverboon

https://www.verboon.info/

Gianni Castaldi

https://twitter.com/castello_johnny

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

https://github.com/KustoKing

https://www.kustoking.com/

Show | Agenda

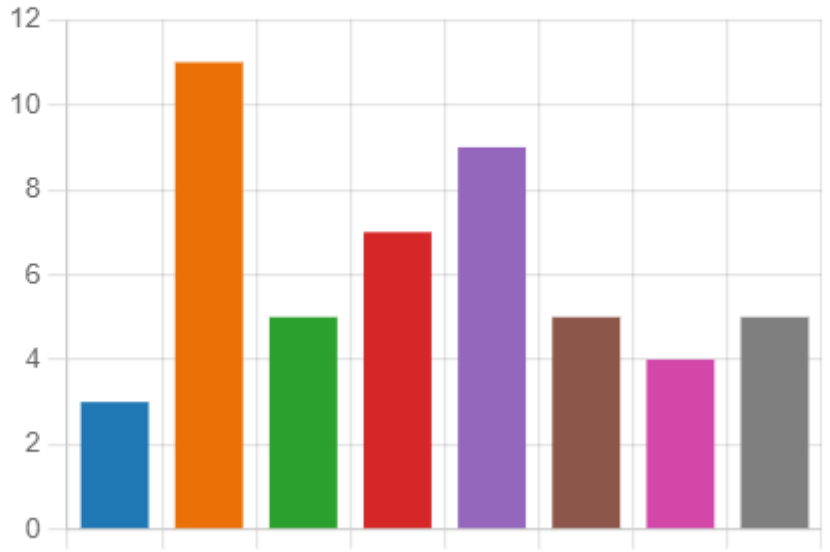
Welcome / Poll Results
What's new in KQL
Working with IOCs
Learning KQL
Our KQL Guest
What did you do with KQL this month?
KQL Challenge of the month

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?

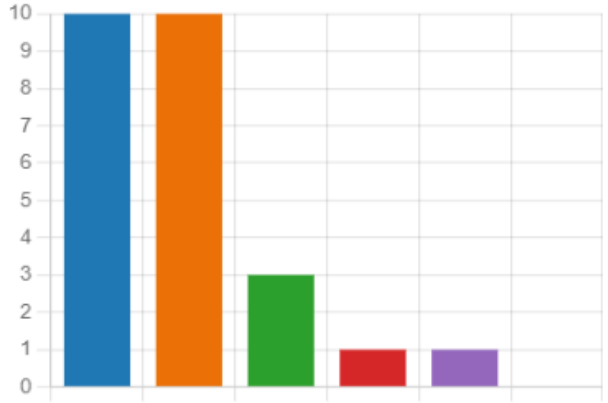
More Details

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?

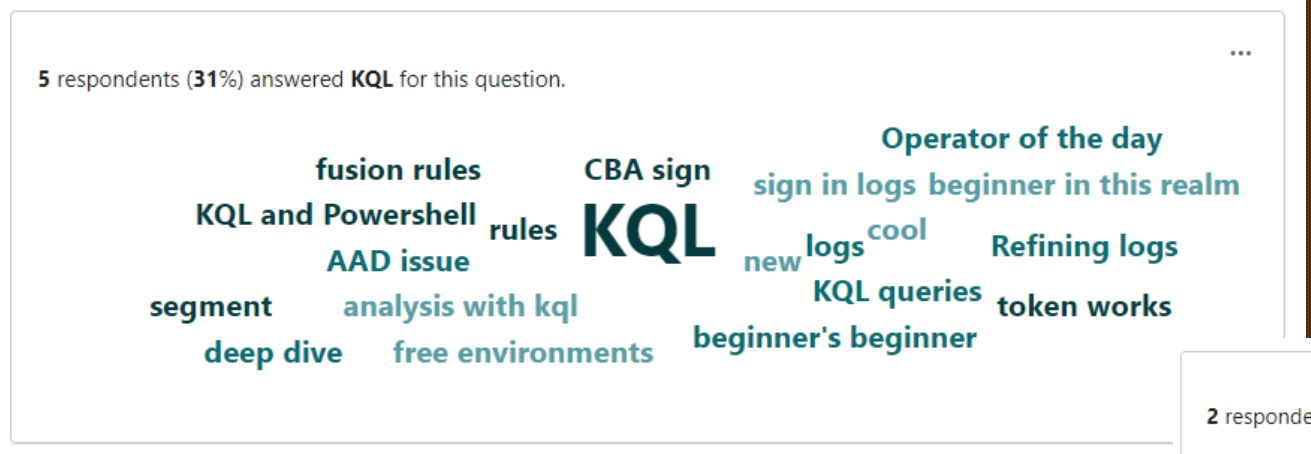
More Details

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

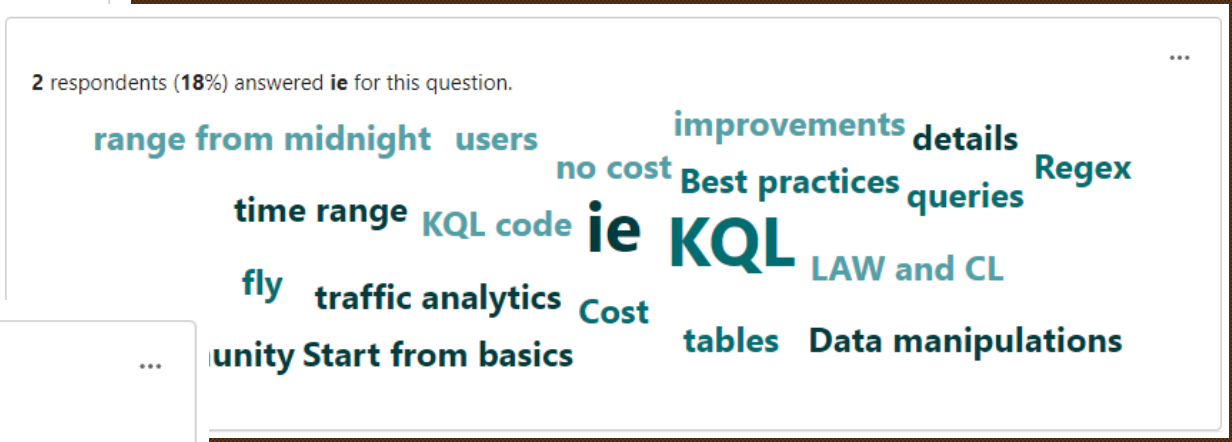


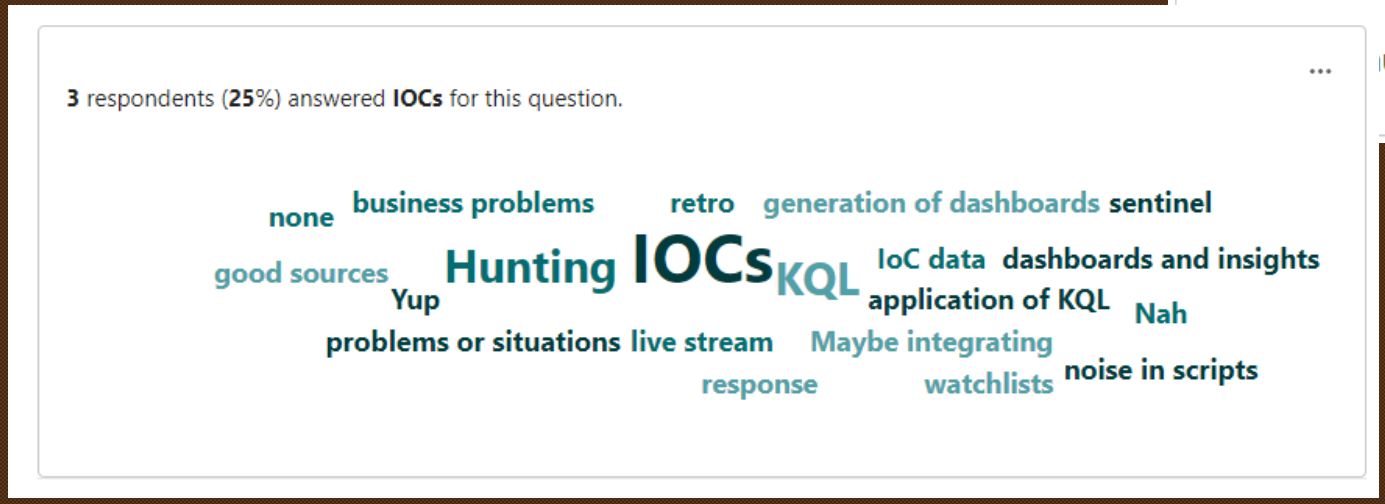
We understand 2 hours can be quite lengthy, hence we decided to shorten the show to approx. 1 hr. 15 minutes

