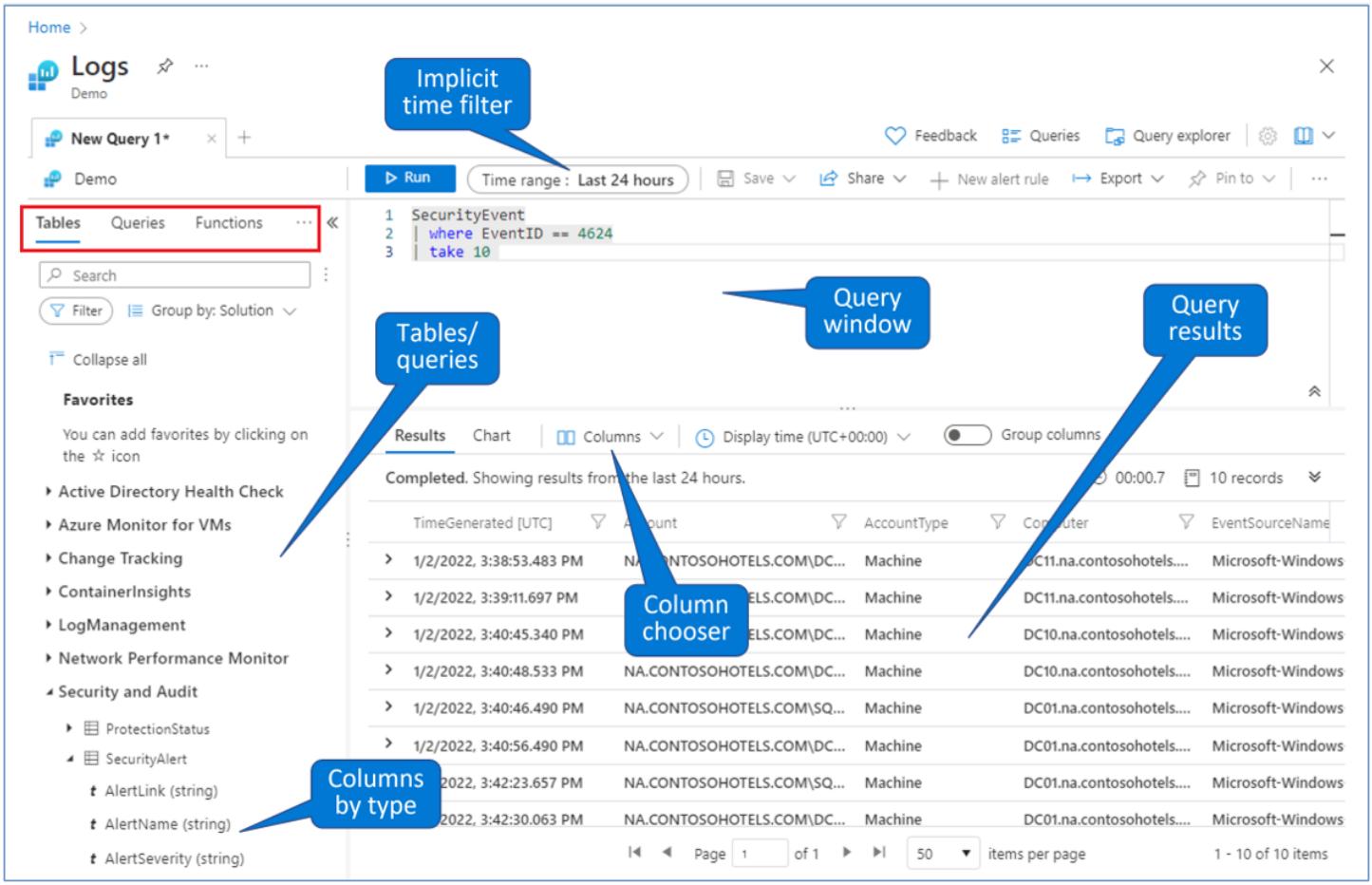
Access Monitoring, SIEM, Audit Logs - KQL (Kusto Query Language)

