

## Access Monitoring, SIEM, Audit Logs - KQL (Kusto Query Language)

By Elie M Camara

- The logs fed into monitoring infrastructure aren't worth much if one can't analyze them and get the important information hidden in all the data. To extract information or knowledge from data and understand what's happening in an environment, one needs to rely on a query language to question and request specific information from various logs and enhance detection efficacy.
- In this project, the KQL (Kusto Query Language) language will be used to work with and manipulate data in Microsoft Sentinel, in a Log Analytics demo environment (<https://aka.ms/lademo>) in the Azure portal, there is no charge to use this practice environment, but an Azure account is needed.

### Environment Overview

The screenshot shows the Microsoft Sentinel Log Analytics interface. The left sidebar contains a 'Tables' tab, a search bar, and a 'Favorites' section. The main area displays a KQL query and its results. Annotations point to various UI elements:

- Implicit time filter**: Points to the 'Time range: Last 24 hours' dropdown.
- Query window**: Points to the KQL query editor.
- Query results**: Points to the table of results.
- Tables/queries**: Points to the 'Tables' tab in the sidebar.
- Column chooser**: Points to the 'Columns' dropdown in the results view.
- Columns by type**: Points to the 'AlertName (string)' entry in the 'SecurityAlert' table.

The KQL query is:

```
1 SecurityEvent
2 | where EventID == 4624
3 | take 10
```

The results table shows the following columns: TimeGenerated [UTC], Account, AccountType, Computer, and EventSourceName. The first 10 records are displayed.

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
1/2/2022, 3:38:53.483 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC11.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:39:11.697 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC10.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:45.340 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC10.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:48.533 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC10.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:46.490 PM	NA.CONTOSOHOTELS.COM\SQ...	Machine	DC01.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:56.490 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC01.na.contosohotels....	Microsoft-Windows
2022, 3:42:23.657 PM	NA.CONTOSOHOTELS.COM\SQ...	Machine	DC01.na.contosohotels....	Microsoft-Windows
2022, 3:42:30.063 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC01.na.contosohotels....	Microsoft-Windows

LAB# 1 - Find all the security events.

SecurityEvent  
| summarize by Activity

Home >

Logs Demo

New Query 1\* x +

Time range: Last 7 days

1 SecurityEvent  
2 | summarize by Activity  
3

Results Chart

Activity

- > 4688 - A new process has been created.
- > 8002 - A process was allowed to run.
- > 4624 - An account was successfully logged on.
- > 4634 - An account was logged off.
- > 4672 - Special privileges assigned to new logon.
- > 4648 - A logon was attempted using explicit credentials.
- > 4799 - A security-enabled local group membership was enumerated.
- > 4798 - A user's local group membership was enumerated.
- > 5059 - Key migration operation.
- > 4768 - A Kerberos authentication ticket (TGT) was requested.
- > 4905 - An attempt was made to unregister a security event source.
- > 4904 - An attempt was made to register a security event source.
- > 4662 - An operation was performed on an object.
- > 8005
- > 4625 - An account failed to log on.
- > 4735 - A security-enabled local group was changed.
- > 4717 - System security access was granted to an account.
- > 4719 - System audit policy was changed.

1s 132ms | Display time (UTC+00:00)

Query details | 1 - 18 of 29

The 4-digit unique identifiers represent the events identification numbers. A unique identifier assigned to each operation that occurs in the Azure environment.

Event ID 4672 means a Special privilege has been assigned to a new logon. This event generates for new account logons if any sensitive privileges are assigned to the new logon session.

Lab# 2 - Find all the events generated for new account logons if any of the sensitive privileges are assigned to the new logon session.