Poll Results

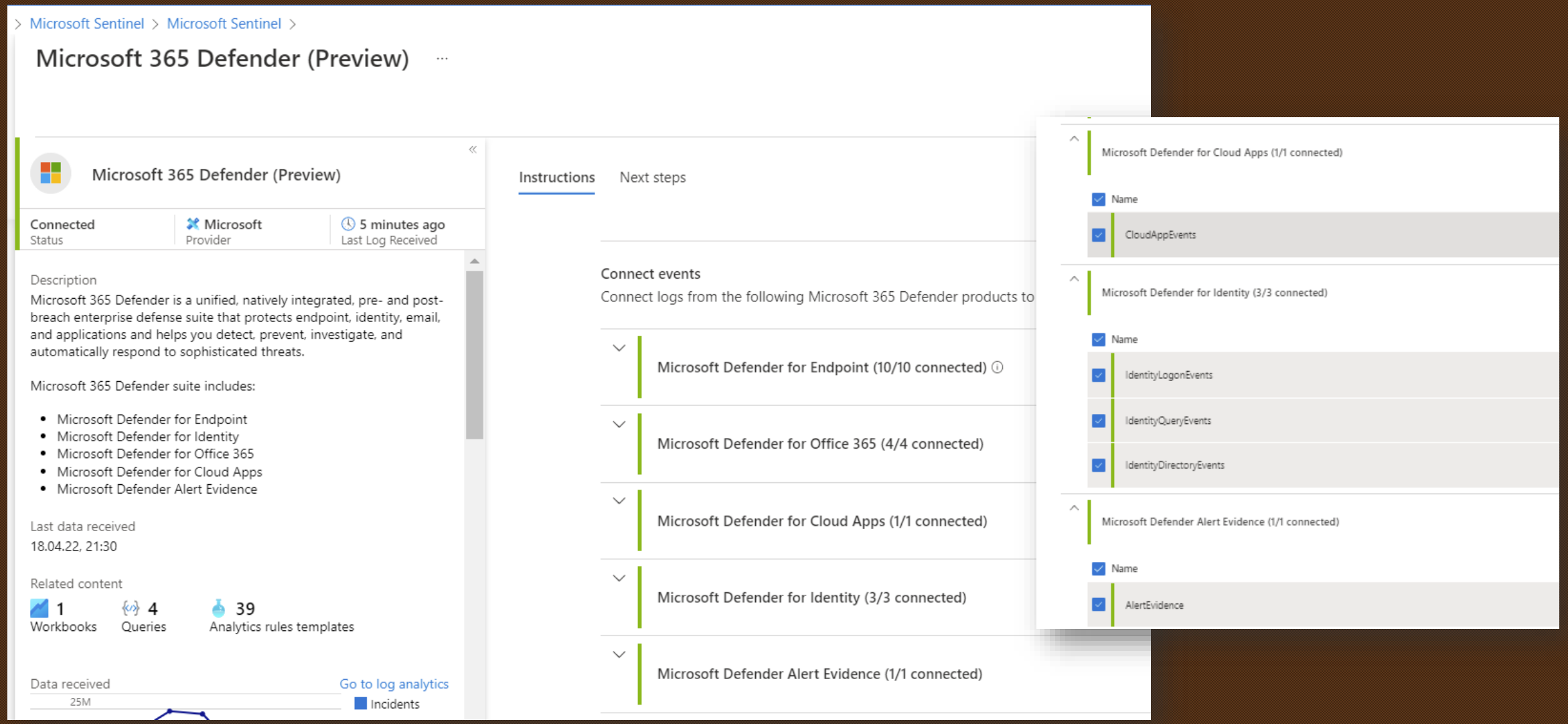


Thanks for all your inputs, you gave us enough ideas for the upcoming shows

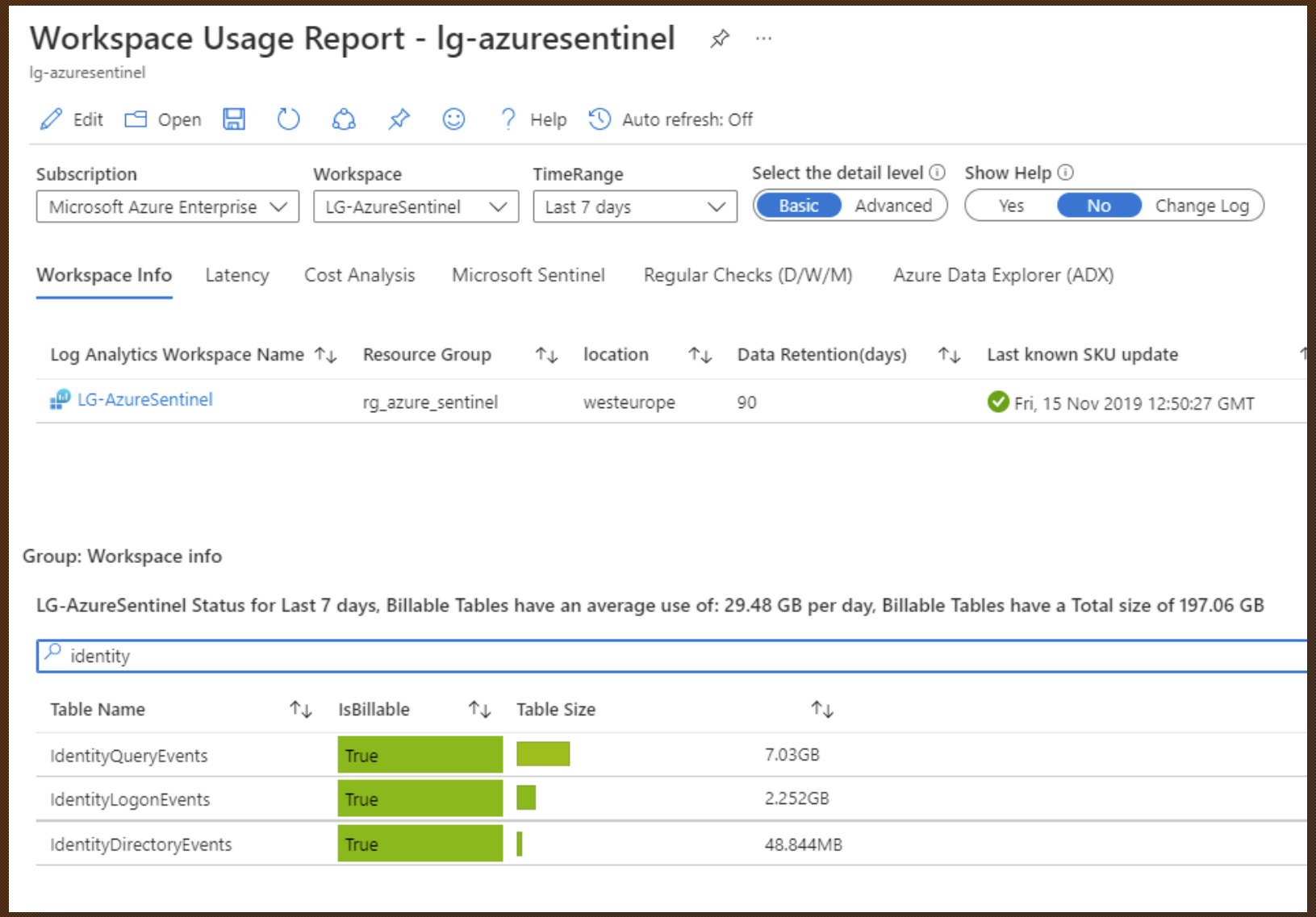




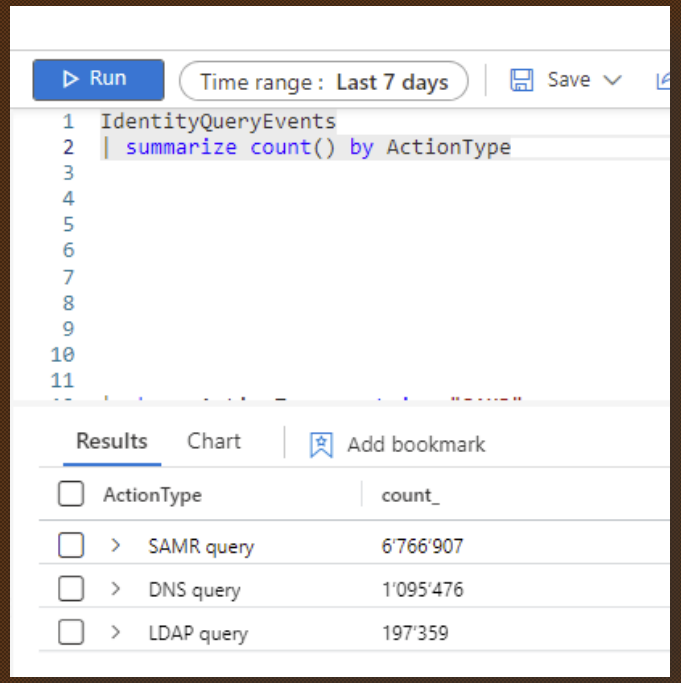