By Elie M Camara

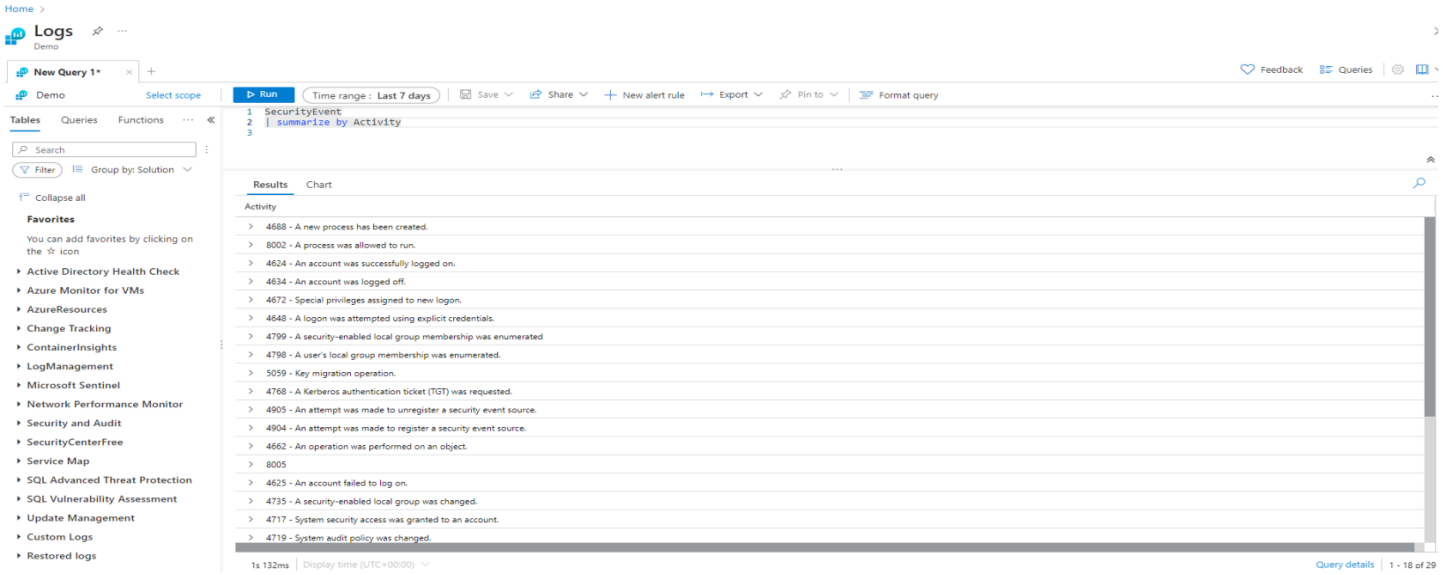
- The logs fed into monitoring infrastructure aren't worth much if one can't analyze them and get the important information hidden in all the data. To extract information or knowledge from data and understand what's happening in an environment, one needs to rely on a query language to question and request 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



LAB# 1 - Find all the security events.

```
SecurityEvent
| summarize by Activity
```

