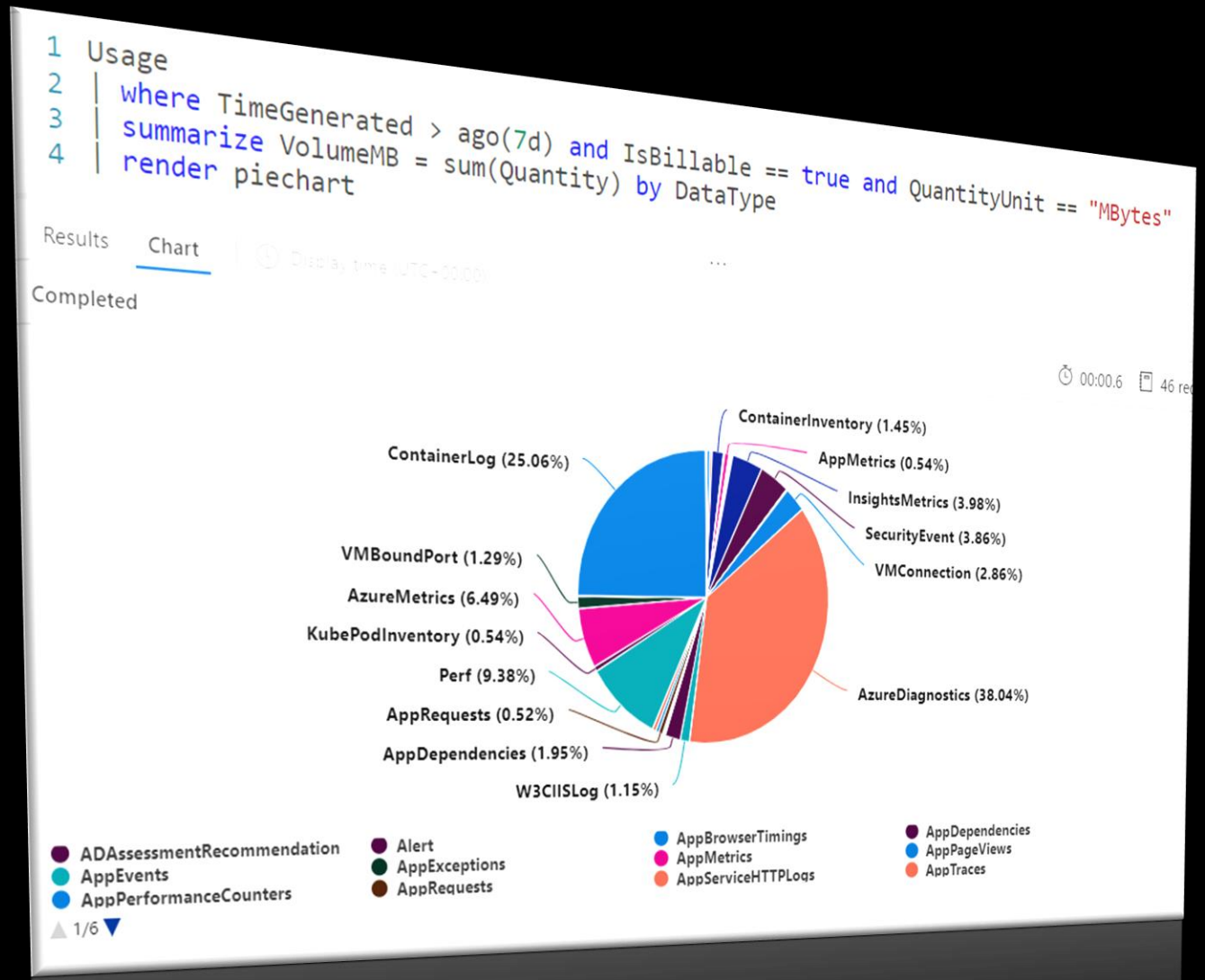


Introduction into KQL

Session Objectives

Introduction into KQL

Provide **simple demonstrations**

Retrieve, Inject Azure Log Analytics data with **PowerShell**

Real World examples

Inspire to learn more

IT Pro Toolbox

Back then

Batch Scripting / SQL

Today

PowerShell, KQL

baseVISION

Microsoft® Most Valuable Professional

Windows Insider MVP

GSEC

MICROSOFT PROFESSIONAL PROGRAM
Cybersecurity

Alex Verboon

Principal Cyber Security Consultant, baseVISION AG

Contact Me

https://twitter.com/alexverboon

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

GitHub https://github.com/alexverboon

https://www.verboon.info/

KQL History

2016 - Introducing Application Insights Analytics by Brian Harry
https://devblogs.microsoft.com/bharry/introducing-application-analytics/

2017 - Azure Log Analytics workspace upgrades are in progress
https://azure.microsoft.com/en-us/blog/azure-log-analytics-workspace-upgrades-are-in-progress/

This upgrade introduces an improved search experience, powered by a highly scalable platform. The new experience includes an interactive and expressive query language, machine learning constructs and a portal for advanced analytics, offering a multiline query editor, full schema view and rich visualizations to help you get deeper insights from your data. Learn more about the new query language.

To take advantage of the following language benefits and more, you'll need to upgrade your Log Analytics workspace:

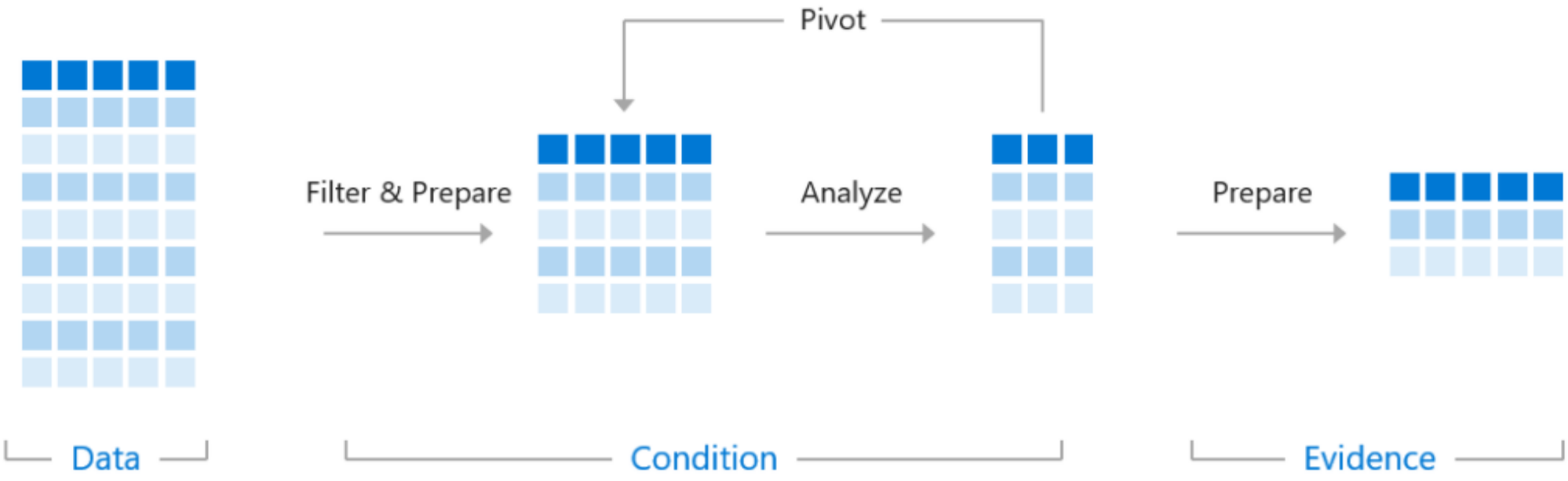
- **Simple yet powerful.** Easier to understand and similar to SQL with constructs like a natural language.
- **Full piping language.** Extensive piping capabilities where any output can be piped to another command to create complex queries that were possible previously.
- **Search-time field extractions.** Calculated fields at runtime lets you use complex calculations for extended fields and then use them for additional commands including joins and aggregations.
- **Advanced joins.** Ability to join tables on multiple fields, using inner and outer joins, and join on extended fields.
- **Date/time functions**. Advanced date/time functions that gives you greater flexibility.
- **Smart Analytics**. Advanced algorithms to evaluate patterns in datasets and compare different sets of data.
- See more information in "Why the new language?"

2017 - The improved Azure Log Analytics: A powerful query language with machine learning, and more
https://channel9.msdn.com/Events/Ignite/Microsoft-Ignite-Orlando-2017/BRK3269

A Kusto query is a **read-only** request to process data and return results. The request is stated in plain text, using a data-flow model designed to make the syntax easy to read, author, and automate. The query uses schema entities that are organized in a hierarchy similar to SQL's: databases, tables, and columns.

KQL

```
SecurityEvent | where EventID == "4626" | summarize count() by Account | limit 10
```



Microsoft Solutions with KQL support

- Azure Log Analytics
- Azure Sentinel
- Microsoft 365 Defender
- CMPIvot – Microsoft Endpoint Configuration Manager
- Jupyter Notebooks
- Azure Data Explorer

KQL – SQL Cheat sheet

Category	SQL Query	Kusto Query
Select data from table	SELECT * FROM dependencies	dependencies
	SELECT name, resultCode FROM dependencies	dependencies | project name, resultCode
	SELECT TOP 100 * FROM dependencies	dependencies | take 100
Comparison operators (date)	SELECT * FROM dependencies WHERE timestamp > getdate()-1	dependencies | where timestamp > ago(1d)
Comparison operators (string)	SELECT * FROM dependencies WHERE type = "Azure blob"	dependencies | where type == "Azure blob"
	-- substring SELECT * FROM dependencies WHERE type like "%blob%"	// substring dependencies | where type contains "blob"

	-- wildcard
	SELECT * FROM dependencies
	WHERE type like "Azure%"
		// wildcard
		dependencies
		| where type startswith "Azure"
		// or
		dependencies
		| where type matches regex "^Azure.*"

Source: SQL to Kusto cheat sheet https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/sqlcheatsheet

Log Analytics Demo Workspace

Log Analytics Demo environment: https://aka.ms/lademo

Microsoft Azure

Search resources, services, and docs (G+/)

DEFAULT DIRECTORY ALEX - PER...

Home >

Logs

Demo

New Query 1*

Demo

Tables Queries Filter

Search

Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the ☆ icon

- Active Directory Health Check
- Azure Monitor for VMs
- Change Tracking
- ContainerInsights
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- Service Map
- Update Management
- Custom Logs
- Functions

Run | Time range : Custom | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

Feedback | Queries | Query explorer

```
1 SecurityAlert
2 | distinct AlertName
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the custom time range.

00:00.6 | 6 records

AlertName
Suspicious process executed [seen multiple times]
Malicious credential theft tool execution detected
Suspected credential theft activity
'Mimikatz' hacktool was detected
Suspicious process executed
Traffic detected from IP addresses recommended for blocking

Page 1 of 1 | 50 items per page | 1 - 6 of 6 items


render
where
let
project
extend
take
count
summarize
search
join
distinct
top

Search - Searches all columns in the table for the value

Run | Time range : Last 7 days | Save | Copy link | New alert rule | Export | Pin to dashb

```
search "Malicious"
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	$table	Computer	AgentId	Type
3/11/2021, 6:02:34.927 PM	SecurityAlert			SecurityAlert
3/11/2021, 6:51:44.156 PM	SecurityAlert			SecurityAlert
3/12/2021, 3:02:40.078 AM	SecurityAlert			SecurityAlert
3/12/2021, 12:07:13.495 PM	SecurityAlert			SecurityAlert
3/8/2021, 8:47:46.168 PM	ADAssessmentRecommendation	DC11.na.contosohotels.com		ADAssessmentRecommenda
3/8/2021, 8:47:46.168 PM	ADAssessmentRecommendation	DC11.na.contosohotels.com		ADAssessmentRecommenda
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	DC11.na.contosohotels.com		ADAssessmentRecommenda
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	DC11.na.contosohotels.com		ADAssessmentRecommenda
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	DC11.na.contosohotels.com		ADAssessmentRecommenda
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	DC11.na.contosohotels.com		ADAssessmentRecommenda
3/8/2021, 8:47:46.128 PM	ADAssessmentRecommendation	DC11.na.contosohotels.com		ADAssessmentRecommenda

Search across all tables

Run | Time range : Last 7 days | Save

```
search "Malicious"
| distinct $table
```

Results | Chart | Columns | Display t

Completed. Showing results from the last 7 days.