Microsoft 365 Defender Connector in Microsoft Sentinel

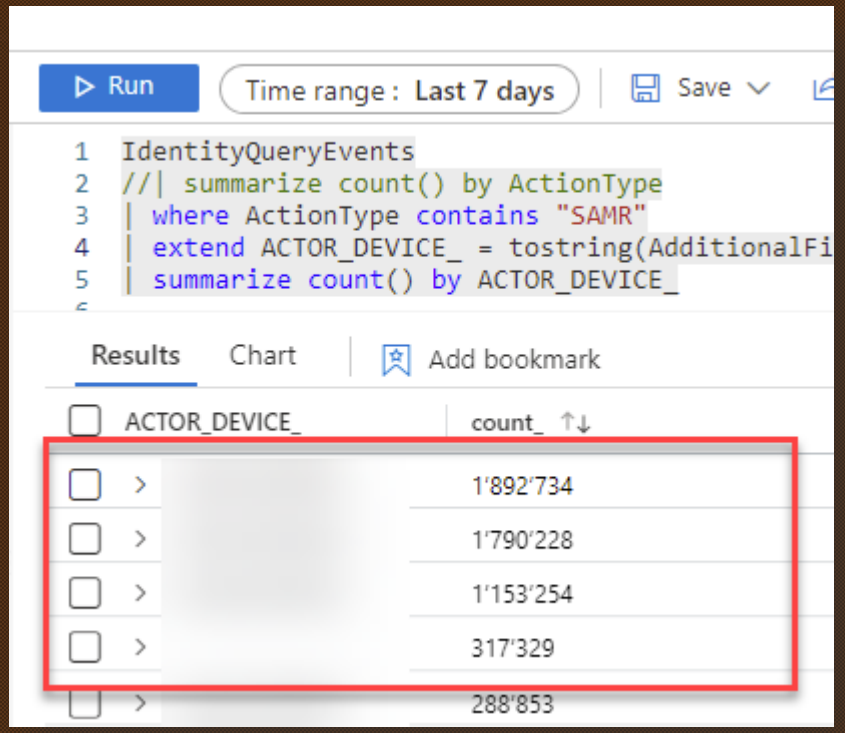


Microsoft 365 Defender Connector in Microsoft Sentinel



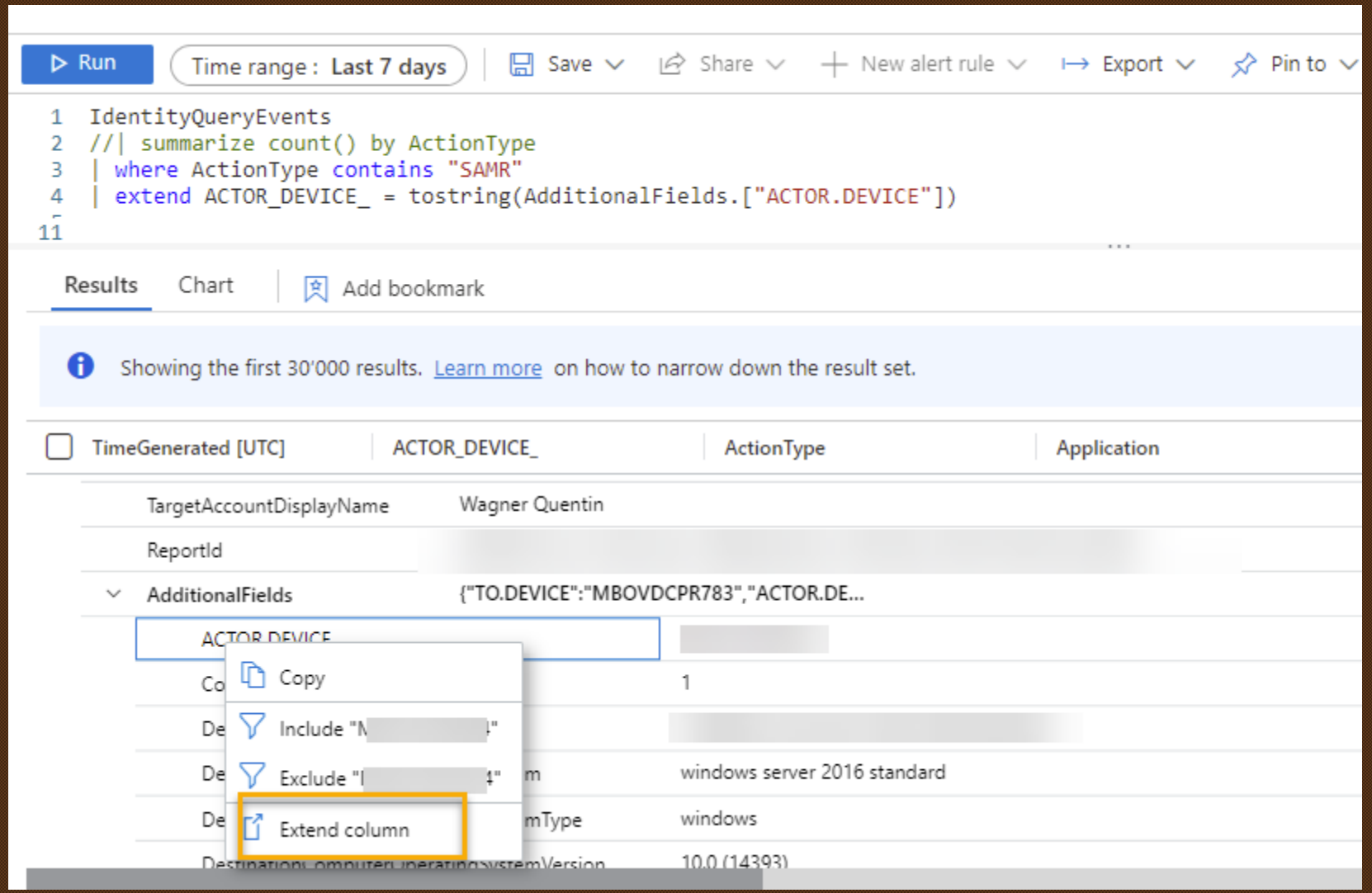
Microsoft 365 Defender Connector in Microsoft Sentinel