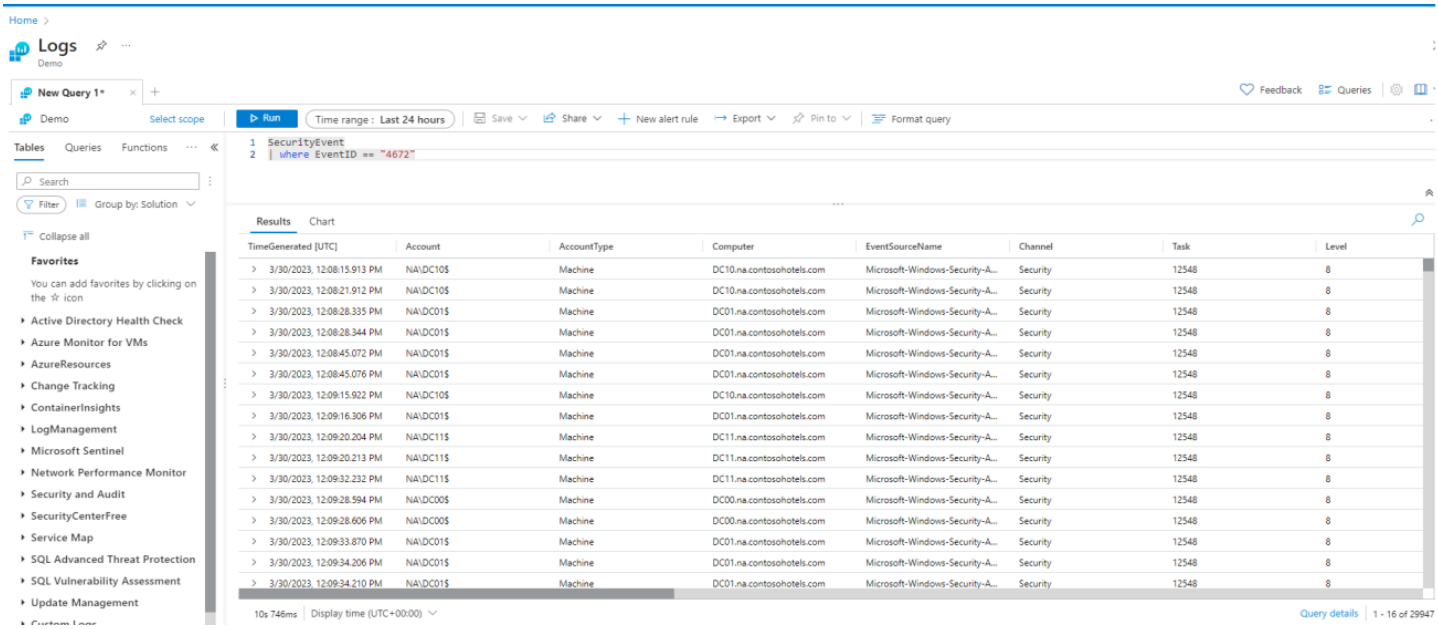


The 4-digit unique identifiers represent the events identification numbers. A unique identifier assigned to each operation that occurs in the Azure environment.

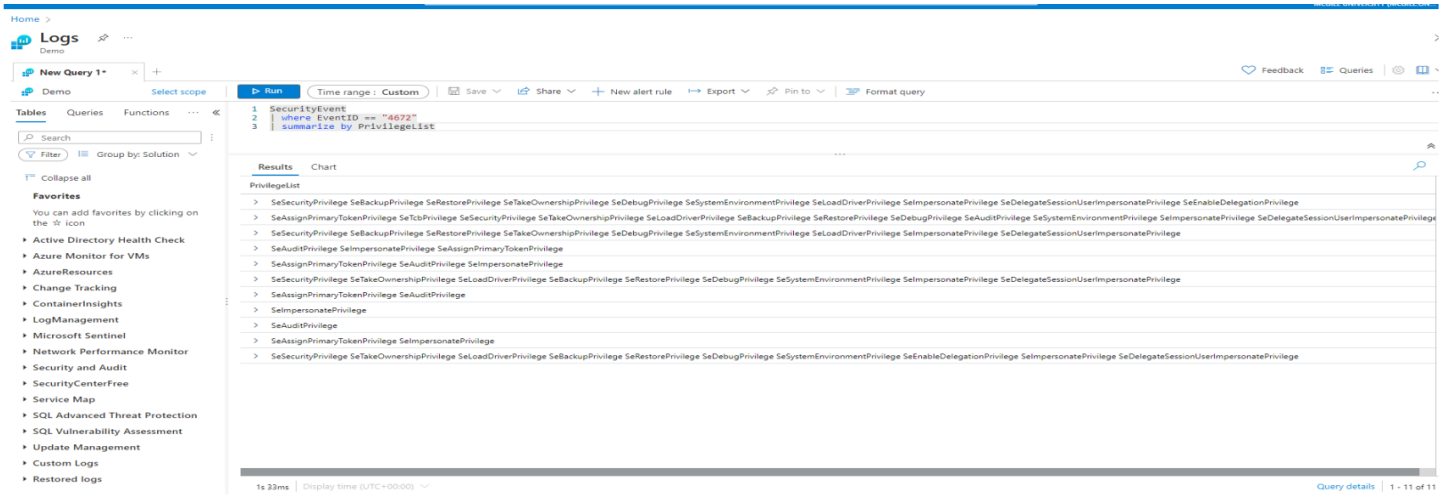
Event ID 4672 means a Special privilege has been assigned to a new logon. This event generates for new account logons if any sensitive privileges are assigned to the new logon session.