$table
ADAssessmentRecommendation
VMProcess
SecurityAlert
Update
SecurityDetection
ConfigurationChange
ConfigurationData
ServiceMapProcess_CL
SecurityEvent

List of all tables where the search has matches

search

Run | Time range : Last 7 days | Save | Copy link | New

```
search in (SecurityAlert, SecurityEvent ) "malicious"
```

Results | Chart | Columns | Display time (UTC+00:00)

Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	$table	DisplayN
3/11/2021, 6:02:34.927 PM	SecurityAlert	Maliciou
3/11/2021, 6:51:44.156 PM	SecurityAlert	Suspicio
3/12/2021, 3:02:40.078 AM	SecurityAlert	Maliciou

Limit search to specified tables

Feedbac

Run | Time range : Last 7 days | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

```
// search in column Description
search Description:"malicious"
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	$table	Description	Computer
3/8/2021, 8:47:46.168 PM	ADAssessmentRecommendation	Failure to keep core infrastructure servers updated with the latest operating system updat...	DC11.na.contosohote
3/8/2021, 8:47:46.168 PM	ADAssessmentRecommendation	Failure to keep core infrastructure servers updated with the latest operating system updat...	DC11.na.contosohote
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	Your Active Directory environment includes FGPPs that allow reversible password encrypti...	DC11.na.contosohote
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	Your environment currently permits blank passwords. This is a serious security deficiency t...	DC11.na.contosohote
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	Your environment is configured to store passwords using reversible encryption. This is ess...	DC11.na.contosohote
3/8/2021, 8:47:46.123 PM	ADAssessmentRecommendation	Your environment does not enforce password complexity rules. This creates a security vuln...	DC11.na.contosohote

Limit search to specified column

where

Run | Time range : Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashboard | Fo

```
SecurityAlert
| where AlertSeverity == "High"
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours.

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	De
3/11/2021, 3:03:45.408 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A
3/11/2021, 2:58:23.936 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A
3/11/2021, 4:03:55.362 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A
3/11/2021, 7:02:54.146 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A
3/12/2021, 1:03:29.040 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A
3/12/2021, 2:02:09.294 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A
3/12/2021, 7:02:59.771 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A
3/12/2021, 11:16:30.194 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A

where

Run | Time range : Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

```
SecurityAlert
| where AlertSeverity == "High" and ProviderName == "MDATP"
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours.

AlertName	AlertSeverity	Description	ProviderName	VendorName
tected Malicious credential theft tool execution detected	High	A known credential theft tool execution command line was detected....	MDATP	Microsoft
tected Malicious credential theft tool execution detected	High	A known credential theft tool execution command line was detected....	MDATP	Microsoft
tected Malicious credential theft tool execution detected	High	A known credential theft tool execution command line was detected....	MDATP	Microsoft
tected Malicious credential theft tool execution detected	High	A known credential theft tool execution command line was detected....	MDATP	Microsoft

Take

take is a simple, quick, and efficient way to view a small sample of records when browsing data interactively,

Run | Time range : Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashboard

```
SecurityAlert
| where AlertSeverity == "High"
| take 10
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours.

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity
3/11/2021, 6:02:34.927 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/11/2021, 6:51:44.156 PM	Suspicious process executed [seen multiple times]	Suspicious process executed [seen multiple times]	High
3/12/2021, 3:02:40.078 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/12/2021, 12:07:13.495 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/11/2021, 5:03:08.580 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/12/2021, 5:03:46.804 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/11/2021, 3:03:45.408 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/11/2021, 2:58:23.936 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/11/2021, 4:03:55.362 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/11/2021, 7:02:54.146 PM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High

Use take if you just need some random data

Count & Summarize

Run | Time range : Last 7 days | Save

```
SecurityAlert
| count
```

Results | Chart | Columns | Display time

Completed. Showing results from the last 7 days.

Count
240

Run | Time range : Last 7 days | Save | Co

```
SecurityAlert
| summarize Alerts = count() by ProductName
```

Results | Chart | Columns | Display time (UTC+

Completed. Showing results from the last 7 days.

ProductName	Alerts
Microsoft Defender ATP	228
Azure Security Center	12

Count & Summarize

Run | Time range : Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashboard | Format quer

```
// Count total computers from last 24 hours
SecurityEvent
| summarize dcount(Computer)

// show last event per computer
SecurityEvent
| summarize arg_max(TimeGenerated,*) by Computer
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours. 00:00.6 62 recc

TimeGenerated [UTC]	Computer	Account	AccountType	EventSourceName	Cha
3/13/2021, 10:17:42.897 AM	DC00.na.contosohotels.com	NA.CONTOSOHOTELS.COM\DC01$	Machine	Microsoft-Windows-Security-Auditing	Sec
3/13/2021, 10:17:08.017 AM	RETAILVM01	NT AUTHORITY\SYSTEM	User	Microsoft-Windows-AppLocker	Mic
3/13/2021, 10:17:05.123 AM	AppFE0000000	NT AUTHORITY\SYSTEM	User	Microsoft-Windows-AppLocker	Mic
3/13/2021, 10:17:12.013 AM	SQL01.na.contosohotels.com	NT AUTHORITY\SYSTEM	User	Microsoft-Windows-AppLocker	Mic
3/13/2021, 10:17:57.013 AM	AppBE01.na.contosohotels.com	NT AUTHORITY\SYSTEM	User	Microsoft-Windows-AppLocker	Mic
3/13/2021, 10:17:36.777 AM	DC01.na.contosohotels.com	NA\SQL01$	Machine	Microsoft-Windows-Security-Auditing	Sec
3/13/2021, 10:17:10.013 AM	SQL00.na.contosohotels.com	NT AUTHORITY\SYSTEM	User	Microsoft-Windows-AppLocker	Mic
3/13/2021, 10:06:26.017 AM	AppFE00001VR	NT AUTHORITY\SYSTEM	User	Microsoft-Windows-AppLocker	Mic
3/13/2021, 10:17:20.520 AM	SQL12.na.contosohotels.com	NT AUTHORITY\SYSTEM	User	Microsoft-Windows-AppLocker	Mic

Extend

Use **extend** to create calculated columns and append them to the result set.

TimeGenerated [UTC]	File_Name_	DisplayName	AlertName	AlertSeverity	Description
3/11/2021, 6:02:34.927 PM	mimikatz.exe	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High	A known credential theft tool

TenantId	81a662b5-8541-481b-977d-5d956616ac5e
TimeGenerated [UTC]	2021-03-11T18:02:34.927Z
DisplayName	Malicious credential theft tool execution detected
AlertName	Malicious credential theft tool execution detected
AlertSeverity	High
Description	A known credential theft tool execution command line was detected. Either the process itself or its command line indicated an intent to dump users' credentials, keys, plain-text passwords and mo
ProviderName	MDATP
VendorName	Microsoft
VendorOriginalId	da637508268687784841_-1738974795:_1jArodPEu5XmfE9oBZ4JAYFUKgyT_kGcabbAtulfq0=:WS81a662b5-8541-481b-977d-5d9
SystemAlertId	2517868152005106304_da637508268687784841_-1738974795:_1jArodPEu5XmfE9oBZ4JAYFUKgyT_kGcabbAtulfq0=:WS81a662b
ResourceId	/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourceGroups/CH1-OpsRG-Pri/providers/Microsoft.Compute/virtua
SourceComputerId	4c41ef38-23b5-438a-b776-a7c7d1cf202d
AlertType	VM.MDATP_f5d3c5d8-ec3a-4412-ab45-934d8faff42c
IsIncident	false
StartTime [UTC]	2021-03-11T17:59:59.489Z
EndTime [UTC]	2021-03-11T17:59:59.489Z
ProcessingEndTime [UTC]	2021-03-11T18:02:38.969Z
RemediationSteps	["1. Make sure the machine is completely updated and all your software has the latest patch.", "2. Contact your incident respo
ExtendedProperties	{ "Windows Defender ATP link": "{\"displayValue\":\"Investigate the alert in the Windows Defender ATP portal\",\"kind\":\"Link\",\"value\":\"https://securitycenter.windows.co
File Name	mimikatz.exe

IsIncident	false
StartTime [UTC]	2021-03-11T17:59:59.489Z
EndTime [UTC]	2021-03-11T17:59:59.489Z
ProcessingEndTime [UTC]	2021-03-11T18:02:38.969Z
RemediationSteps	["1. Make sure the machine is completely updated and all y
ExtendedProperties	{ "Windows Defender ATP link": "{\"displayValue\":\"Investi
File Name	mimikatz.exe
	contosohotels.com
	m00
	re
	c73b8-9ebd-4176-abcd-f5fe690bb748
Windows Defender ATP link	{"displayValue":"Investigate the alert in the Wind
resourceType	Virtual Machine

Extend column

Include "mimikatz.exe"

Exclude "mimikatz.exe"

Extend

Run | Time range : Last 7 days | Save | Copy link | New alert rule | Export | Pin to dashboard | Format

```
SecurityAlert
| extend File_Name_ = tostring(parse_json(ExtendedProperties).["File Name"])
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	File_Name_	DisplayName	AlertName	AlertS
3/11/2021, 6:02:34.927 PM	mimikatz.exe	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/11/2021, 6:51:44.156 PM		Suspicious process executed [seen multiple times]	Suspicious process executed [seen multiple times]	High
3/12/2021, 3:02:40.078 AM	mimikatz.exe	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/12/2021, 12:07:13.495 PM	mimikatz.exe	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/5/2021, 3:06:02.015 PM	mimikatz.exe	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/10/2021, 1:02:49.463 AM	samlib.dll	Suspected credential theft activity	Suspected credential theft activity	Mediu
3/10/2021, 3:02:18.374 AM	hid.dll	Suspected credential theft activity	Suspected credential theft activity	Mediu
3/10/2021, 4:03:27.377 AM	vaultcli.dll	Suspected credential theft activity	Suspected credential theft activity	Mediu

Extend

Run | Time range : Set in query | Save | Copy link | New alert rule | Export

```
SecurityAlert
| where TimeGenerated > ago(7d)
| extend severityOrder = case (
    AlertSeverity == "High", 3,
    AlertSeverity == "Medium", 2,
    AlertSeverity == "Low", 1,
    AlertSeverity == "Informational", 0,
    -1)
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed

TimeGenerated [UTC]	AlertSeverity	severityOrder	DisplayName	Al
3/6/2021, 3:01:28.575 PM	High	3	Malicious credential theft tool execution detected	M
3/6/2021, 11:01:15.953 AM	High	3	Malicious credential theft tool execution detected	M
3/6/2021, 1:01:11.899 PM	High	3	Malicious credential theft tool execution detected	M
3/6/2021, 2:02:12.363 PM	High	3	Malicious credential theft tool execution detected	M
3/6/2021, 12:02:46.739 PM	High	3	Malicious credential theft tool execution detected	M
3/6/2021, 9:01:34.988 PM	High	3	Malicious credential theft tool execution detected	M
3/6/2021, 11:02:02.438 PM	High	3	Malicious credential theft tool execution detected	M

Distinct

Produces a table with the distinct combination of the provided columns of the input table.

Run | Time range : Custom | Save | Copy link | New alert rule | Export | Pin to dashboard | Format qu

```
SecurityAlert
| extend HostName_ = tostring(parse_json(Entities)[1].HostName)
| distinct AlertName
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the custom time range.

AlertName
Malicious credential theft tool execution detected
Suspicious process executed [seen multiple times]
Suspected credential theft activity
'Mimikatz' hacktool was detected
Suspicious process executed
Suspicious WMI process creation
Traffic detected from IP addresses recommended for blocking

Run | Time range : Custom | Save | Copy link | New alert rule | Export

```
SecurityAlert
| extend HostName_ = tostring(parse_json(Entities)[1].HostNa
| distinct AlertName, HostName_
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the custom time range.

AlertName	HostName_
Malicious credential theft tool execution detected	victim00
Suspected credential theft activity	
Suspicious process executed [seen multiple times]	
Malicious credential theft tool execution detected	
'Mimikatz' hacktool was detected	
Suspicious process executed	
Suspicious WMI process creation	appfe00000g4
Suspicious WMI process creation	
Suspicious WMI process creation	appfe00000g5
Suspicious WMI process creation	appfe00000g7
Traffic detected from IP addresses recommended for blocking	

project

Project – select the columns to include in the output

```
let timeago = 7d;
let xEventIDs = dynamic(['4624','4634']);
SecurityEvent
| where TimeGenerated > ago (timeago)
| where (EventID) in (xEventIDs)
| project TimeGenerated, Computer, EventID, Activity, TargetUserName, LogonTypeName
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed with partial results. 00:01.1 30,000+ records

Showing the first 30,000 results. Learn more on how to narrow down the result set.

