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



* Click on the arrow next to **Properties**
* Copy the full entity path and paste onto notepad (for later use)



* Open PowerShell as Administrator
* Type Connect-MsolService and press Enter

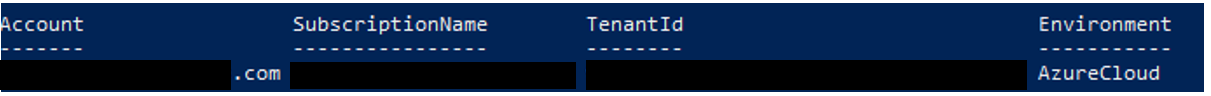


* Sign into your Microsoft account

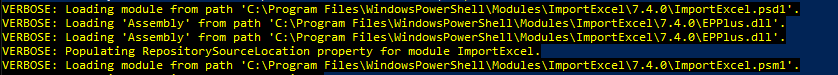
Graphical user interface, application

Description automatically generated

* Type Connect-AzureRmAccount  
  



* Type Install-Module ImportExcel -AllowClobber -Force  
  
* Type Get-Module ImportExcel -ListAvailable | Import-Module -Force -Verbose

* Type Get-AzureRmRoleAssignment -Scope /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/xxxxxxx/providers/Microsoft.Authorization/roleAssignments/ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx | Export-Excel C:\Temp\AzureRmRoleAssignment.xlsx

**Use the Entity path after -Scope**



* Go to the Temp folder to open the AzureRmRoleAssignment spreadsheet

Text

Description automatically generated

* Search for the RoleAssignementId using the entity path. Scroll to the right to view the DisplayName of the user who was granted permission will be displayed  
  