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

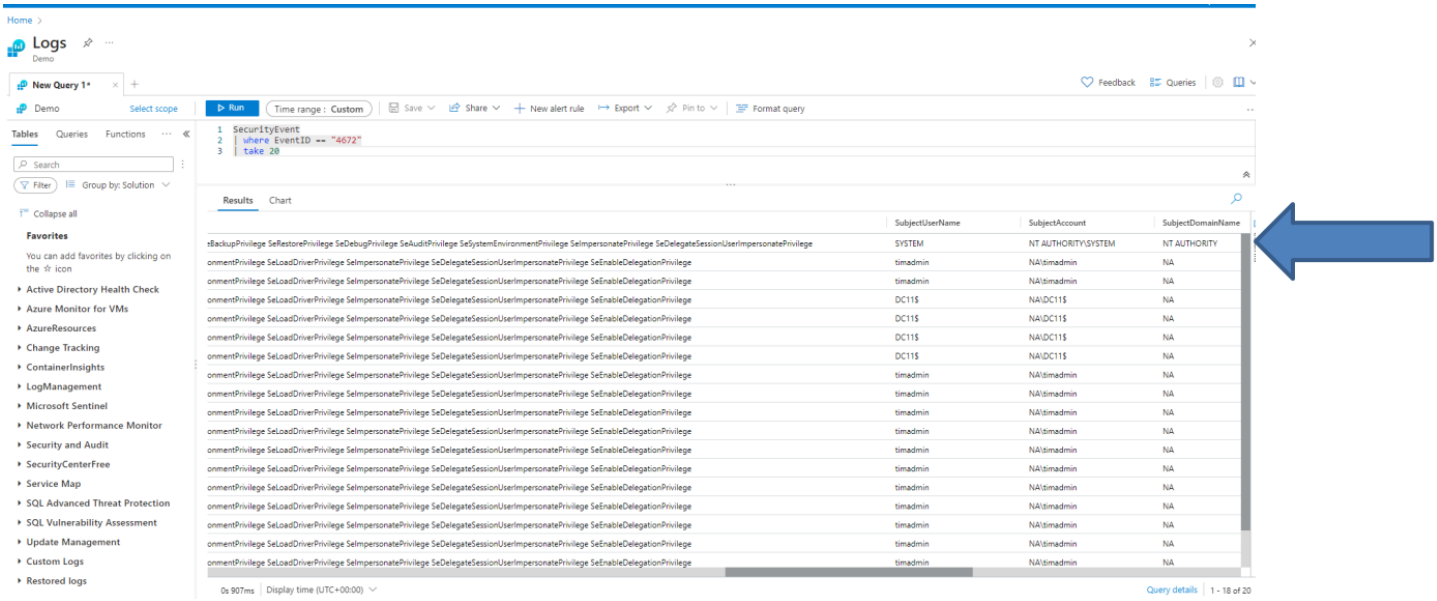
```
SecurityEvent
| where EventID == "4672"
```



11 privileges were assigned (See Screenshot below)