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

Extend Columns in Microsoft Sentinel Log Analytics



Black/Cat ALPHV ransomware

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

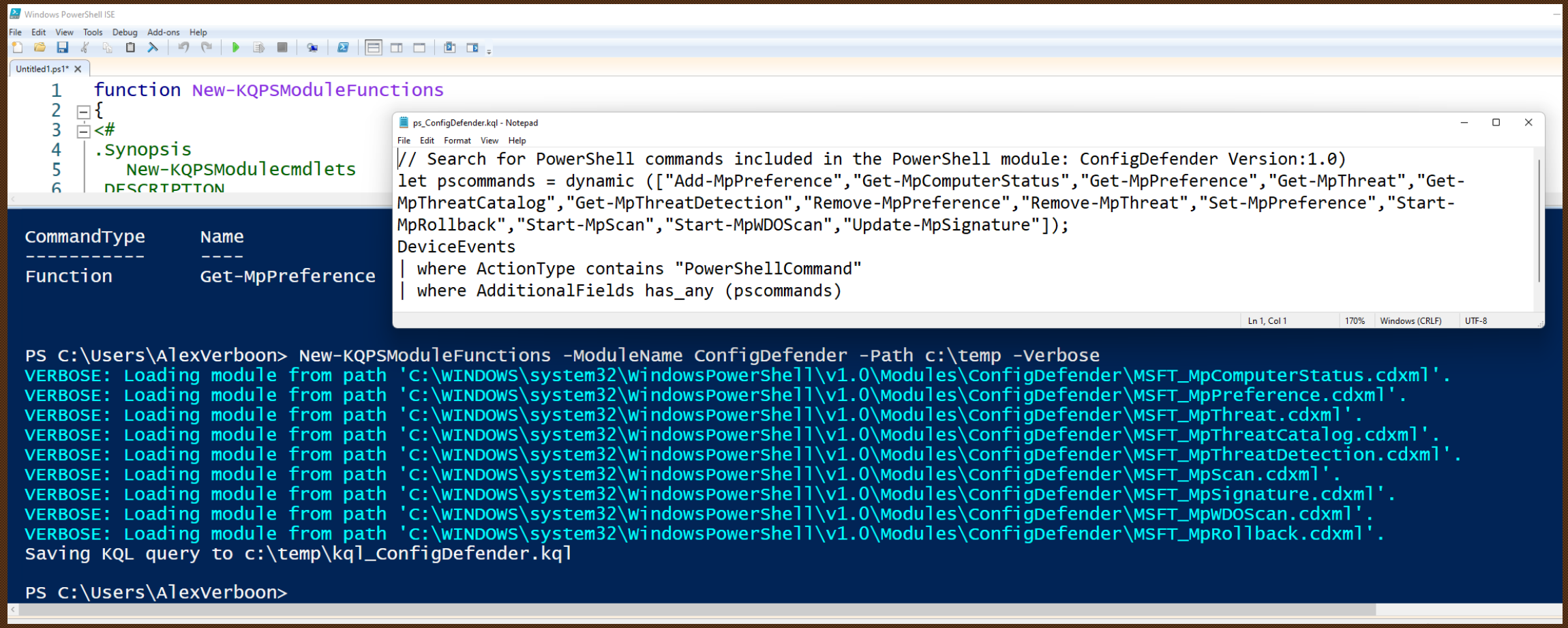
TLP: WHITE

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

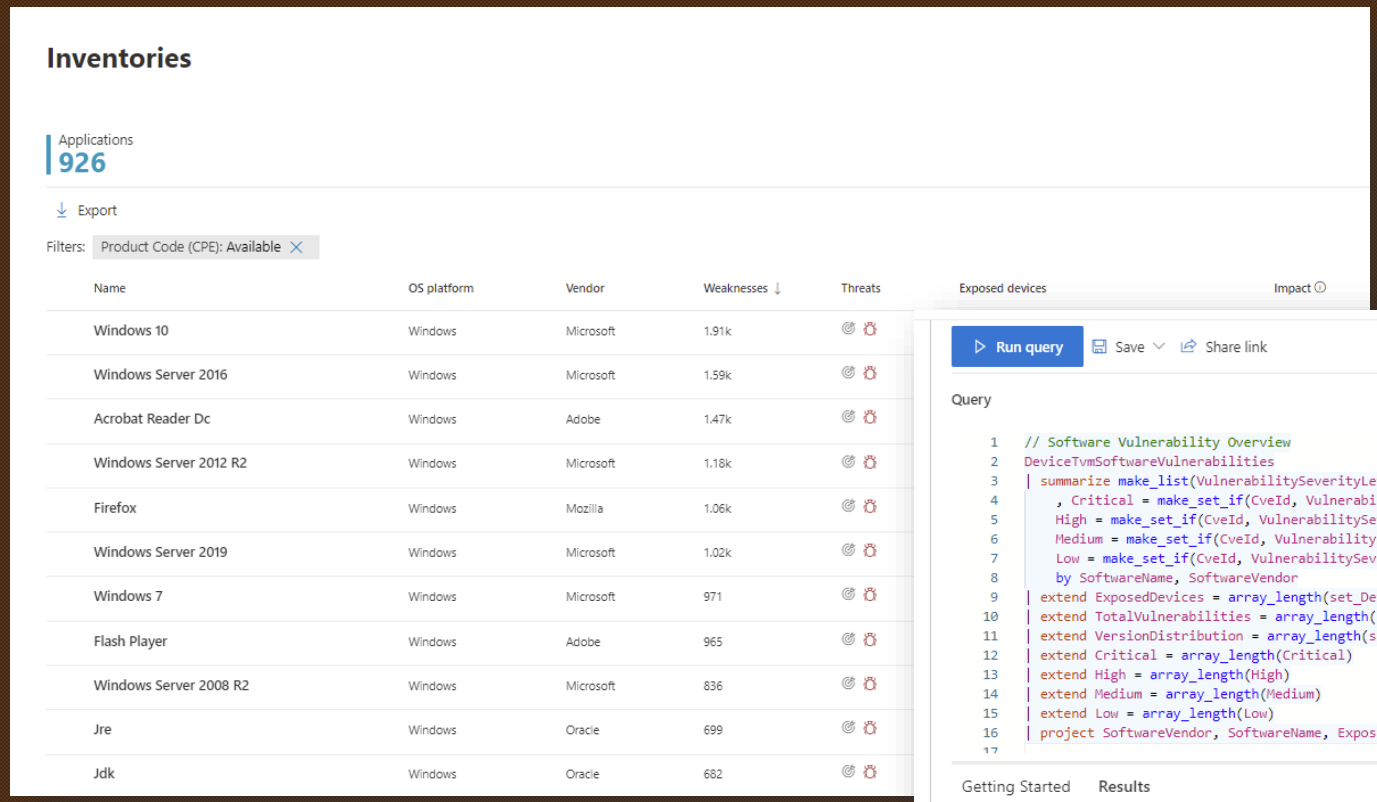


https://gist.github.com/alexverboon/9ccf8af7569103397da2b8ba4079529d

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



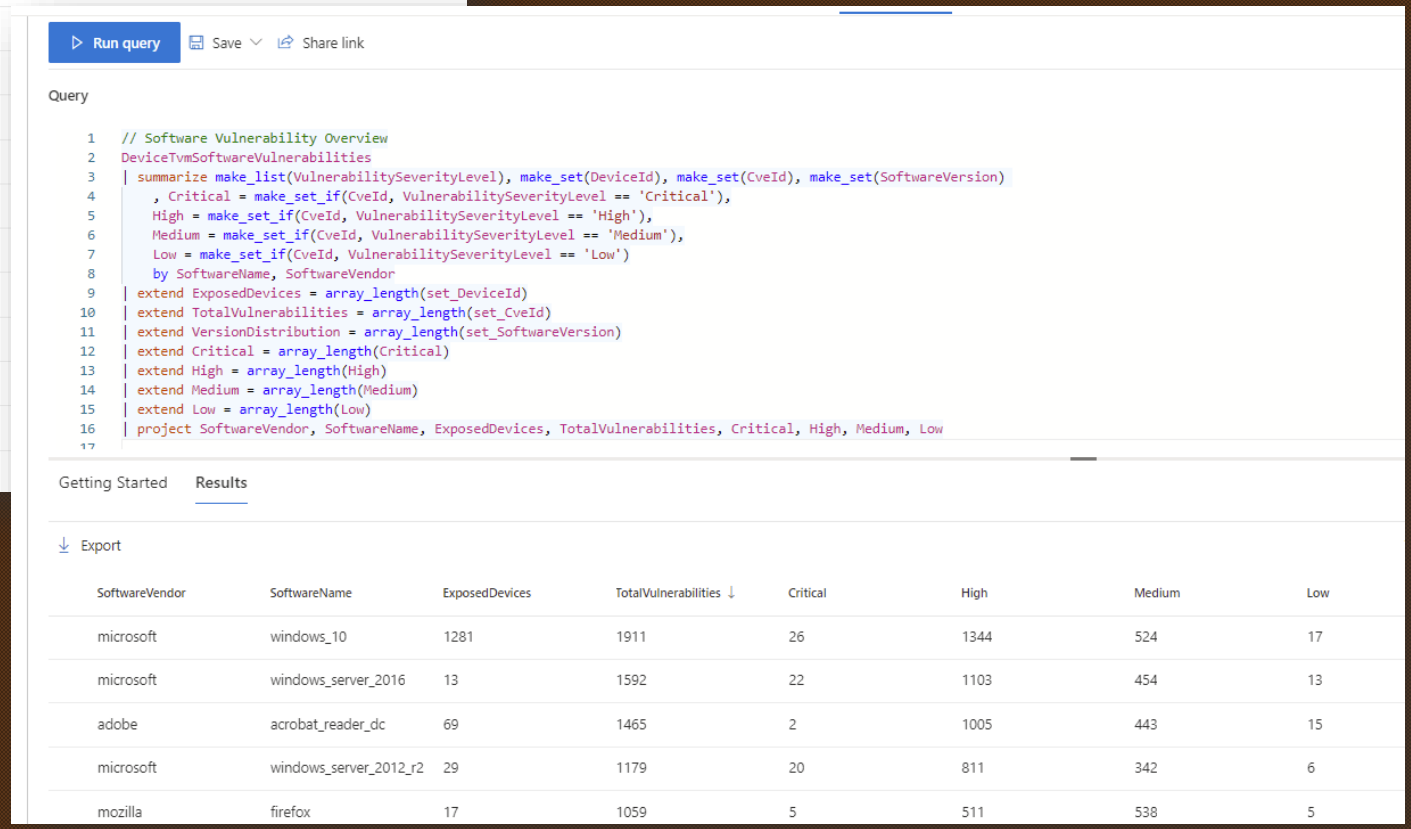
Inventories

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