SecurityEvent  
| where EventID == "4672"

Home >

Logs Demo

New Query 1\* x +

Time range: Last 24 hours

1 SecurityEvent  
2 | where EventID == "4672"

Results Chart

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task	Level
> 3/30/2023, 12:08:15.913 PM	NAIDC105	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:08:21.912 PM	NAIDC105	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:08:28.335 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:08:28.344 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:08:45.072 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:08:45.076 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:15.922 PM	NAIDC105	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:16.306 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:20.204 PM	NAIDC115	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:20.213 PM	NAIDC115	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:32.232 PM	NAIDC115	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:28.594 PM	NAIDC005	Machine	DC00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:28.606 PM	NAIDC005	Machine	DC00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:33.870 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:34.206 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8
> 3/30/2023, 12:09:34.210 PM	NAIDC015	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12548	8

10s 746ms | Display time (UTC+00:00)

Query details | 1 - 16 of 29947

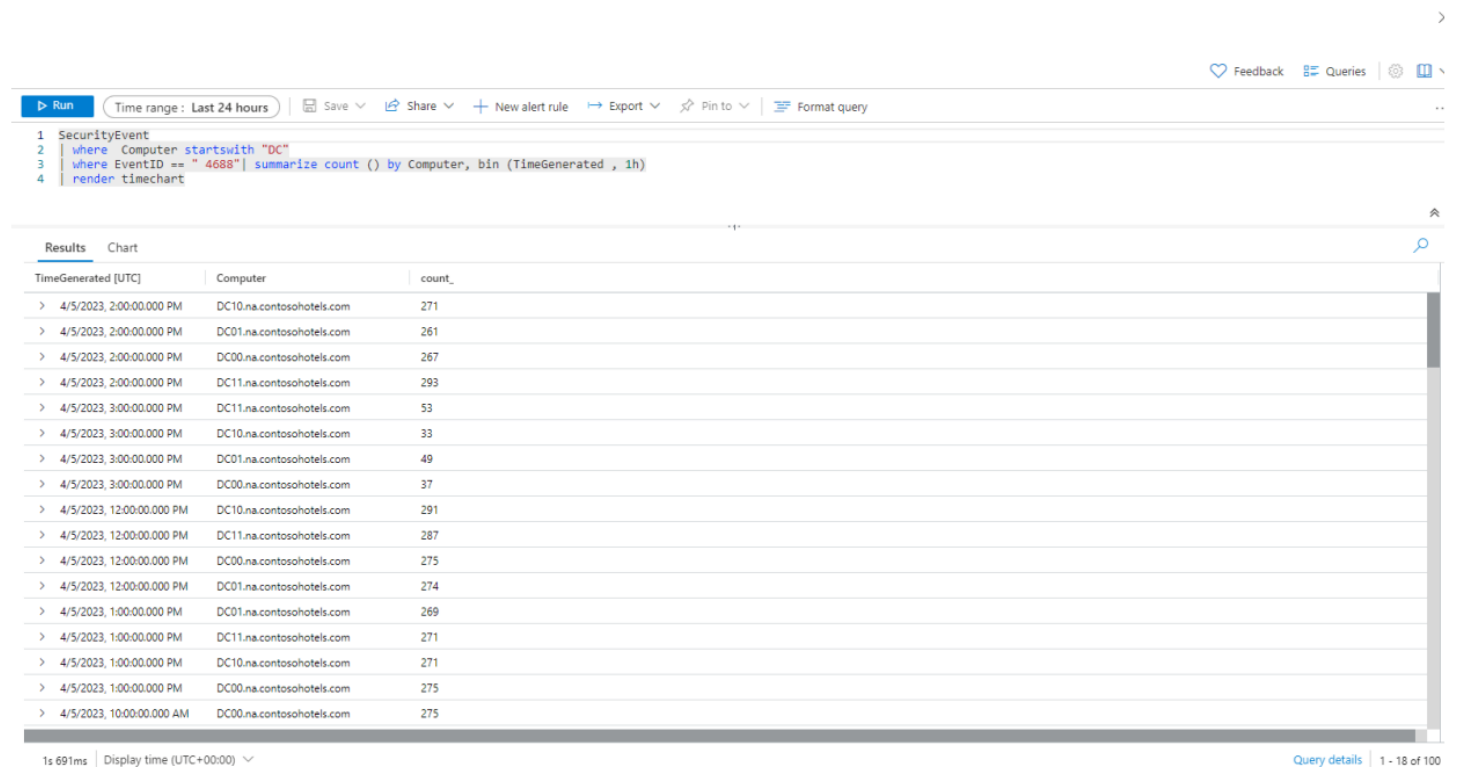
11 privileges were assigned (See Screenshot below)



