Extract the display name of “Suspicious granting of permissions to an account”

* **Click on Events**

Graphical user interface, text, application, email

Description automatically generated

* Click on arrow
* Highlight CorrelationId



* Open new Tab



* Paste the **Suspicious granting of permissions to an account incident response query** (see below) and **Shift + Enter** to run the query

AzureActivity

| where CorrelationId == 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx'

| project TimeGenerated, Caller, CallerIpAddress, ResourceGroup, Category, Level, OperationNameValue, Properties,ActivityStatus

* Click on the arrow



* Copy the **ResourceGroup** onto notepad (for later use)



* Click on the arrow next to **Properties**



* Click on the arrow next to **requestbody**
* Copy the **Id** onto notepad (for later use)



* Go to Azure Home page

A picture containing graphical user interface

Description automatically generated

* Search for Resource groups and select **Resource groups**Application

  Description automatically generated with low confidence
* Search for the Resource group and click on it

Graphical user interface

Description automatically generated with medium confidence

* Click on **Access Control (IAM)**



* Click on **Download Role Assignments**



* Got to Downloads to open the CSV file

Graphical user interface, application

Description automatically generated

* Split the single column into multiple columns
* Highlight row 1A to filter the Columns hen click on the down arrow



* Paste the ID in the search field and click OK

Graphical user interface, text, application

Description automatically generated

* The DisplayName of the user who was granted permission will be displayed