TimeGenerated [UTC]	Computer	EventID	Activity	TargetUserName	LogonTypeName
3/11/2021, 11:37:43.390 PM	AppFE00001TY	4,624	4624 - An account was successfully logged on.	SYSTEM	5 - Service
3/11/2021, 11:42:14.687 PM	SQL01.na.contosohotels.com	4,624	4624 - An account was successfully logged on.	SYSTEM	5 - Service
3/11/2021, 11:43:01.240 PM	DC00.na.contosohotels.com	4,624	4624 - An account was successfully logged on.	SYSTEM	5 - Service
3/11/2021, 11:43:16.557 PM	DC00.na.contosohotels.com	4,624	4624 - An account was successfully logged on.	DC00$	3 - Network

project-away – exclude columns from the output
project-rename – rename a column
project-keep – columns to keep
Project-reorder – reorder columns in the output

String Operators

Operator	Description	Case-Sensitive	Example (yields true)
==	Equals	Yes	"aBc" == "aBc"
!=	Not equals	Yes	"abc" != "ABC"
=~	Equals	No	"abc" =~ "ABC"
!~	Not equals	No	"aBc" !~ "xyz"
has	Right-hand-side (RHS) is a whole term in left-hand-side (LHS)	No	"North America" has "america"
!has	RHS isn't a full term in LHS	No	"North America" !has "amer"
has_cs	RHS is a whole term in LHS	Yes	"North America" has_cs "America"
!has_cs	RHS isn't a full term in LHS	Yes	"North America" !has_cs "amer"
hasprefix	RHS is a term prefix in LHS	No	"North America" hasprefix "ame"
!hasprefix	RHS isn't a term prefix in LHS	No	"North America" !hasprefix "mer"
hasprefix_cs	RHS is a term prefix in LHS	Yes	"North America" hasprefix_cs "Ame"
!hasprefix_cs	RHS isn't a term prefix in LHS	Yes	"North America" !hasprefix_cs "CA"
hassuffix	RHS is a term suffix in LHS	No	"North America" hassuffix "ica"
!hassuffix	RHS isn't a term suffix in LHS	No	"North America" !hassuffix "americ"
hassuffix_cs	RHS is a term suffix in LHS	Yes	"North America" hassuffix_cs "ica"
!hassuffix_cs	RHS isn't a term suffix in LHS	Yes	"North America" !hassuffix_cs "icA"
contains	RHS occurs as a subsequence of LHS	No	"FabriKam" contains "BRik"
!contains	RHS doesn't occur in LHS	No	"Fabrikam" !contains "xyz"
contains_cs	RHS occurs as a subsequence of LHS	Yes	"FabriKam" contains_cs "Kam"
!contains_cs	RHS doesn't occur in LHS	Yes	"Fabrikam" !contains_cs "Kam"
startswith	RHS is an initial subsequence of LHS	No	"Fabrikam" startswith "fab"
!startswith	RHS isn't an initial subsequence of LHS	No	"Fabrikam" !startswith "kam"
startswith_cs	RHS is an initial subsequence of LHS	Yes	"Fabrikam" startswith_cs "Fab"
!startswith_cs	RHS isn't an initial subsequence of LHS	Yes	"Fabrikam" !startswith_cs "fab"
endswith	RHS is a closing subsequence of LHS	No	"Fabrikam" endswith "Kam"
!endswith	RHS isn't a closing subsequence of LHS	No	"Fabrikam" !endswith "brik"
endswith_cs	RHS is a closing subsequence of LHS	Yes	"Fabrikam" endswith_cs "kam"
!endswith_cs	RHS isn't a closing subsequence of LHS	Yes	"Fabrikam" !endswith_cs "brik"
matches regex	LHS contains a match for RHS	Yes	"Fabrikam" matches regex "b.*k"
in	Equals to one of the elements	Yes	"abc" in ("123", "345", "abc")
!in	Not equals to any of the elements	Yes	"bca" !in ("123", "345", "abc")
in~	Equals to one of the elements	No	"abc" in~ ("123", "345", "ABC")
!in~	Not equals to any of the elements	No	"bca" !in~ ("123", "345", "ABC")
has_any	Same as has but works on any of the elements	No	"North America" has_any("south", "north")

ago

Subtracts the given timespan from the current UTC clock time.

Feedback

Run | Time range : **Last 24 hours** | Save | Share | New alert rule | Export | Pin to dashboa

```
SecurityAlert
| where TimeGenerated > ago (1d)

SecurityAlert
| where TimeGenerated > ago (4h)
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed

TimeGenerated [UTC]	DisplayName	AlertName	AlertSev
3/18/2021, 3:02:35.854 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/18/2021, 4:02:16.902 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/18/2021, 6:02:58.584 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High
3/18/2021, 5:03:58.340 AM	Malicious credential theft tool execution detected	Malicious credential theft tool execution detected	High

bin

Run | Time range : **Last 3 days** | Save | Share | New

```
SecurityAlert
| summarize Events = count() by bin(TimeGenerated,1d)
```

Results | Chart | Columns | Display time (UTC+00:00)

Completed. Showing results from the last 3 days.

TimeGenerated [UTC]	Events
3/15/2021, 12:00:00.000 AM	14
3/16/2021, 12:00:00.000 AM	32
3/17/2021, 12:00:00.000 AM	34
3/18/2021, 12:00:00.000 AM	8

Run | Time range : **Set in query** | Save | Share | New alert rul

```
SecurityAlert
| extend DayGenerated = startofday(TimeGenerated)
| where TimeGenerated between (ago(3d) .. ago(1d))
| summarize Events = count() by bin(TimeGenerated,1d)
```

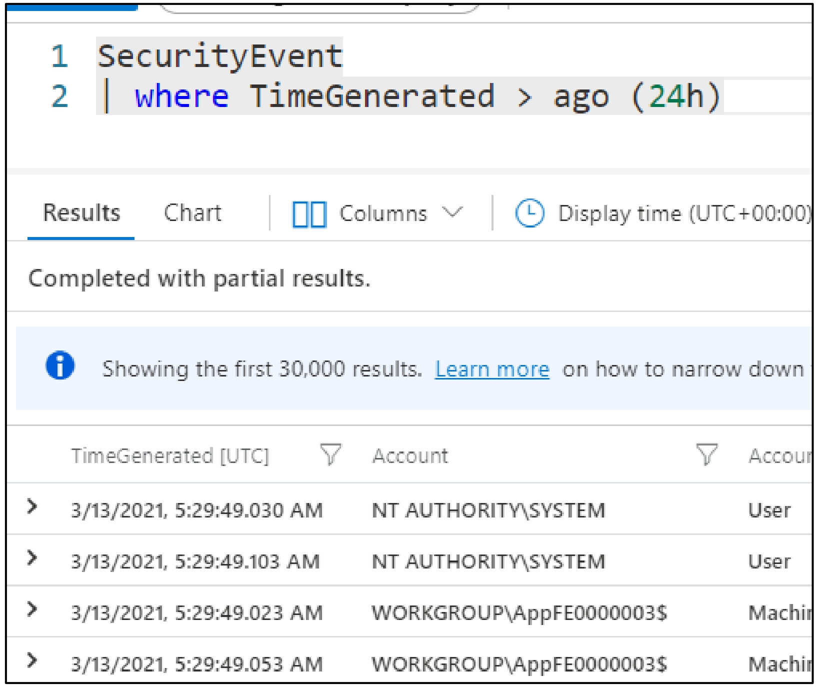
Results | Chart | Columns | Display time (UTC+00:00) | Grou

Completed

TimeGenerated [UTC]	Events
3/17/2021, 12:00:00.000 AM	14
3/16/2021, 12:00:00.000 AM	32
3/15/2021, 12:00:00.000 AM	14

let

Use **let** to define variables

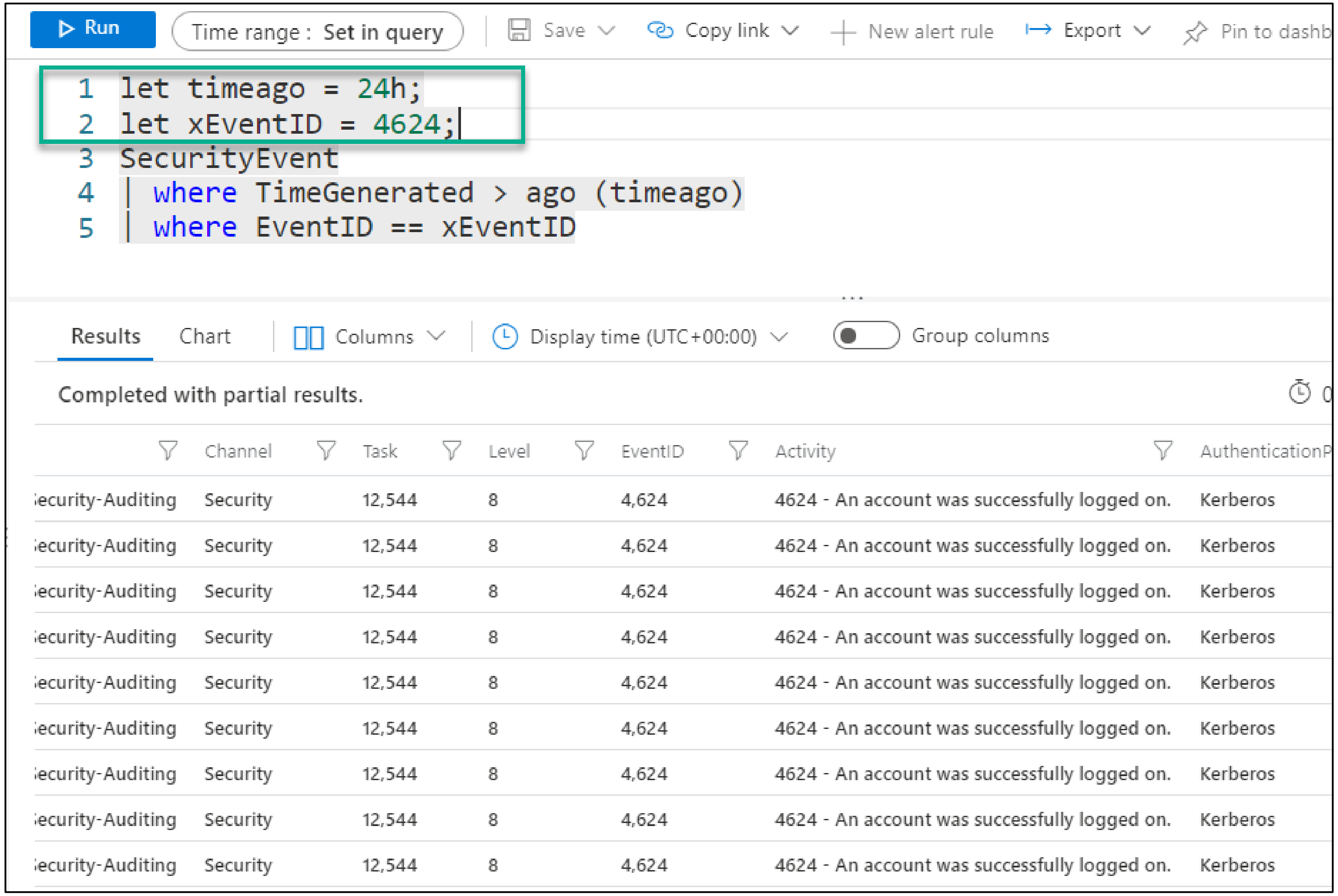


```
SecurityEvent
| where TimeGenerated > ago (24h)
```

Completed with partial results.

Showing the first 30,000 results. Learn more on how to narrow down

	TimeGenerated [UTC]	Account	Accour
›	3/13/2021, 5:29:49.030 AM	NT AUTHORITY\SYSTEM	User
›	3/13/2021, 5:29:49.103 AM	NT AUTHORITY\SYSTEM	User
›	3/13/2021, 5:29:49.023 AM	WORKGROUP\AppFE0000003$	Machi
›	3/13/2021, 5:29:49.053 AM	WORKGROUP\AppFE0000003$	Machi



```
let timeago = 24h;
let xEventID = 4624;
SecurityEvent
| where TimeGenerated > ago (timeago)
| where EventID == xEventID
```

Completed with partial results.

	Channel	Task	Level	EventID	Activity	AuthenticationP
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ecurity-Auditing	Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos

let

Run | Time range : Set in query | Save | Copy link | New alert rule | Export

```
let timeago = 24h;
let xEventIDs = dynamic(['4624','4634']);
SecurityEvent
| where TimeGenerated > ago (timeago)
| where (EventID) in (xEventIDs)
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed with partial results.

