Overview:

We are building a logic app which is capable of querying Microsoft Defender ATP and retrieve Advanced Hunting and Device related risk.

Actors:

Logic app and its OOB actions. We can use the Defender APIs (Application Programming Interface) using Http, but logic app provides OOB connectors for Defender ATP.

Prerequisites:

Auth: We need a service account to query Defender ATP. (We can also use Service principal/ managed identity. Covering it is not part of this POC)

How it looks:

Graphical user interface, application

Description automatically generated

Digging In:

Let's create a logic app. Search Logic app in your azure subscription, create new as follows.  
Graphical user interface, text, application, email

Description automatically generated  
  
Now let's go into logic app and build it from scratch. The logic app starts off with a trigger, has few actions to carry out our tasks

1. **Configure the Trigger:** After creating a fresh logic app, select blank logic app. We need to create Http Trigger This can be called from any tenant using its URL.:   
   Type “Request” to see .  
   Select it. The logic app in our case expects a Json structure as input. Which looks as follows  
   {  
    “query”:”DeviceTvmSecureConfigurationAssessment | where …….”,  
    “machineName”:”machine1”  
   }  
     
   Click on ‘Use sample payload to generate schema’ in the trigger, paste the above Json.  
   Graphical user interface, text, application, email

   Description automatically generated  
     
   Select method as POST
2. Going forward in this document, click on the **+** symbol trailing the logic app box when asked to create a new action. This will add new step beneath the existing step.
3. **Have a variable handy to hold machine object:** Add a new action and search ‘variables’ => select initialize variable, configure it as follows.  
   Graphical user interface, text, application, email

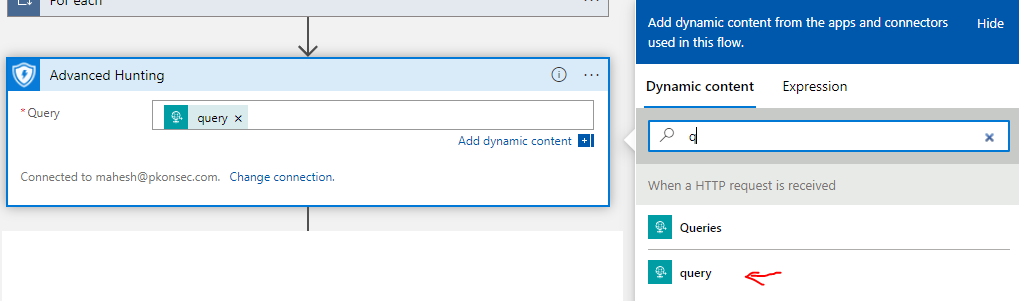
   Description automatically generated
4. **Get Machine by Name: We** have the machine name as part of input (in HttpTrigger). Let's use OOB action that is present for Defender ATP to get machine details. Add new action and search ‘Defender ATP’, select the connector.  
   Graphical user interface, text, application, email

   Description automatically generated  
     
   Authorise the connection with user who has read access to Security Center.  
   Once authorised, you can see the actions we can perform using this connector.  
   Graphical user interface, text, application

   Description automatically generated  
     
   Go through the actions and select ‘Machines- Get List Of machines’. Place the cursor in any text box to see a tool tip type wizard which has outputs from earlier actions. See below image for more info.  
     
   Graphical user interface, text, application

   Description automatically generated  
     
   We need machine name from http trigger which we can see in the Dynamic Content (popup tool tip). Configure the action as shown in above image.
5. **Get Machine Details:** As we got the machine Id from above action, it's time to get more details. Luckily, the connector “Defender ATP” has the action to get the details using machine Id. Add an action to above step, type ‘Defender’ and select ‘Machines – Get single machine’ this time from the actions listing.  
   This action expects machineId to get full details of the machine. The earlier action (Machines - Get List of Machines) gave us the id that we need.   
   In order to pass it, click in the text box, select ‘Machine Id’ from ‘Dynamic content’ as shown below  
   Graphical user interface, text, application

   Description automatically generated
6. **Store the machine retrieved into variable:** Lets store theoutput of above action into variable ‘machine**’** that we have created earlier. Add an action, type variable, and select ‘Set Variable’.  
   Click on the Name dropdown and select ‘machine’.  
   Click on Value textbox. This will open the Dynamic content where we can select the machine entity from earlier actions.  
   Graphical user interface, application

   Description automatically generated  
     
   The output of above data is complete info about the machine.
7. **Use Advanced Hunting to run query:** Add an action and type in ‘Defender’. Select Defender ATP connector and select ‘Advanced Hunting ‘from dropdown. We have the query in the outputs of ‘HttpTrigger’ . We need to use it in this action to run the same in defender’s Advanced Hunting.   
     
   
8. **Putting everything together and send response:** Now we have output Advanced hunting and the machine details. We need to combine them and send as response.  
   Add an action => type response, select . We can use ‘Dynamic Content’ to select the Advanced hunting output and machine variable to add them to response as follows.  
     
   Graphical user interface, text, application

   Description automatically generated
9. **Save the logic app and pick up the URL from trigger:** Click on save. Once saved, the trigger action will display a URL to which the Json need to be posted.  
   Graphical user interface, text, application, email

   Description automatically generated  
     
   Copy it and test it from any rest client. Check the run history in overview section of logic app.  
     
   Graphical user interface, application

   Description automatically generated