Windows Security events are stored under the "SecurityEvent" table. The event ID 4624 represents the Windows Event ID that corresponds to a successful user login. It is generated when a user successfully logs on to a Windows computer or server, either locally or remotely, using a valid username and password.

#### Lab# 4 - Charting the rate of process creation on all domain controllers

```
SecurityEvent
| where Computer startswith "DC"
| where EventID == " 4688"| summarize count () by Computer, bin (TimeGenerated,
1h)
| render timechart
```



Notice that we have 4 different domain controllers: DC00.na.contosohotels.com, DC01.na.contosohotels.com, DC10.na.contosohotels.com and DC11.na.contosohotels.com

## Lab# 5 – Queries similarities and differences (Pointing out the differences between the next two queries)

### Query a

SecurityEvent

```
| summarize arg_max (TimeGenerated , *) by Account  
| where EventID == "4624"
```

Run	Time range: Last 24 hours	Save	Share	New alert rule	Export	Pin to	Format query
1	SecurityEvent						
2	summarize arg_max (TimeGenerated , *) by Account						
3	where EventID == "4624"						

Account	TimeGenerated [UTC]	AccountType	Computer	EventSourceName	Channel	Task	Level
> NA.CONTOSOHOTELS.COM\sqlcs	4/5/2023, 2:46:00.227 PM	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\sh360DB\$	4/5/2023, 2:46:01.002 PM	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\SQL00\$	4/5/2023, 3:34:35.186 PM	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\DC01\$	4/5/2023, 3:34:47.065 PM	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\APPE01\$	4/5/2023, 3:33:32.887 PM	Machine	DC00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\timadmin	4/5/2023, 3:32:35.461 PM	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\APPE00\$	4/5/2023, 3:27:19.291 PM	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA\SQLCS	4/5/2023, 3:28:13.373 PM	Machine	SQL00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\DC10\$	4/5/2023, 3:34:34.984 PM	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\DC00\$	4/5/2023, 3:34:54.127 PM	Machine	DC00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\SQL01\$	4/5/2023, 3:34:35.487 PM	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\SQL10\$	4/5/2023, 3:34:23.972 PM	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
> NA.CONTOSOHOTELS.COM\DC11\$	4/5/2023, 3:34:43.879 PM	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8

### Query b

SecurityEvent

```
| where EventID == "4624"  
| summarize arg_max (TimeGenerated , *) by Account
```

Run	Time range: Last 24 hours	Save	Share	New alert rule	Export	Pin to	Format query
1	SecurityEvent						
2	where EventID == "4624"						
3	summarize arg_max (TimeGenerated , *) by Account						

Account	TimeGenerated [UTC]	TenantId	SourceSystem	AccountType	Computer	EventSourceName	Channel
> NA\DC10\$	4/5/2023, 12:10:11.209 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\SQL00\$	4/5/2023, 3:43:46.209 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NT AUTHORITY\SYSTEM	4/5/2023, 3:43:19.666 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	RETAILVM01	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\DC01\$	4/5/2023, 3:43:47.162 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\APPE01\$	4/5/2023, 3:33:32.887 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\timadmin	4/5/2023, 3:42:18.594 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	User	DC00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\APPE00\$	4/5/2023, 3:42:19.612 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA\SQLCS	4/5/2023, 3:43:15.181 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	SQL00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\DC10\$	4/5/2023, 3:43:41.851 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\DC00\$	4/5/2023, 3:44:05.890 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC01.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\SQL01\$	4/5/2023, 3:43:29.911 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\SQL10\$	4/5/2023, 3:43:58.441 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA.CONTOSOHOTELS.COM\DC11\$	4/5/2023, 3:43:38.393 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NA\timadmin	4/5/2023, 12:57:40.940 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	User	SQL00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
> NT AUTHORITY\NETWORK SERVICE	4/5/2023, 10:23:10.375 AM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	am-temp8298ee9b	Microsoft-Windows-Security-A...	Security
> NT AUTHORITY\LOCAL SERVICE	4/5/2023, 10:23:11.671 AM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	am-temp8298ee9b	Microsoft-Windows-Security-A...	Security
> Window Manager\DWM-1	4/5/2023, 10:23:11.705 AM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	User	am-temp8298ee9b	Microsoft-Windows-Security-A...	Security
> NA\sh360DB\$	4/4/2023, 9:46:00.859 PM	81a662b5-8541-481b-977d-5d956616ac5e	OpsManager	Machine	SQL00.na.contosohotels.com	Microsoft-Windows-Security-A...	Security