Channel	Task	Level	EventID	Activity	AuthenticationP
ng Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ng Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ng Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ng Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ng Security	12,545	8	4,634	4634 - An account was logged off.	
ng Security	12,545	8	4,634	4634 - An account was logged off.	
ng Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos
ng Security	12,545	8	4,634	4634 - An account was logged off.	
ng Security	12,544	8	4,624	4624 - An account was successfully logged on.	Kerberos

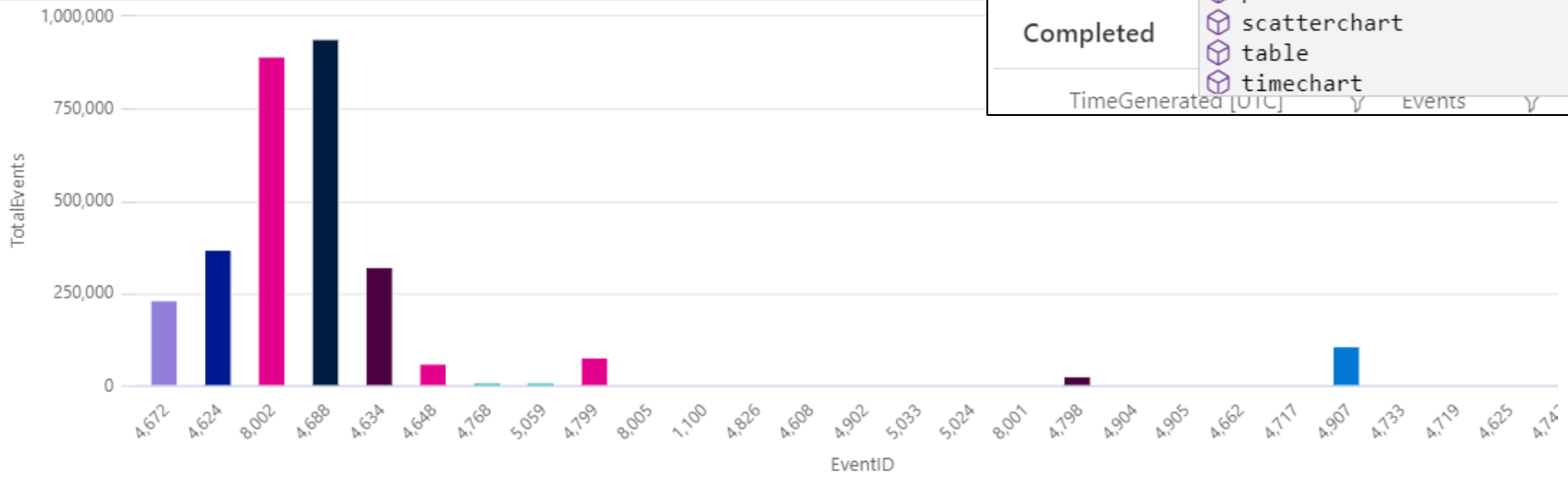
render

Run | Time range : Last 7 days | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

```
SecurityEvent
| summarize TotalEvents = count() by EventID, Activity
| render columnchart
```

Results | Chart | Display time (UTC+00:00)

Completed. Showing results from the last 7 days.



- 1100 - The event logging service has shut down.
- 4624 - An account was successfully logged on.
- 4634 - An account was logged off.
- 4608 - Windows is starting up.
- 4625 - An account failed to log on.
- 4648 - A logon was attempted using explicit credentials.

1/7

```
6 | render
7
```

- areachart
- barchart
- columnchart
- piechart
- scatterchart
- table
- timechart

Results | Completed

TimeGenerated [UTC] | Events

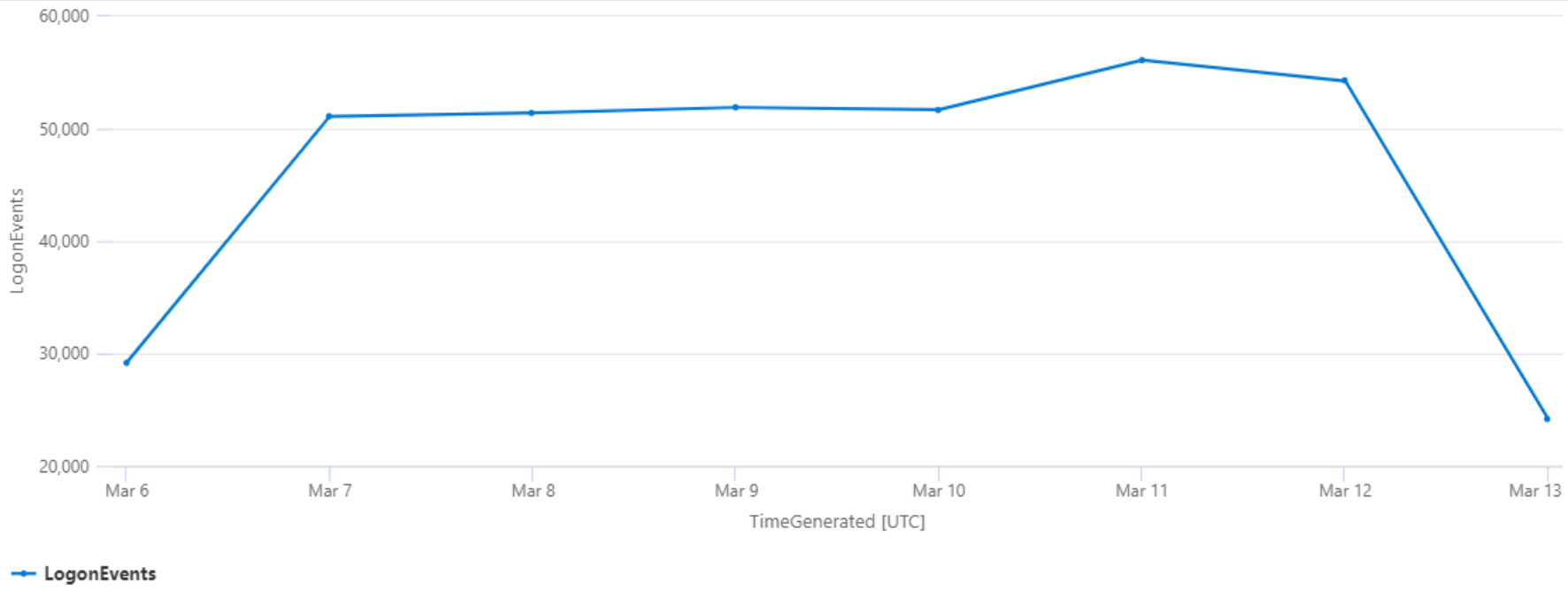
render

Run | Time range : Last 7 days | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

```
SecurityEvent
| where EventID == 4624
| summarize LogonEvents = count() by bin(TimeGenerated,1d)
| render timechart
```

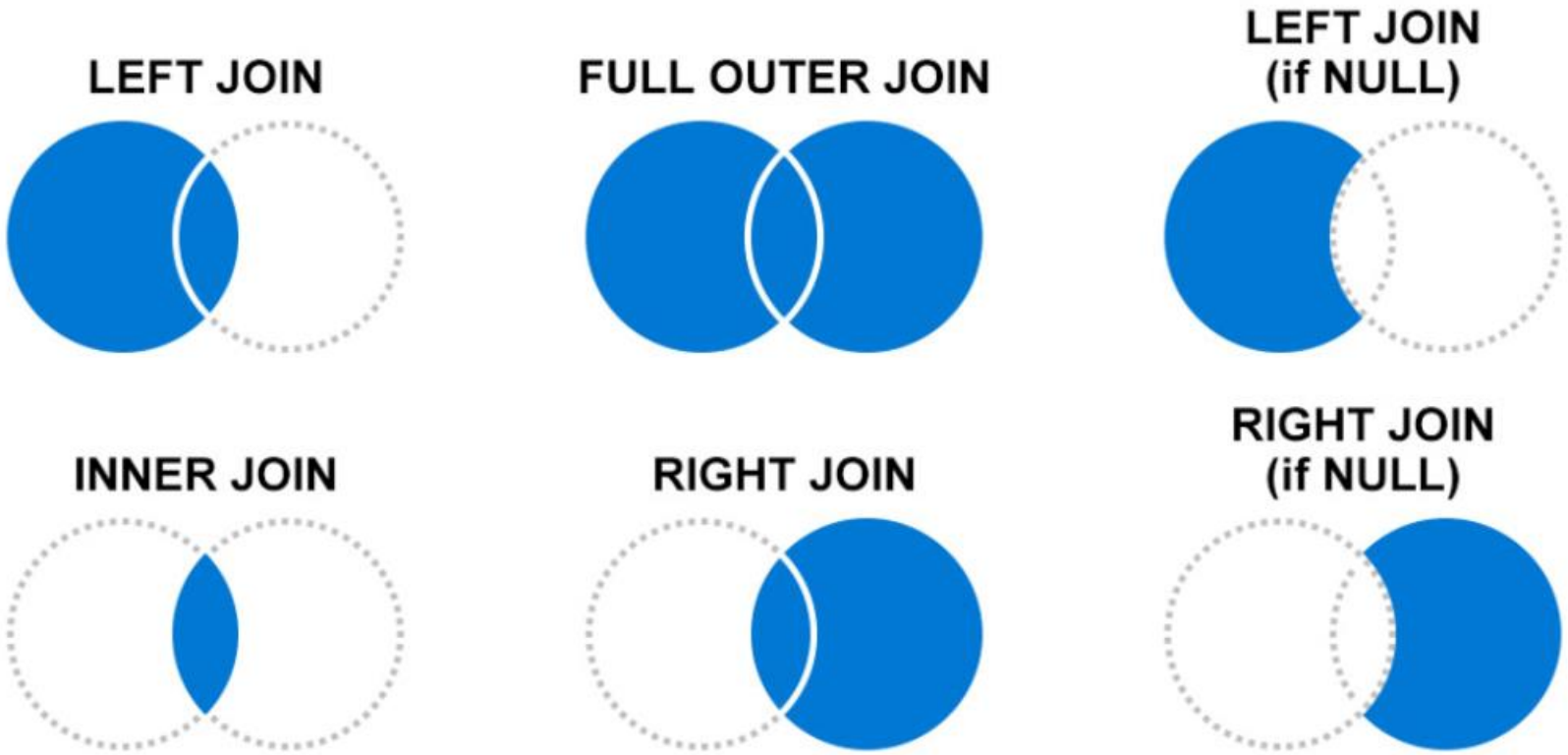
Results | Chart | Display time (UTC+00:00)

Completed. Showing results from the last 7 days. 00:00.6 8 records



join

LeftTable | join [JoinParameters] (RightTable) on Attributes



join

Join Flavor	Output Records
kind=leftanti, kind=leftantisemi	Returns all the records from the left side that don't have matches from the right
kind=rightanti, kind=rightantisemi	Returns all the records from the right side that don't have matches from the left.
kind unspecified, kind=innerunique	Only one row from the left side is matched for each value of the on key. The output contains a row for each match of this row with rows from the right
kind=leftsemi	Returns all the records from the left side that have matches from the right.
kind=rightsemi	Returns all the records from the right side that have matches from the left.
kind=inner	Contains a row in the output for every combination of matching rows from left and right.
kind=leftouter (or kind=rightouter or kind=fullouter)	Contains a row for every row on the left and right, even if it has no match. The unmatched output cells contain nulls.

join

```
SecurityEvent
| where EventID == "4624"
| where Account contains "tim"
| summarize LogOnCount=count() by EventID, Account
| project LogOnCount, Account
| join kind = inner (
    SecurityEvent
    | where EventID == "4634"
    | summarize LogOffCount=count() by EventID, Account
    | project LogOffCount, Account
) on Account
```

esults Chart | Columns | Display time (UTC+00:00) | Group columns

mpleted. Showing results from the last 24 hours.