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

Getting Started | Results

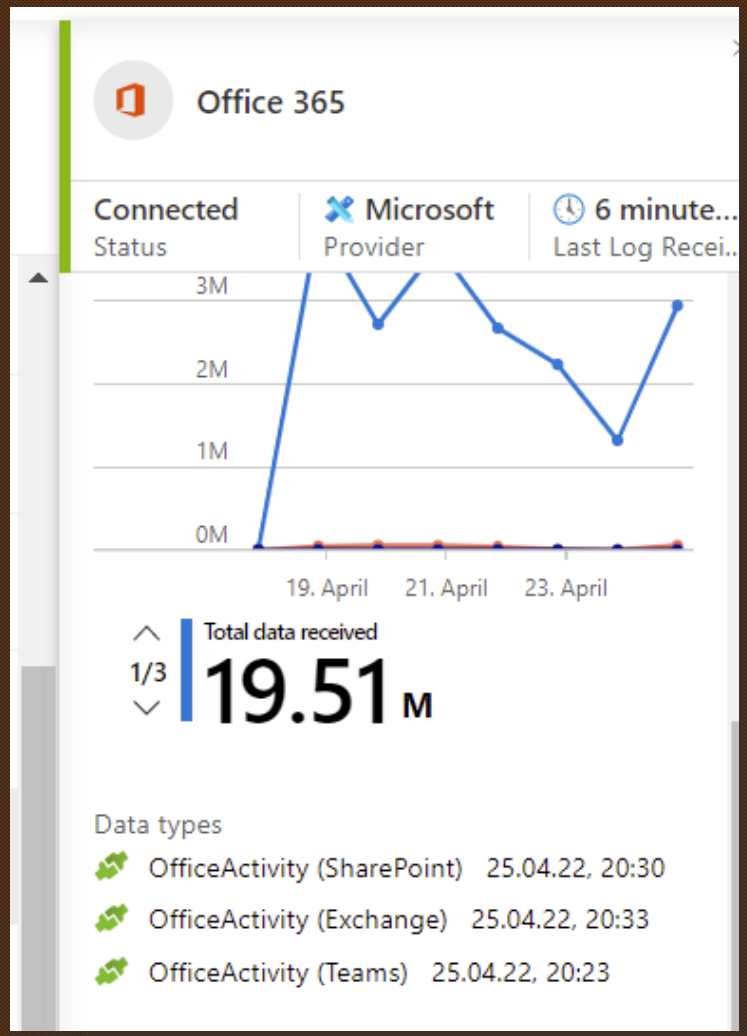
Export

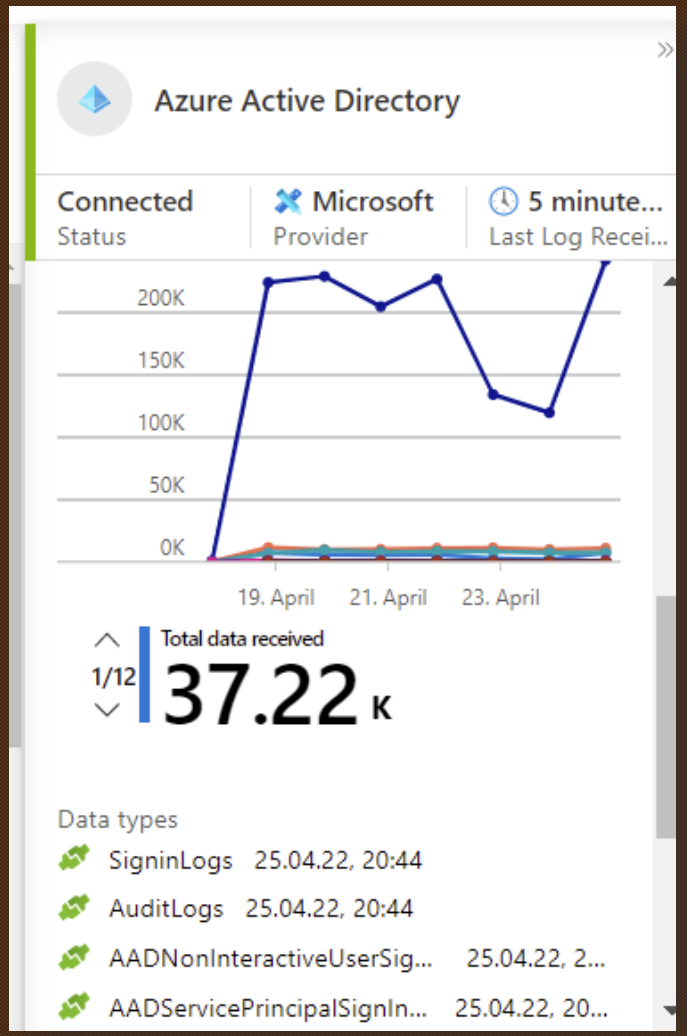
SoftwareVendor	SoftwareName	ExposedDevices	TotalVulnerabilities	Critical	High	Medium	Low
microsoft	windows_10	1281	1911	26	1344	524	17
microsoft	windows_server_2016	13	1592	22	1103	454	13
adobe	acrobat_reader_dc	69	1465	2	1005	443	15
microsoft	windows_server_2012_r2	29	1179	20	811	342	6
mozilla	firefox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