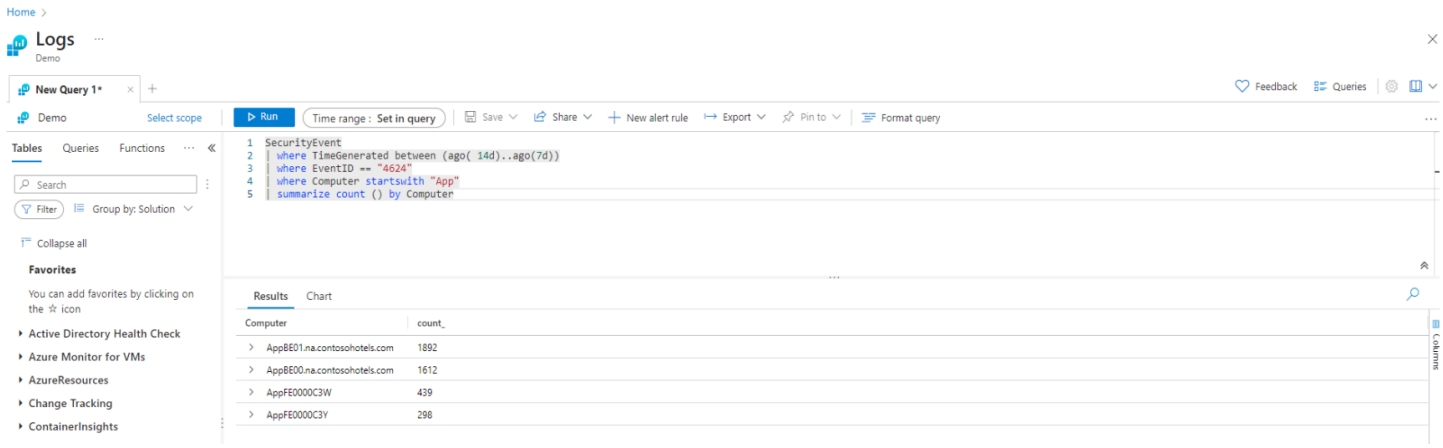


The Subject account name NT AUTHORITY\SYSTEM was assigned special privileges and the username is SYSTEM



Lab# 3 - Finding all windows logon events starting 2 weeks ago until 1 week ago that occurred on a computer with name which starts with “App”.

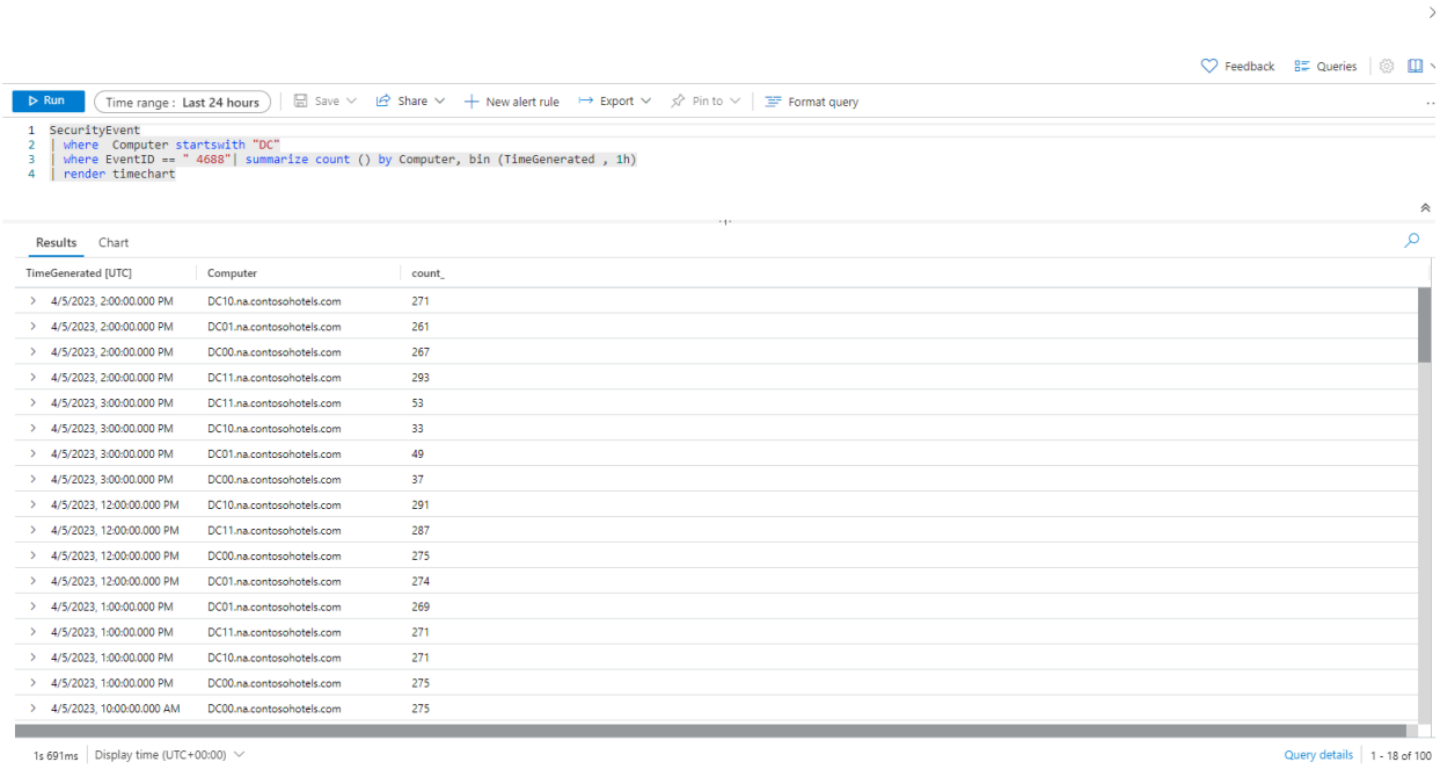
```
SecurityEvent
| where TimeGenerated between (ago( 14d)..ago(7d))
| where EventID == "4624"
| where Computer startswith "App"| summarize count () by Computer
```