LogOnCount	Account	LogOffCount	Account1
96	RETAILVM01\timadmin	96	RETAILVM01\timadmin
196	SQL00\timadmin	196	SQL00\timadmin

Externaldata

Use externaldata to include …. External Data in your queries

```
let exchangeserverioninfo = (externaldata (ProductName:string, ReleaseDate:string, Build_short:string, Build_long:string)
[@"https://raw.githubusercontent.com/alexverboon/MDATP/master/AdvancedHunting/Exchange/exchnage_versions.csv"]
with(format="csv",ignoreFirstRecord=true))
| where ProductName !startswith "#"
| project ProductName,ReleaseDate, Build_long, Build_short;
exchangeserverioninfo
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours. 00:01.1 115 records

ProductName	ReleaseDate	Build_long	Build_short
Exchange Server 2019 CU8	15-Dec-20	15.02.0792.003	15.2.792.3
Exchange Server 2019 CU7	15-Sep-20	15.02.0721.002	15.2.721.2
Exchange Server 2019 CU6	16-Jun-20	15.02.0659.004	15.2.659.4
Exchange Server 2019 CU5	17-Mar-20	15.02.0595.003	15.2.595.3
Exchange Server 2019 CU4	17-Dec-19	15.02.0529.005	15.2.529.5

Hello Table

Run | Time range : Last 7 days | Save | Share | New alert rule | Export | Pin to dashboard

```
SecurityAlert
| take 10
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	DisplayName	AlertName	AlertSe
3/10/2021, 1:02:49.463 AM	Suspected credential theft activity	Suspected credential theft activity	Mediu
3/10/2021, 3:02:18.374 AM	Suspected credential theft activity	Suspected credential theft activity	Mediu
3/10/2021, 4:03:27.377 AM	Suspected credential theft activity	Suspected credential theft activity	Mediu

Run | Time range : Last 7 days | Save | Share | New aler

```
SecurityAlert
| getschema
```

Results | Chart | Columns | Display time (UTC+00:00)

Completed. Showing results from the last 7 days.

ColumnName	ColumnOrdinal	DataType	ColumnType
TenantId	0	System.String	string
TimeGenerated	1	System.DateTime	datetime
DisplayName	2	System.String	string
AlertName	3	System.String	string
AlertSeverity	4	System.String	string
Description	5	System.String	string
ProviderName	6	System.String	string
VendorName	7	System.String	string
VendorOriginalId	8	System.String	string
SystemAlertId	9	System.String	string
ResourceId	10	System.String	string
SourceComputerId	11	System.String	string

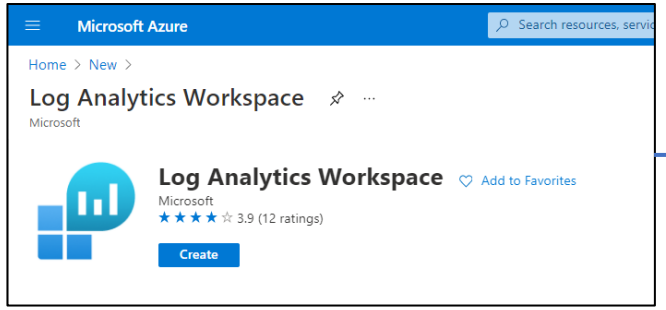
Recommendations

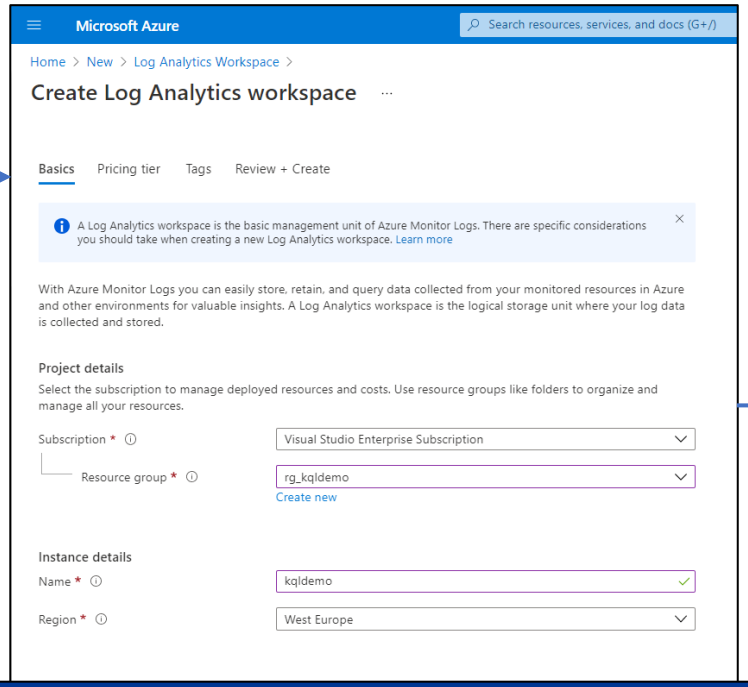
- Use time filters first
- When using join, make the table with fewer rows come first (the left table)
- Look in specific columns
- Use filters as early as possible, before using extend
- Has beats contains
- Size new queries—If you suspect that a query will return a large result set, assess it first using the count operator. Use limit or its synonym take to avoid large result sets.

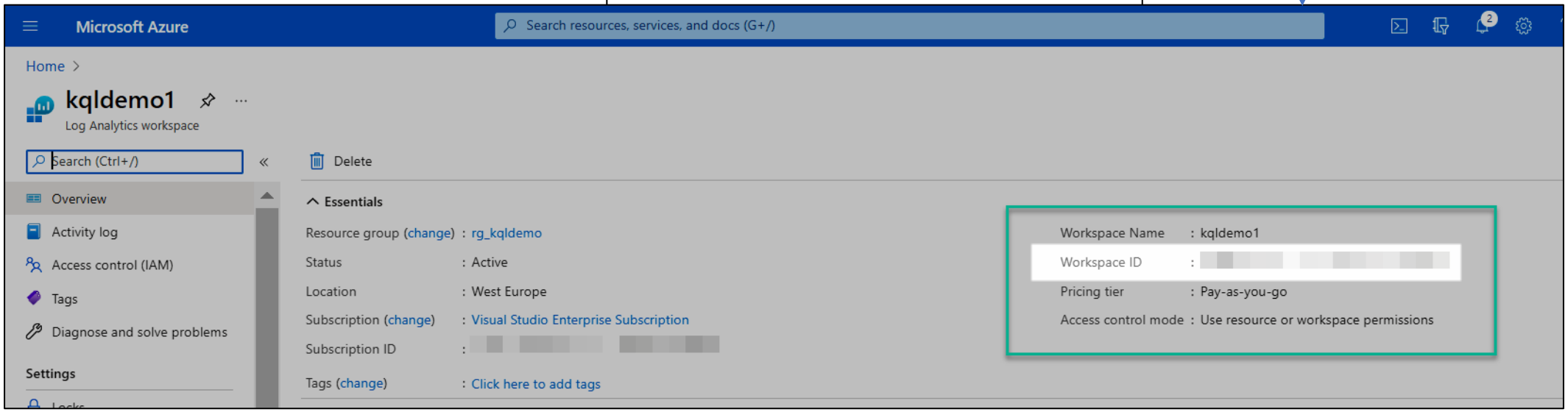
For more recommendations and best practices refer to the learning and training references

https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-best-practices?view=o365-worldwide

Create your own log Analytics workspace







Create your own log Analytics workspace

Microsoft Azure

Search resources, services, and docs (G+/)

Home > kqldemo1

kqldemo1 | Agents management

Log Analytics workspace

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Locks
- Agents management
- Agents configuration
- Computer Groups
- Linked storage accounts

Windows servers | Linux servers

0 Windows computers connected

Go to logs

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.
You'll need the Workspace ID and Key to install the agent.

Download Windows Agent (64 bit)

Download Windows Agent (32 bit)

Workspace ID		
Primary key		Regenerate
Secondary key		Regenerate

Send log data to log analytics with PowerShell

File Edit Selection View Go Run Terminal Help • Send-LADataSample.ps1 - SendData - Visual Studio Code

Send-LADataSample.ps1 ●

Send-LADataSample.ps1 > ...

```
1
2   # Log Analytics workspace
3   $customerId = "[redacted]"
4   $SharedKey = "[redacted]"
5
6   # You can use an optional field to specify the timestamp from the data. If the time field is not specified, Azure Monitor assumes the time is th
7   $TimeStampField = ""
8
9   # InputData
10  $LogType = "CountryCodes"
11  $inputData = Get-Content -Path C:\data\SendData\country.json
12
```

Microsoft Azure | Search resources, services, and docs (G+/)

Home > Log Analytics workspaces > kqldemo

kqldemo | Logs

Log Analytics workspace

New Query 1* | Feedback | Queries | Query explorer

kqldemo | Select scope | Run | Time range : Custom | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

Tables | Queries | Filter

Search

Filter | Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the ☆ icon

LogManagement

Usage

Custom Logs

CountryCodes_CL

Functions

```
1 CountryCodes_CL
```

Results | Chart | Columns | Display time (UTC+00:00) | Group columns

Completed. Showing results from the custom time range. 00:00.4 | 249 records

TimeGenerated [UTC]	Computer	RawData	Code_s	Name_s	Type	_ResourceId	TenantId	SourceSystem
3/6/2021, 3:56:43.603 PM			AX	Åland Islands	CountryCodes_CL		1e0dcc1a-68dc-473c-ac2d-f10d42ef6541	RestAPI
3/6/2021, 3:56:43.603 PM			AL	Albania	CountryCodes_CL		1e0dcc1a-68dc-473c-ac2d-f10d42ef6541	RestAPI
3/6/2021, 3:56:43.603 PM			DZ	Algeria	CountryCodes_CL		1e0dcc1a-68dc-473c-ac2d-f10d42ef6541	RestAPI
3/6/2021, 3:56:43.603 PM			AS	American Samoa	CountryCodes_CL		1e0dcc1a-68dc-473c-ac2d-f10d42ef6541	RestAPI
3/6/2021, 3:56:43.603 PM			AD	Andorra	CountryCodes_CL		1e0dcc1a-68dc-473c-ac2d-f10d42ef6541	RestAPI
3/6/2021, 3:56:43.603 PM			AO	Angola	CountryCodes_CL		1e0dcc1a-68dc-473c-ac2d-f10d42ef6541	RestAPI
3/6/2021, 3:56:43.603 PM			AI	Anguilla	CountryCodes_CL		1e0dcc1a-68dc-473c-ac2d-f10d42ef6541	RestAPI

https://docs.microsoft.com/en-au/azure/azure-monitor/logs/data-collector-api#powershell-sample?WT.mc_id=EM-MVP-5002871

Executing KQL queries from PowerShell

Administrator: PowerShell

```
PS C:\Users\KQLUser>    Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

Administrator: PowerShell

```
PS C:\Users\KQLUser> Connect-AzAccount
```

Administrator: PowerShell

```
PS C:\Users\KQLUser> $query = "CountryCodes_CL | project Code_s,Name_s"
PS C:\Users\KQLUser> $WorkSpaceID = "[redacted]"
PS C:\Users\KQLUser>
```

Administrator: PowerShell