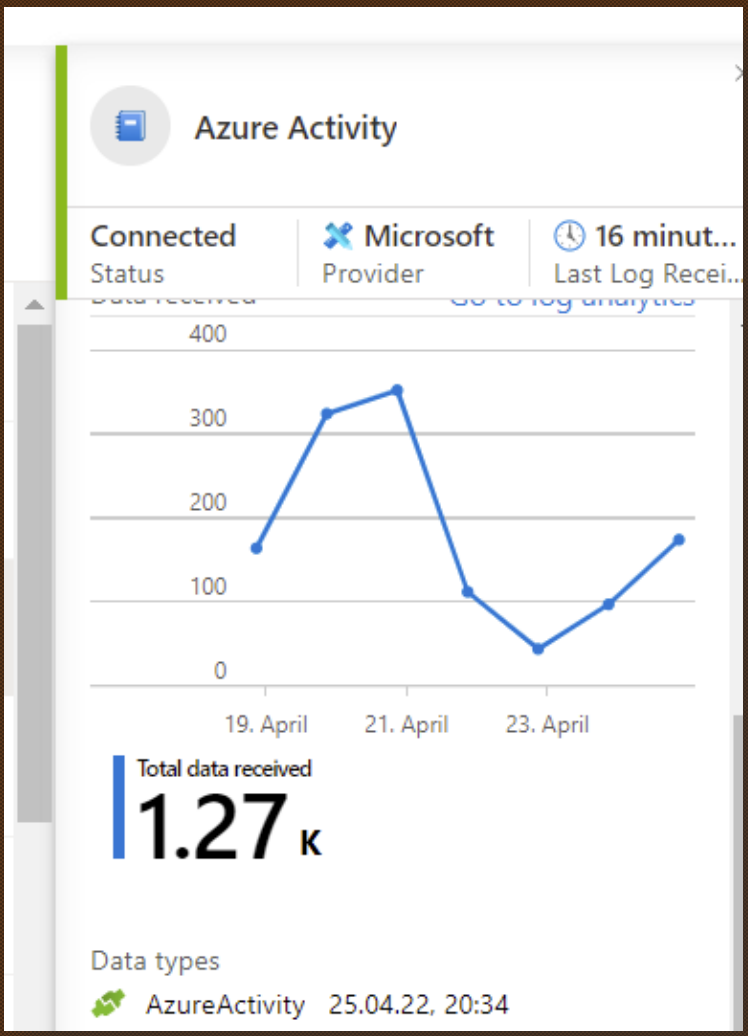
This Month – Microsoft Defender for Endpoint – Software Vulnerabilities

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

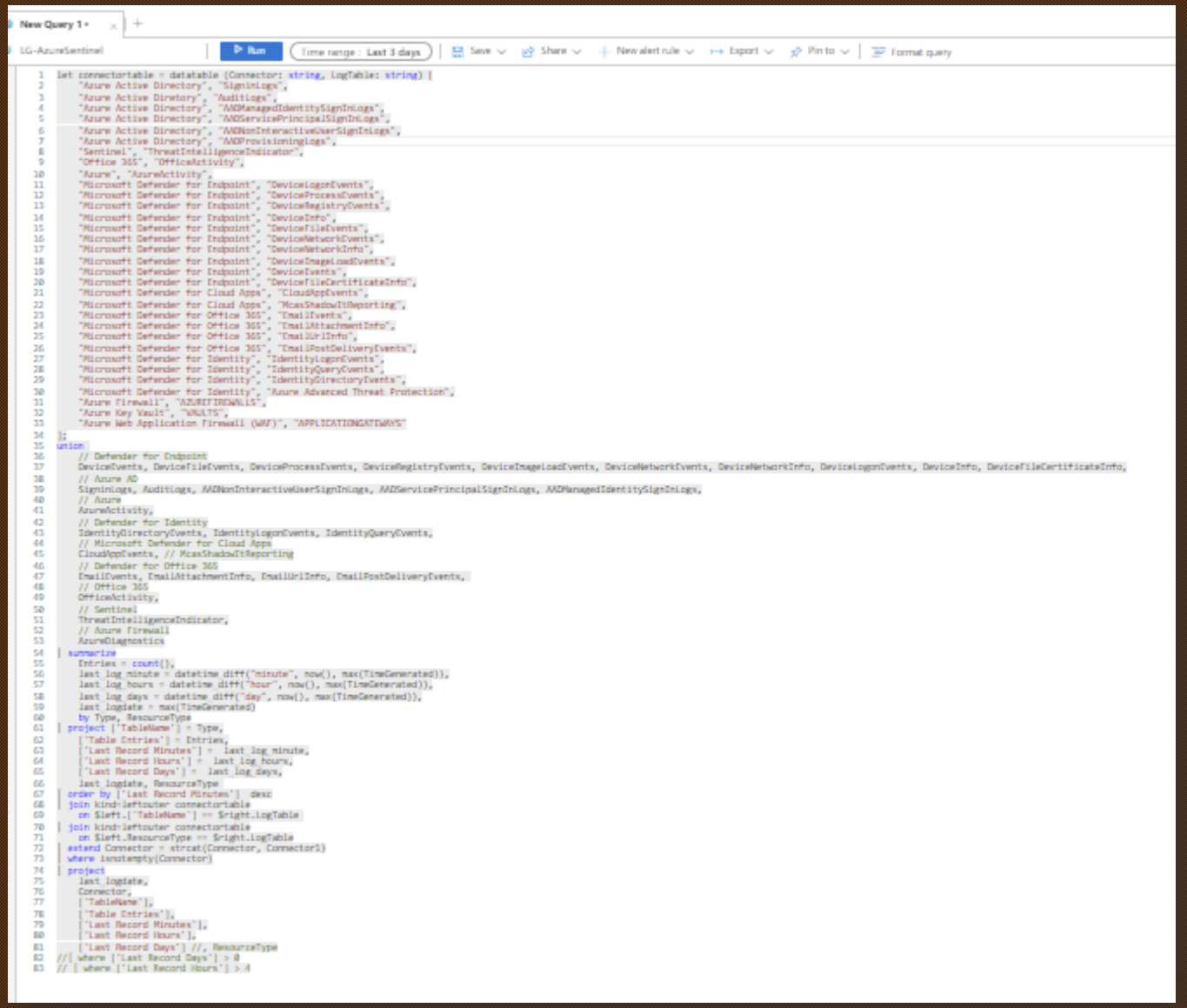
This Month – Microsoft Sentinel – Connector Health