1s 92ms | Display time (UTC+00:00) | Query details | 3 - 20 of 20

**Query a** retrieves all Security events, then groups them by Account and uses the arg\_max operator to find the latest event for each Account. Then, it filters the results to only include events with EventID equal to "4624".

**Query b** first filters the Security events to include only events with EventID equal to "4624". Then it groups them by Account and uses the arg\_max operator to find the latest event for each Account.

The difference between the two queries is that query a applies the filter after the retrieval of all Security events grouped by Account and the latest event for each Account, while query b applies the filter [arg\_max operator to find the latest event for each Account] to the retrieved Security events that only include events with EventID equal to "4624", grouped by Account. The order of the operations has clearly affected the performance and the accuracy of the results.

## Lab# 6 – Successful Activity event code

```
SecurityEvent
| top 10 by TimeGenerated
| extend EventCode=substring(Activity, 0, 4)
| project EventCode, Computer, AccountType, TimeGenerated, EventDetails=Activity, NewProcessName
```

The screenshot shows a Kusto query interface with a query editor and a results table. The query is:

```
SecurityEvent
| top 10 by TimeGenerated
| extend EventCode=substring(Activity, 0, 4)
| project EventCode, Computer, AccountType, TimeGenerated, EventDetails=Activity, NewProcessName
```

The results table has the following columns: EventCode, Computer, AccountType, TimeGenerated [UTC], and EventDetails. The results are sorted by TimeGenerated in descending order. The last row, with EventCode 4624, is highlighted by a blue arrow.

EventCode	Computer	AccountType	TimeGenerated [UTC]	EventDetails
> 8002	SQL01.na.contosohotels.com	User	4/6/2023, 3:35:06.310 AM	8002 - A process was allowed to run.
> 4688	SQL01.na.contosohotels.com	Machine	4/6/2023, 3:35:06.307 AM	4688 - A new process has been created.
> 8002	SQL01.na.contosohotels.com	User	4/6/2023, 3:35:06.303 AM	8002 - A process was allowed to run.
> 4688	SQL01.na.contosohotels.com	Machine	4/6/2023, 3:35:06.291 AM	4688 - A new process has been created.
> 8002	J8CIX00	User	4/6/2023, 3:35:01.928 AM	8002 - A process was allowed to run.
> 4688	J8CIX00	Machine	4/6/2023, 3:35:01.924 AM	4688 - A new process has been created.
> 4634	DC00.na.contosohotels.com	Machine	4/6/2023, 3:35:01.327 AM	4634 - An account was logged off.
> 4634	DC00.na.contosohotels.com	Machine	4/6/2023, 3:35:01.321 AM	4634 - An account was logged off.
> 4634	DC00.na.contosohotels.com	Machine	4/6/2023, 3:35:01.321 AM	4634 - An account was logged off.
> 4624	DC00.na.contosohotels.com	Machine	4/6/2023, 3:35:01.296 AM	4624 - An account was successfully logged on.

The event code 4624 for the computer DC00.na.contosohotels.com is the one from which there was a successful log on activity.