```
PS C:\Users\KQLUser> $kqlresult = Invoke-AzOperationalInsightsQuery -WorkspaceId $WorkSpaceID -Query $query
PS C:\Users\KQLUser>
```

https://dev.loganalytics.io/documentation/Tools/PowerShell-Cmdlets

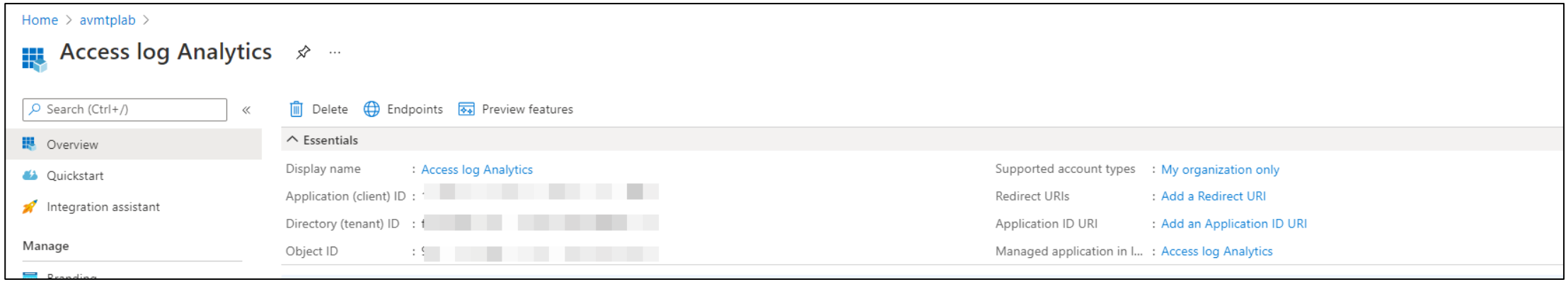
Executing KQL queries from PowerShell

Administrator: PowerShell

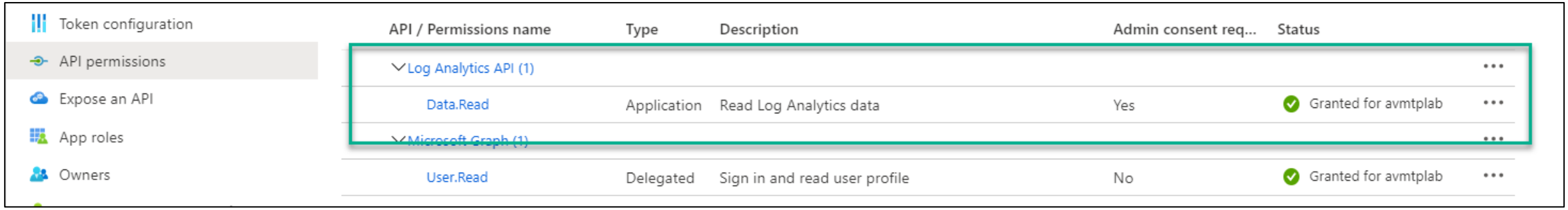
```
PS C:\Users\KQLUser> $kqlresult.Results | Sort-Object Code_s

Code_s Name_s
------ ------
AD     Andorra
AE     United Arab Emirates
AF     Afghanistan
AG     Antigua and Barbuda
AI     Anguilla
AL     Albania
AM     Armenia
AO     Angola
AQ     Antarctica
AR     Argentina
AS     American Samoa
AT     Austria
AU     Australia
AW     Aruba
AX     Åland Islands
AZ     Azerbaijan
BA     Bosnia and Herzegovina
```

Executing KQL queries using API

Register an application , in this example the name is “Access log Analytics”

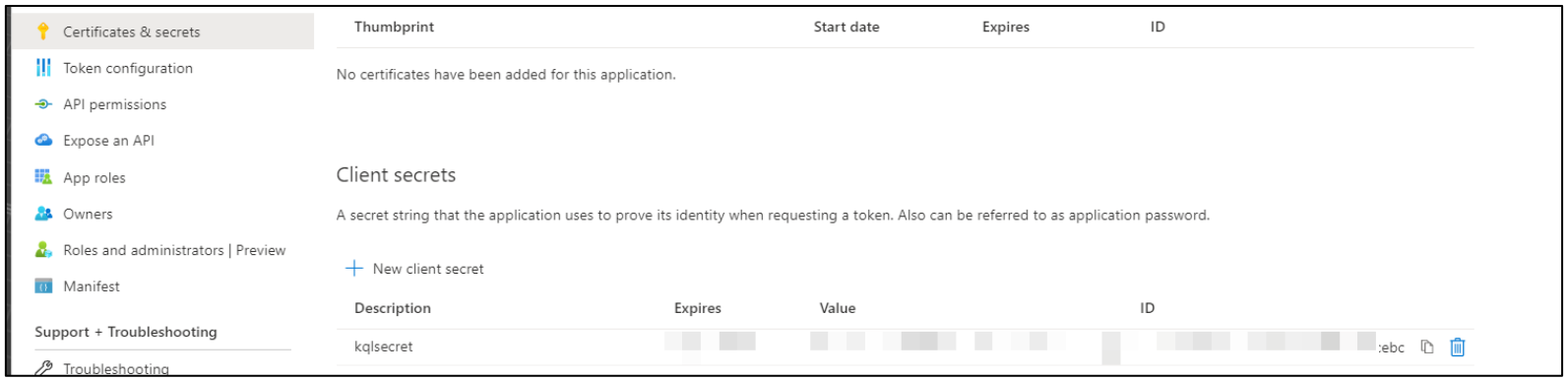


Grant API permissions

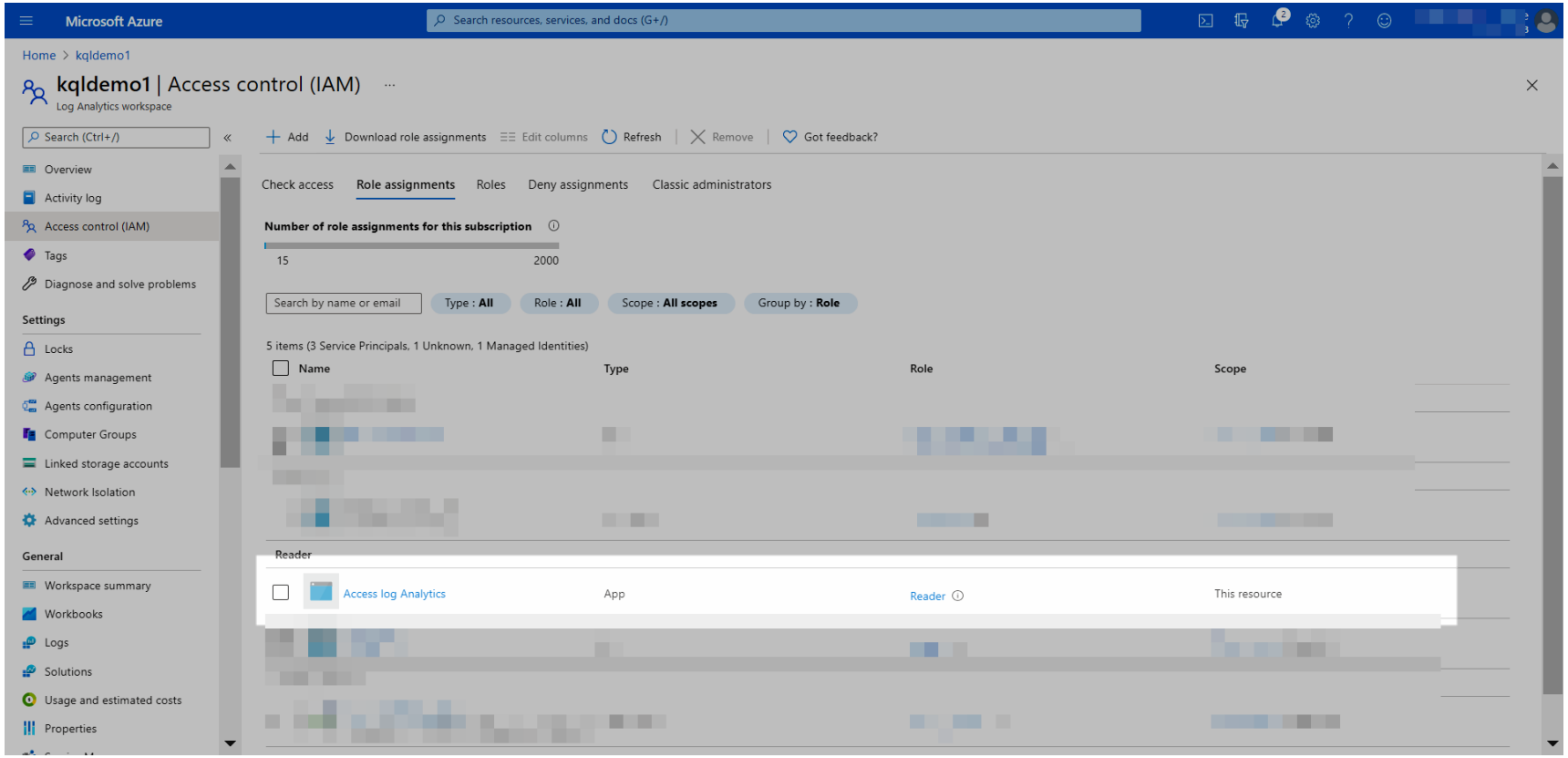


Executing KQL queries using API

Create a client secret



On the log analytics workspace grant permissions



Executing KQL queries using API

QuerylogAPI.ps1 > ...

```
1   $TenantId = '[redacted]
2   $loggingClientID = [redacted]
3   $loggingSecret = [redacted]
4   $logAnalyticsWorkspace = [redacted]
5   $customLogName = "CountryCodes_CL"
6
7   # Get Access Token for Log Analytics to allow KQL Queries to get last ingested events in Custom Logs
8   $loginURL = "https://login.microsoftonline.com/$TenantId/oauth2/token"
9   $resource = "https://api.loganalytics.io"
10  $authbody = @{grant_type = "client_credentials"; resource = $resource; client_id = $loggingClientID; client_secret = $loggingSecret }
11  $oauth = Invoke-RestMethod -Method Post -Uri $loginURL -Body $authbody
12  $headerParams = @{'Authorization' = "$($oauth.token_type) $($oauth.access_token)" }
13  $logAnalyticsBaseURI = "https://api.loganalytics.io/v1/workspaces"
14
15  # submit the query
16  $result = invoke-RestMethod -method Get -uri "$($logAnalyticsBaseURI)/$($logAnalyticsWorkspace)/query?query=$($customLogName)" -Headers $headerParams
17
18  # Format Result to PSObject
19  $headerRow = $null
20  $headerRow = $result.tables.columns | Select-Object name
21  $columnsCount = $headerRow.Count
22  $logData = @()
23  foreach ($row in $result.tables.rows) {
24      $data = new-object PSObject
25      for ($i = 0; $i -lt $columnsCount; $i++) {
26          $data | add-member -membertype NoteProperty -name $headerRow[$i].name -value $row[$i]
27      }
28      $logData += $data
29      $data = $null
30  }
31  $logData
```

PROBLEMS 1 OUTPUT TERMINAL DEBUG CONSOLE

```
RawData             :
Code_s              : US
Name_s              : United States
Type                : CountryCodes_CL
_ResourceId         :