This Month – Microsoft Sentinel – Connector Health

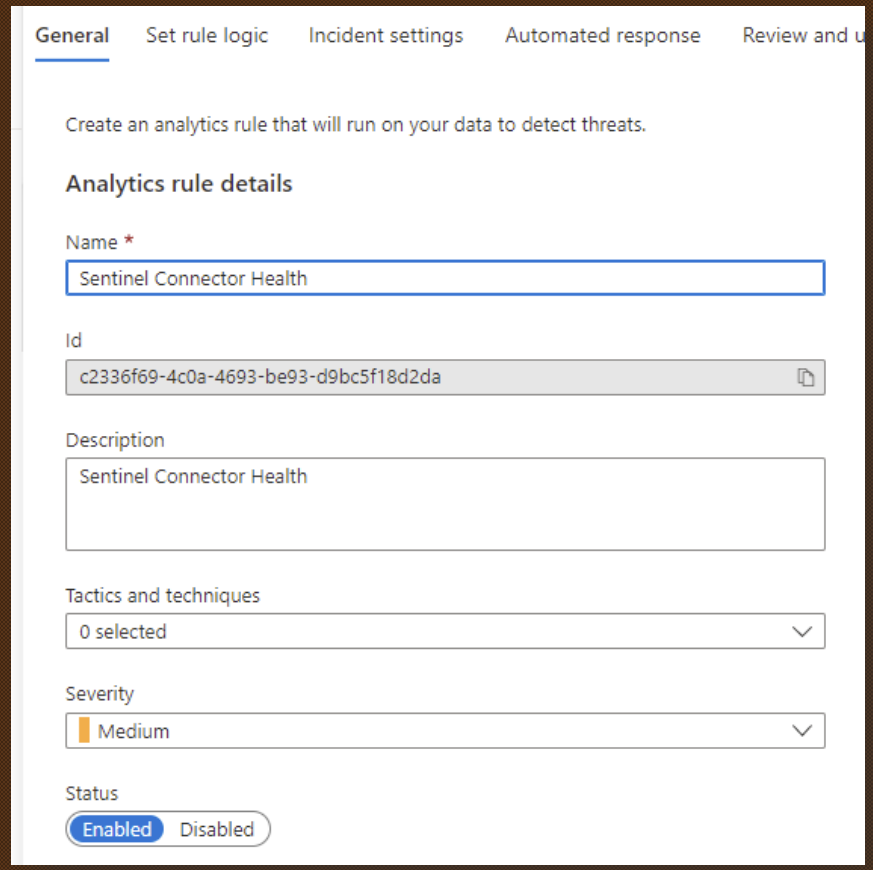


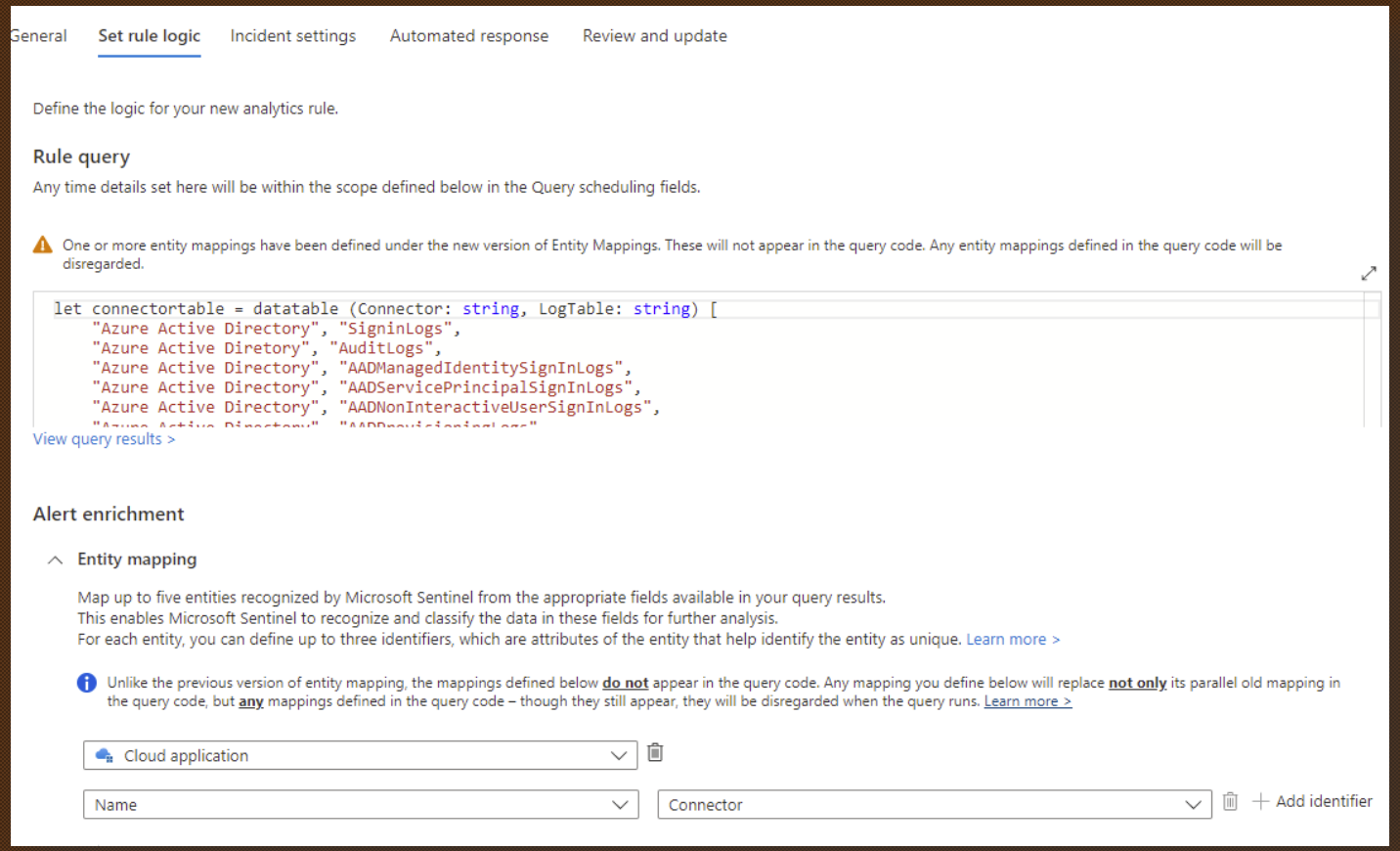
```
let connectortable = datatable (Connector: string, LogTable: string) [
    "Azure Active Directory", "SigninLogs",
    "Azure Active Directory", "AuditLogs",
    "Azure Active Directory", "AADManagedIdentitySignInLogs",
    "Azure Active Directory", "AADServicePrincipalSignInLogs",
    "Azure Active Directory", "AADNonInteractiveUserSignInLogs",
    "Azure Active Directory", "AADProvisioningLogs",
    "Sentinel", "ThreatIntelligenceIndicator",
    "Office 365", "OfficeActivity",
    "Azure", "AzureActivity",
    "Microsoft Defender for Endpoint", "DeviceLogonEvents",
    "Microsoft Defender for Endpoint", "DeviceProcessEvents",
    "Microsoft Defender for Endpoint", "DeviceRegistryEvents",
    "Microsoft Defender for Endpoint", "DeviceInfo",
    "Microsoft Defender for Endpoint", "DeviceFileEvents",
    "Microsoft Defender for Endpoint", "DeviceNetworkEvents",
    "Microsoft Defender for Endpoint", "DeviceNetworkInfo",
    "Microsoft Defender for Endpoint", "DeviceImageLoadEvents",
    "Microsoft Defender for Endpoint", "DeviceEvents",
    "Microsoft Defender for Endpoint", "DeviceFileCertificateInfo",
    "Microsoft Defender for Cloud Apps", "CloudAppEvents",
    "Microsoft Defender for Cloud Apps", "McasShadowItReporting",
    "Microsoft Defender for Office 365", "EmailEvents",
    "Microsoft Defender for Office 365", "EmailAttachmentInfo",
    "Microsoft Defender for Office 365", "EmailUrlInfo",
    "Microsoft Defender for Office 365", "EmailPostDeliveryEvents",
    "Microsoft Defender for Identity", "IdentityLogonEvents",
    "Microsoft Defender for Identity", "IdentityQueryEvents",
    "Microsoft Defender for Identity", "IdentityDirectoryEvents",
    "Microsoft Defender for Identity", "Azure Advanced Threat Protection",
    "Azure Firewall", "AZUREFIREWALLS",
    "Azure Key Vault", "VAULTS",
    "Azure Web Application Firewall (WAF)", "APPLICATIONGATEWAYS"
];
union
    // Defender for Endpoint
    DeviceEvents, DeviceFileEvents, DeviceProcessEvents, DeviceRegistryEvents, DeviceImageLoadEvents, DeviceNetworkEvents, DeviceNetworkInfo, DeviceLogonEvents, DeviceInfo, DeviceFileCertificateInfo,
    // Azure AD
    SigninLogs, AuditLogs, AADNonInteractiveUserSignInLogs, AADServicePrincipalSignInLogs, AADManagedIdentitySignInLogs,
    // Azure
    AzureActivity,
    // Defender for Identity
    IdentityDirectoryEvents, IdentityLogonEvents, IdentityQueryEvents,
    // Microsoft Defender for Cloud Apps
    CloudAppEvents, // McasShadowItReporting
    // Defender for Office 365
    EmailEvents, EmailAttachmentInfo, EmailUrlInfo, EmailPostDeliveryEvents,
    // Office 365
    OfficeActivity,
    // Sentinel
    ThreatIntelligenceIndicator,
    // Azure Firewall
    AzureDiagnostics
| summarize
    Entries = count(),
    last_log_minute = datetime_diff("minute", now(), max(TimeGenerated)),
    last_log_hours = datetime_diff("hour", now(), max(TimeGenerated)),
    last_log_days = datetime_diff("day", now(), max(TimeGenerated)),
    last_logdate = max(TimeGenerated)
    by Type, ResourceType
| project ['TableName'] = Type,
    ['Table Entries'] = Entries,
    ['Last Record Minutes'] =  last_log_minute,
    ['Last Record Hours'] =  last_log_hours,
    ['Last Record Days'] =  last_log_days,
    last_logdate, ResourceType
| order by ['Last Record Minutes']  desc
| join kind=leftouter connectortable
  on $left.['TableName'] == $right.LogTable
| join kind=leftouter connectortable
  on $left.ResourceType == $right.LogTable
| extend Connector = strcat(Connector, Connector1)
| where isnotempty(Connector)
| project
    last_logdate,
    Connector,
    ['TableName'],
    ['Table Entries'],
    ['Last Record Minutes'],
    ['Last Record Hours'],
    ['Last Record Days'] //, ResourceType
//| where ['Last Record Days'] > 0
// | where ['Last Record Hours'] > 4
```