Windows Security events are stored under the “SecurityEvent” table. The event ID 4624 represents the Windows Event ID that corresponds to a successful user logon. 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
```

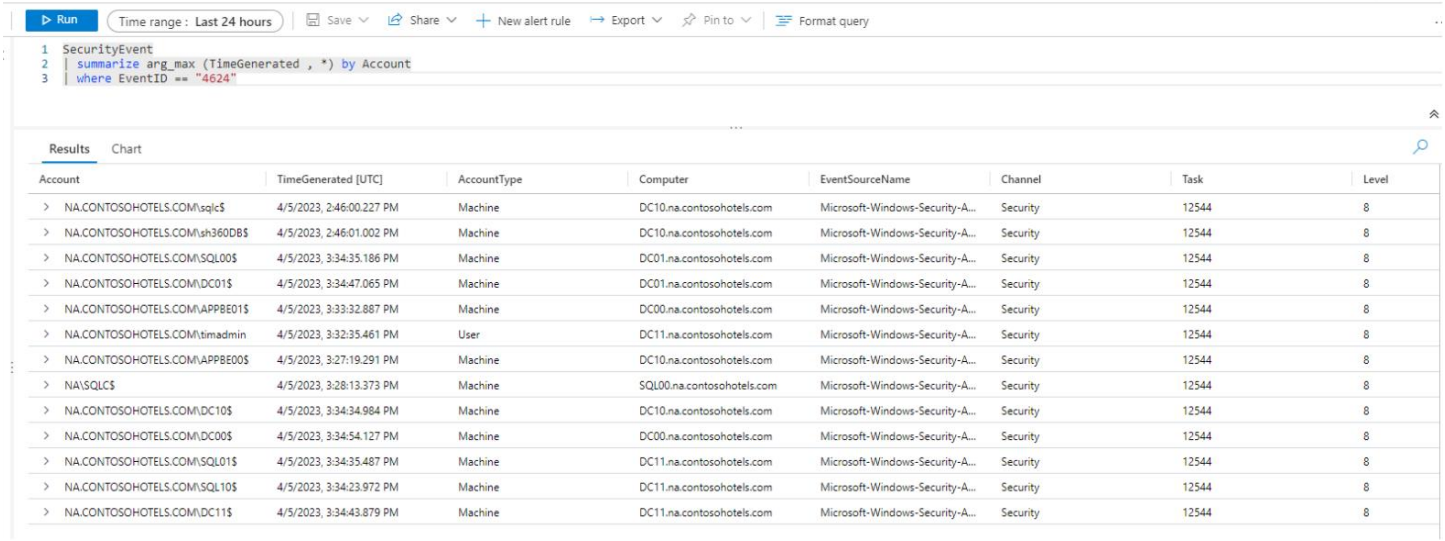


Notice that we have 4 different domain controllers: DC00.na.contosohotels.com, DC01.na.contosohotels.com, DC10.na.contosohotels.com and DC11.na.contosohotels.com

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

Query a

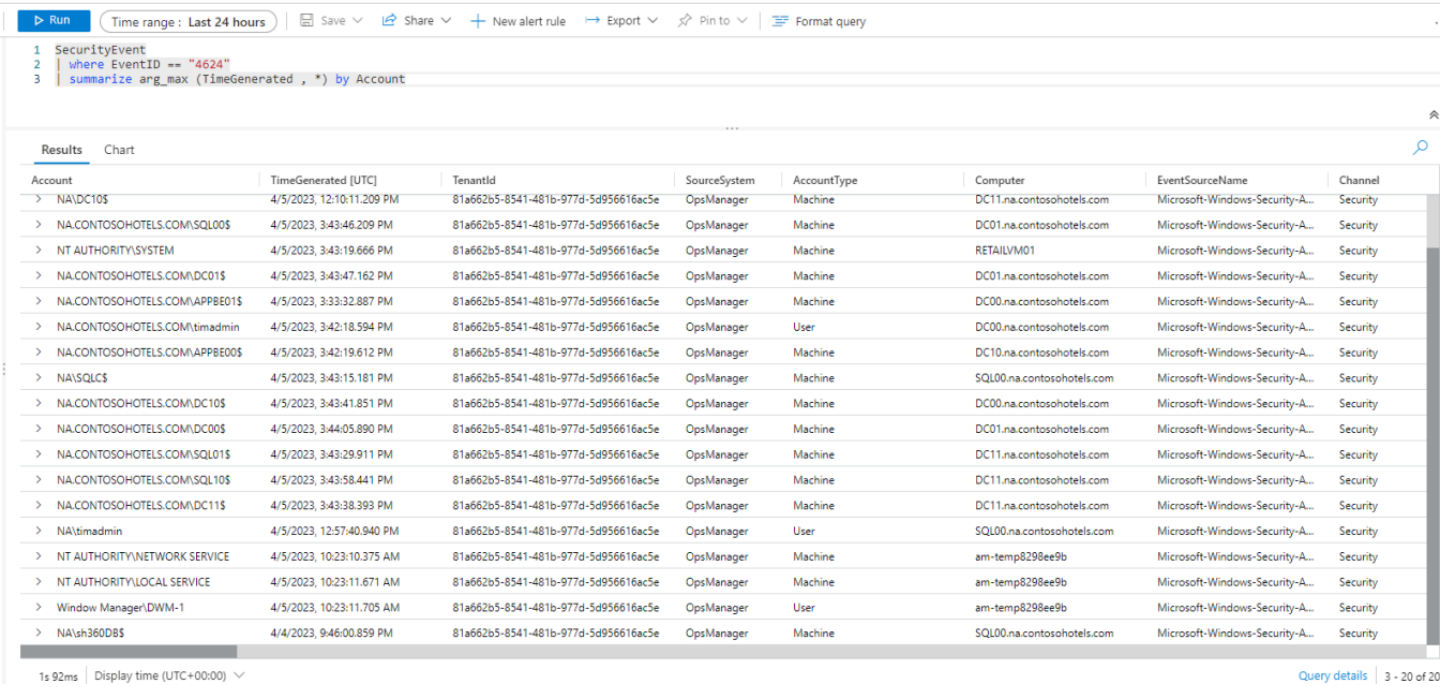
```
SecurityEvent
| summarize arg_max (TimeGenerated , *) by Account
| where EventID == "4624"
```



Account	TimeGenerated [UTC]	AccountType	Computer	EventSourceName	Channel	Task	Level
NA.CONTOSOHOTELS.COM\sqlc$	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\APPBE01$	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\APPBE00$	4/5/2023, 3:27:19.291 PM	Machine	DC10.na.contosohotels.com	Microsoft-Windows-Security-A...	Security	12544	8
NA\SQLC$	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
```