TenantId            : 6237b86f-6859-4f86-ab56-6cd0c788dd55
SourceSystem        : RestAPI
MG                  :
ManagementGroupName :
```

https://blog.darrenjrobinson.com/sending-and-querying-custom-log-data-to-azure-monitor-logs/

KQL in Azure Workbooks

Home > avmtplab

avmtplab | Workbooks | Gallery

Azure Active Directory

- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security

Monitoring

- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings
- Workbooks
- Usage & insights

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

New | Open | Refresh | Feedback | Help | Community Git repo

To get started, choose a report or template below, or use 'Open' to open an existing report.

Search

Subscription: Visual Studio Enterprise Subscription

Quick start

- Empty — A completely empty workbook.

Recently modified workbooks (0)

No items found.

Usage (4)

- Sign-ins
- Sign-ins using Legacy Authent...
- App Consent Audit
- Access Package Activity

Conditional access (4)

- Conditional Access Insights an...
- Sign-ins by Conditional Access...
- Sign-ins by Grant Controls (De...
- Conditional Access Gap Analyz...

Troubleshoot (4)

- Sensitive Operations Report
- Sign-ins Failure Analysis
- Provisioning Analysis
- Archived Log Date Range

Health (1)

- App sign-in health

KQL in Azure Workbooks

Home > Log Analytics workspaces > kqldemo1

kqldemo1 | Workbooks | Gallery

Log Analytics workspace

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Locks
- Agents management
- Agents configuration
- Computer Groups
- Linked storage accounts
- Network Isolation
- Advanced settings

General

- Workspace summary
- Workbooks
- Logs
- Solutions
- Usage and estimated costs
- Properties

New | Open | Refresh | Feedback | Help | Community Git repo

To get started, choose a report or template below, or use 'Open' to open an existing report.

Search

Subscription: Visual Studio Enterprise Subscription

Quick start

- **Default Template** — A report with text and query sections.
- **Empty** — A completely empty workbook.

Recently modified workbooks (1)

- **Demo KQL workbook** — rg_kqldemo

View Designer Guides (8)

- **View Designer Transition Guide** — Quick start guide to use Workbooks fo...
- **Tabbed Overview** — Combines multiple views into a tabbed...
- **Vertical Overview** — Combines multiple views into a vertical...
- **Donut & List** — Outline of the Donut & List Tile from V...
- **Line Chart, Callout, & List** — Outline of the Line Chart, Callout, & Lis...
- **Number & List** — Outline of the Number & List Tile from...
- **Timeline & List** — Outline of the Timeline & List Tile from...
- **Two Numbers & List** — Outline of the Two Numbers & List Tile...

Azure Monitor essentials (1)

- **Log Analytics Agent Health**

Workspace Reports (2)

- **Agent Health**
- **Workspace Usage**

KQL in Azure Workbooks

Home > Log Analytics workspaces > kqldemo1

kqldemo1 | Workbooks | Demo KQL workbook

Log Analytics workspace

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Locks
- Agents management
- Agents configuration
- Computer Groups
- Linked storage accounts
- Network Isolation
- Advanced settings

General

- Workspace summary
- Workbooks
- Logs
- Solutions
- Usage and estimated costs
- Properties

Workbooks | Done Editing | Help

4 Editing query item: query - 2

Settings | Advanced Settings | Style

Query (change) | Time Range | Visualization | Size

Run Query | Samples | kqldemo1 | Set in query | Grid | Medium | Column Settings

Log Analytics workspace Logs Query

Query help

```
let timeago = 900d;
CountryCodes_CL
| where TimeGenerated > ago(timeago)
| extend Code = Code_s
| extend Name = Name_s
| project Code, Name
```

Search

Code	Name
AF	Afghanistan
AX	Åland Islands
AL	Albania
DZ	Algeria
AS	American Samoa
AD	Andorra
AO	Angola

KQL in Azure Workbooks

Home > Azure Sentinel > Azure Sentinel >

Azure AD Sign-in logs - MTPLabSentinel01

mtplabsentinel01

Edit Help

Sign-in Analysis

TimeRange: Last 30 days | Apps: All | Users: All

All Sign-ins	Success	Pending user action	Failure
1.3 K	1.14 K	103	57

Click on a tile or a row in the grid to drill-in further

Sign-ins by Location

Search

Name	Sign-in Count	Trend	Failure Count	Interrupt Count
CH	800		31	64
US	377		9	20
NL	72		3	6
DE	38		14	8
RO	7		0	3

Location Sign-in details

Search

User	Sign-in Status
	Success
	Success
	Success
	Pending user action
	Success

Inspiration

(Real world examples)

Security – Hunting for new scheduled tasks

Run query | New | Save | Share link

```
| where ActionType contains 'ScheduledTaskCreated'
| extend TaskInfo = parse_json(AdditionalFields)
| extend Taskname = TaskInfo.TaskName
| project Timestamp, DeviceName, ActionType, AccountName, Taskname
```

Export | Choose columns

Timestamp	DeviceName	ActionType	AccountName	Taskname
2/22/2021 11:58:26	lclient04	ScheduledTaskCreated		\Microsoft\Windows\Windows Defender\Windows Defender Verification
2/22/2021 11:58:26	lclient04	ScheduledTaskCreated		\Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance
2/22/2021 11:58:26	lclient04	ScheduledTaskCreated		\Microsoft\Windows\Windows Defender\Windows Defender Cleanup
2/22/2021 11:58:26	lclient04	ScheduledTaskCreated		\Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan
2/22/2021 13:37:01	lclient04	ScheduledTaskCreated		\Microsoft\Windows\UpdateOrchestrator\MusUx_LogonUpdateResults
2/22/2021 12:18:49	client01.corp.n	ScheduledTaskCreated		\Microsoft\Windows\Windows Defender\Windows Defender Verification
2/22/2021 12:18:49	client01.corp.n	ScheduledTaskCreated		\Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance

KQL – In the Real world

Monitoring AzureAD Service Principal sign-ins

Microsoft Azure | Search resources, services, and docs (G+/)

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Logs

Selected workspace: 'mtplabsentinel01'

Servicepincipal MT... | New Query 1* | Example queries | Query explorer

MTPLabSentinel01 | Run | Time range : Last 48 hours | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

Tables | Queries | Filter

Search

Group by: Solution Filters: not selected

Favorites

You can add favorites by clicking on the ☆ icon

- Azure Sentinel
- Azure Sentinel UEBA
- LogManagement
- Custom Logs
- Functions

```
1 AADServicePrincipalSignInLogs
```

Results | Chart | Columns | Add bookmark | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 48 hours. 00:00.2 | 28 records

TimeGenerated [UTC]	OperationName	OperationVersion	ServicePrincipalName	Category	ResultType	ResultSignature	Correla
10/9/2020, 7:22:31.989 AM	Sign-in activity	1.0	MTPAPI	ServicePrincipalSignInLogs	0	None	69bafd
10/9/2020, 7:22:44.659 AM	Sign-in activity	1.0	MTPAPI	ServicePrincipalSignInLogs	0	None	a41fc5
10/9/2020, 7:22:49.679 AM	Sign-in activity	1.0	MTPAPI	ServicePrincipalSignInLogs	0	None	a77e3a
10/9/2020, 7:25:59.445 AM	Sign-in activity	1.0	MTPAPI	ServicePrincipalSignInLogs	0	None	981576
10/9/2020, 7:24:03.483 AM	Sign-in activity	1.0	MTPAPI	ServicePrincipalSignInLogs	0	None	34fead
10/9/2020, 7:26:04.397 AM	Sign-in activity	1.0	MTPAPI	ServicePrincipalSignInLogs	0	None	413455
10/9/2020, 1:13:19.369 PM	Sign-in activity	1.0	LogicApp	ServicePrincipalSignInLogs	0	None	db6db
10/9/2020, 1:55:57.670 PM	Sign-in activity	1.0	MTPAPI	ServicePrincipalSignInLogs	0	None	63e67

Page 1 of 1 | 50 items per page | 1 - 28 of 28 items

https://www.verboon.info/2020/10/monitoring-service-principal-sign-ins-with-azuread-and-azure-sentinel/

Monitoring AzureAD Service Principal sign-ins

Active rules | Rule templates

API

Severity : **All** | Rule Type : **All** | Status : **All** | Tactics : **All**

SEVERITY	NAME	RULE TYPE	STATUS	TACTICS	LAST MODIFIED
Medium	Someone used my MTPAPI	Scheduled	Enabled		10/10/20, 12:41 PM

Someone used my MTPAPI

Medium
Severity

Enabled
Status

Id
7f33adcf-fee5-4118-a63a-522dff1158a2

Description
somenoe used my MTPAPI

Tactics
- Privilege Escalation
- Initial Access
- Credential Access
- Discovery

Rule query

```
AADServicePrincipalSignInLogs
| where ServicePrincipalName contains "MTPAPI"
| where IPAddress !=
| extend countryOrRegion_ = tostring(parse_json
(LocationDetails).countryOrRegion)
| extend state_ = tostring(parse_json
```

https://www.verboon.info/2020/10/monitoring-service-principal-sign-ins-with-azuread-and-azure-sentinel/

Monitoring Microsoft Defender for Endpoint deployment progress

```
DeviceInfo
| summarize arg_max(Timestamp,*) by DeviceName
| count

DeviceInfo
| where Timestamp > ago(30d)
| summarize FirstSeen =  arg_min(Timestamp,*) by DeviceId
| where FirstSeen > ago(4h)
| summarize NewClients = count() by bin(FirstSeen, 15m)
| render timechart
```

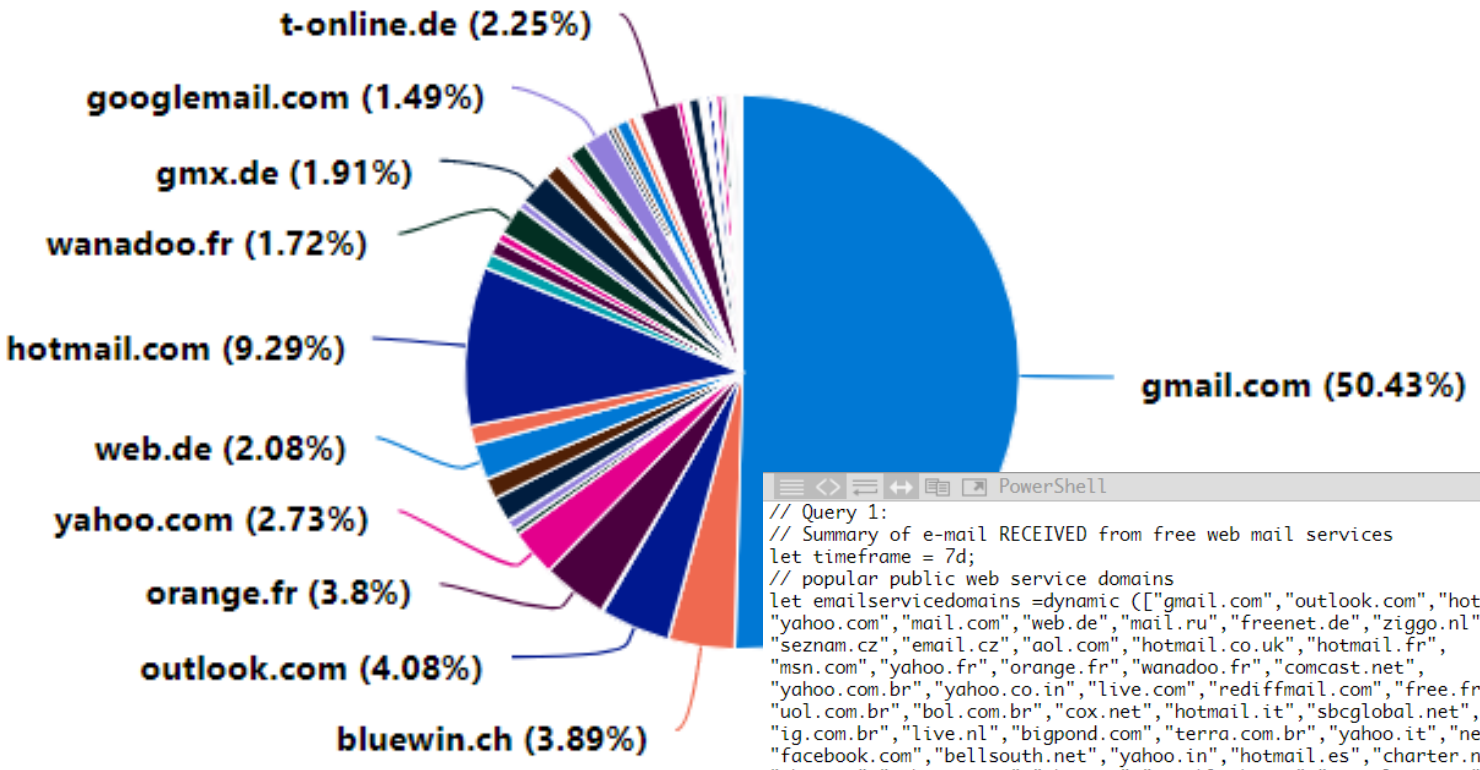
Export

Chart type

Show filters

NewClients

Monitoring e-mail traffic to and from free mail services



PowerShell