This Month – Microsoft Sentinel – Connector Health

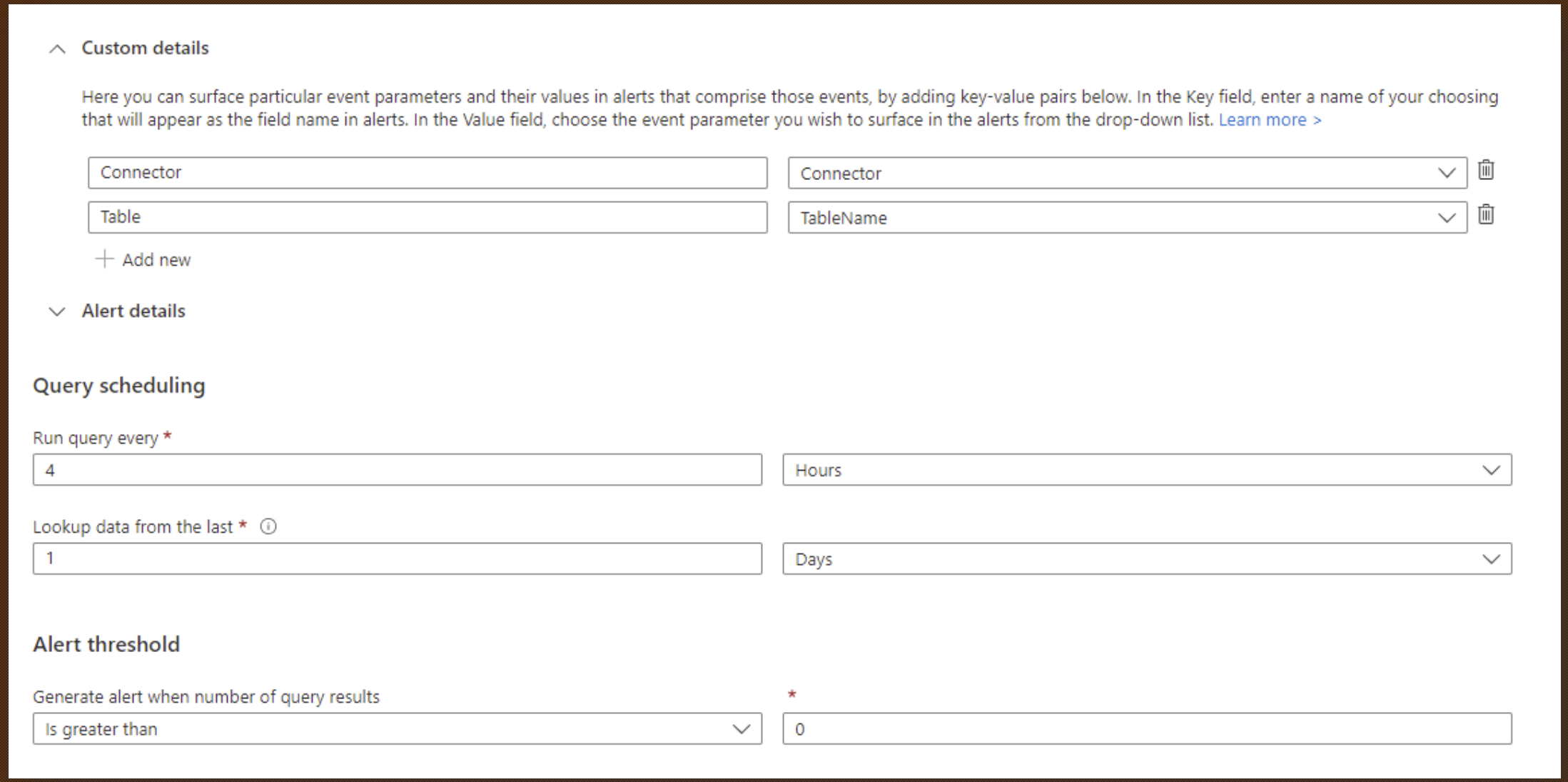
last_logdate [UTC]	Connector	TableName	Table Entries	Last Record Minutes	Last Record Hours	Last Record Days
25.4.2022, 18:34:59.965	Azure	AzureActivity	174	20	0	0
25.4.2022, 18:51:58.179	Azure Active Directory	AADNonInteractiveUse...	242'579	3	0	0
25.4.2022, 18:46:06.340	Azure Active Directory	AADServicePrincipalSig...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

This Month – Microsoft Sentinel – Connector Health

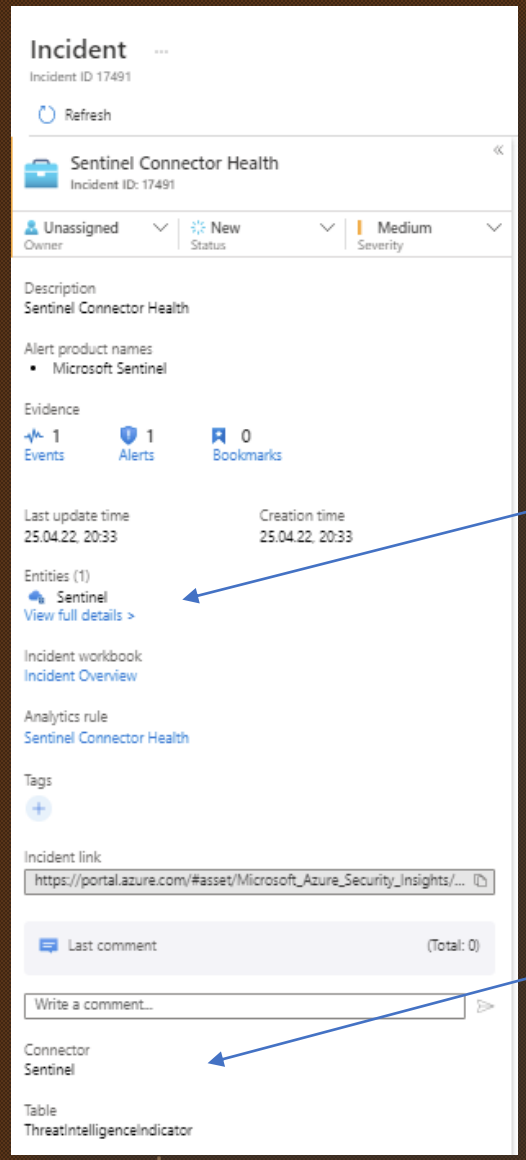


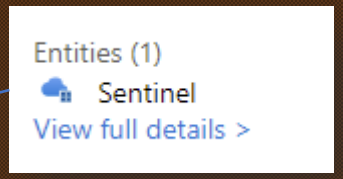


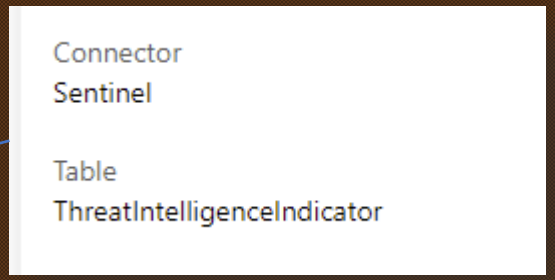
This Month – Microsoft Sentinel – Connector Health



This Month – Microsoft Sentinel – Connector Health







Questions?

Thanks for attending