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\APPBE01$	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\APPBE00$	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\SQLC$	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

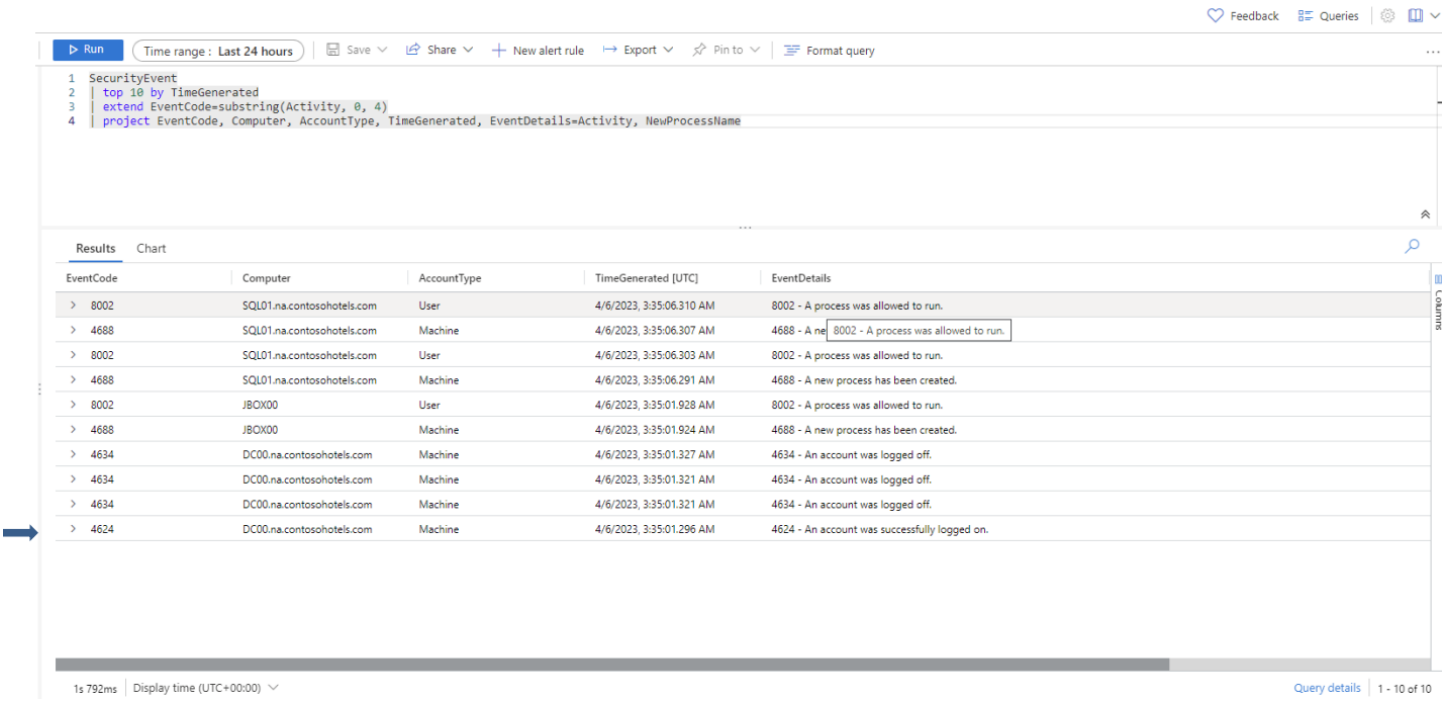
Query a retrieves all Security events, then groups them by Account and uses the arg_max operator to find the latest event for each Account. Then, it filters the results to only include events with EventID equal to "4624".

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