```
// Query 1:
// Summary of e-mail RECEIVED from free web mail services
let timeframe = 7d;
// popular public web service domains
let emailservicedomains =dynamic (["gmail.com","outlook.com","hotmail.com","gmx.de",
"yahoo.com","mail.com","web.de","mail.ru","freenet.de","ziggo.nl","xs4all.nl",
"seznam.cz","email.cz","aol.com","hotmail.co.uk","hotmail.fr",
"msn.com","yahoo.fr","orange.fr","wanadoo.fr","comcast.net",
"yahoo.com.br","yahoo.co.in","live.com","rediffmail.com","free.fr","yandex.ru","ymail.com","libero.it",
"uol.com.br","bol.com.br","cox.net","hotmail.it","sbcglobal.net","sfr.fr","live.fr","verizon.net","live.co.uk","googlemail.com","yahoo.es",
"ig.com.br","live.nl","bigpond.com","terra.com.br","yahoo.it","neuf.fr","yahoo.de","alice.it","rocketmail.com","att.net","laposte.net",
"facebook.com","bellsouth.net","yahoo.in","hotmail.es","charter.net","yahoo.ca","yahoo.com.au","rambler.ru","hotmail.de","tiscali.it",
"shaw.ca","yahoo.co.jp","sky.com","earthlink.net","optonline.net","freenet.de","t-online.de","aliceadsl.fr",
"virgilio.it","home.nl","qq.com","telenet.be","me.com","yahoo.com.ar","tiscali.co.uk","yahoo.com.mx","voila.fr","gmx.net",
"mail.com","planet.nl","tin.it","live.it","ntlworld.com","arcor.de","yahoo.co.id","frontiernet.net","hetnet.nl","live.com.au",
"yahoo.com.sg","zonnet.nl","club-internet.fr","juno.com","optusnet.com.au","blueyonder.co.uk","bluewin.ch","highspeed.ch",
"skynet.be","sympatico.ca","windstream.net","mac.com","centurytel.net","chello.nl","live.ca","aim.com","bigpond.net.au"
"yahoo.co.uk"]);
EmailEvents
| where Timestamp > ago (timeframe)
| extend ReceipientDomain = tostring(split(RecipientEmailAddress,"@",1)[0])
| where SenderFromDomain  in (emailservicedomains)
| summarize count() by SenderFromDomain
```

https://www.verboon.info/2020/09/mtp-advanced-hunting-public-free-e-mail-services/

KQL – In the Real world

Run | Time range : Custom | Save

```
SecurityEvent
| summarize count() by EventID
| sort by count_
```

Results | Chart | Columns | Add bookmar

Completed. Showing results from the custom time range.

EventID	count_
4'703	213'497'101
4'768	114'777'377

```
SecurityEvent
| where EventID == 4768
| summarize count() by TargetAccount
| sort by count_
```

Results | Chart | Columns | Add bookmark

Completed. Showing results from the custom time range.

TargetAccount	count_
[redacted]	103'388'648

```
SecurityEvent
| where EventID == 4768
| where TargetAccount == "[redacted]"
| summarize TotalEvents = count()  by bin(TimeGenerated,1d)
| render timechart
```

SecurityEvent

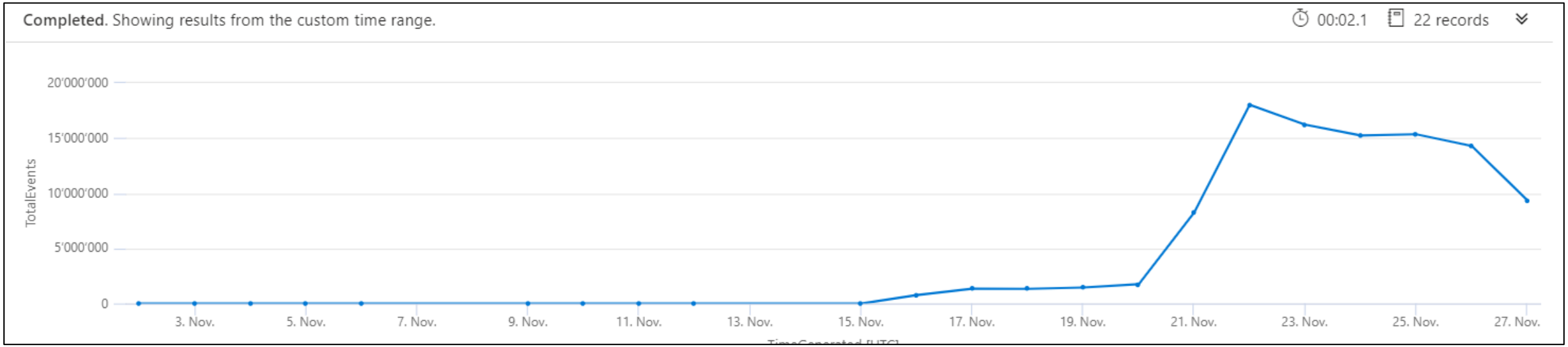
esults | Chart | Line | TimeGenerated | TotalEvents | *Split by* | Sum | Display time (UTC+00:00)

mpleted. Showing results from the custom time range. | 00:02.1 | 22 records

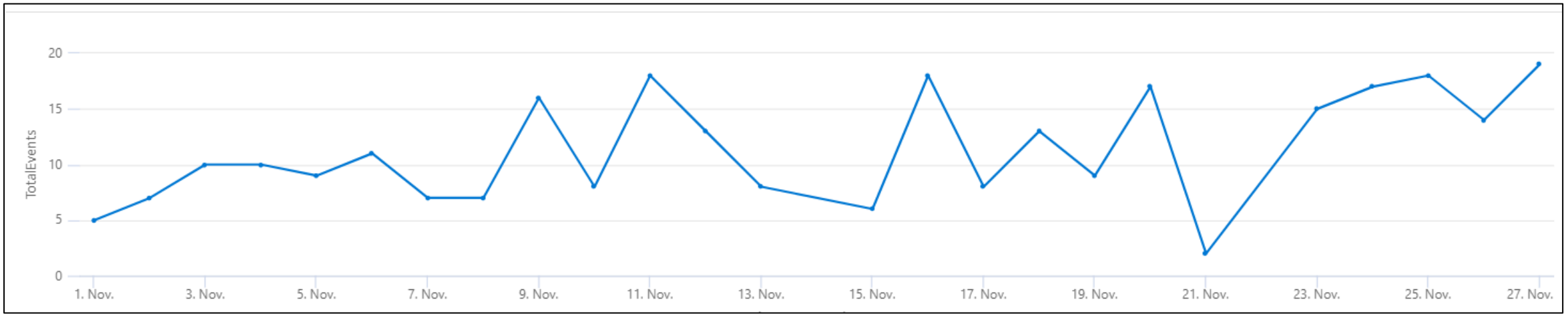
Let's find a pattern….

KQL – In the Real world

Stats from problematic account



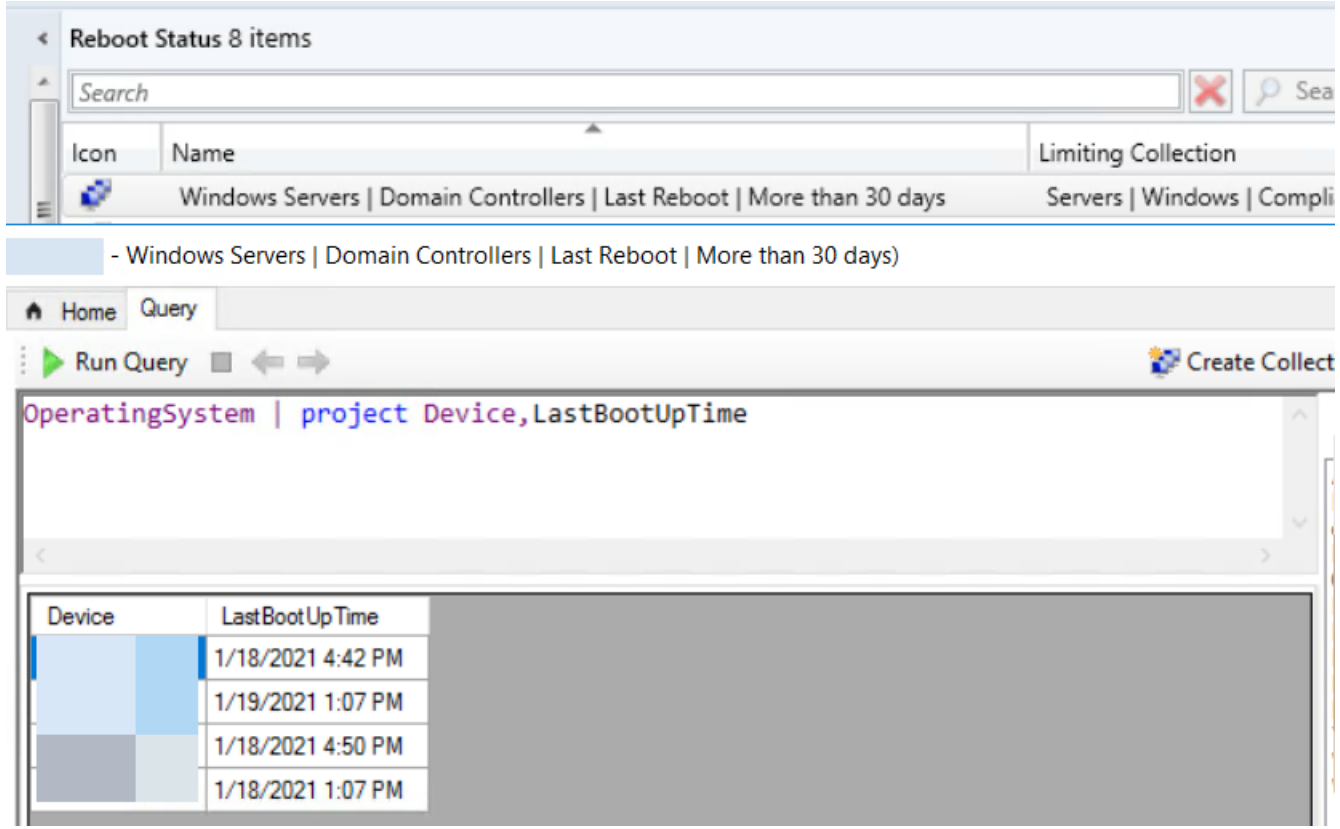
Stats from a random account



KQL – In the Real world

CMPivot provides access to **real-time** state of devices managed with Microsoft Endpoint Configuration Manager. It immediately runs a query on all currently connected devices in the target collection and returns the results.

CMPivot uses a **subset** of the Kusto Query Language (KQL).



https://docs.microsoft.com/en-us/mem/configmgr/core/servers/manage/cmpivot

Run KQL in Power Automate

Power Automate

Search for helpful resources

Home
Action items
My flows
Create
Templates
Connectors
Data
Monitor
AI Builder
Process advisor (preview)
Solutions
Learn

Defender ATP - Monthly TVM Report

Save | Flow checker | Test

Recurrence

Advanced Hunting

* Query

```
DeviceTvmSoftwareInventoryVulnerabilities
| project  DeviceName, SoftwareName, CveId, SoftwareVersion,
VulnerabilitySeverityLevel
| join (DeviceTvmSoftwareVulnerabilitiesKB
| project AffectedSoftware, VulnerabilityDescription , CveId , CvssScore ,
IsExploitAvailable
)
on CveId
| project CveId , SoftwareName , SoftwareVersion , VulnerabilityDescription ,
VulnerabilitySeverityLevel, IsExploitAvailable , CvssScore
| distinct SoftwareName , SoftwareVersion, CveId, VulnerabilityDescription ,
VulnerabilitySeverityLevel, IsExploitAvailable
| sort by SoftwareName asc , SoftwareVersion
```

Learn
Practice
Share

Learning Resources

Log Analytics Demo Environment
https://dev.loganalytics.io/
https://analytics.applicationinsights.io/demo#/discover/home

Microsoft Learn
https://docs.microsoft.com/en-us/search/?terms=KUSTO&category=Learn
https://docs.microsoft.com/en-us/search/?terms=kql&category=Learn

Best practices for queries
https://azure.microsoft.com/en-us/blog/best-practices-for-queries-used-in-log-alerts-rules/
https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/best-practices
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-best-practices?view=o365-worldwide

Kusto King Blog
https://www.kustoking.com/

Microsoft 365 Defender Hunting Queries
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries

Azure Sentinel
https://github.com/Azure/Azure-Sentinel

Pluralsight
https://www.pluralsight.com/courses/kusto-query-language-kql-from-scratch
https://www.pluralsight.com/courses/microsoft-azure-data-exploring

Other great KQL resources
https://identityandsecuritydotcom.files.wordpress.com/2020/08/kql_internals_hk.pdf
https://github.com/ashwin-patil/blue-teaming-with-kql

This slide and demo scripts
https://github.com/alexverboon/SessionPresentations/tree/main/Introduction%20into%20KQL

Thank You