# Provision a Dataverse Table in Teams

1. Navigate to <https://teams.microsoft.com> and login with provided credentials.
2. When prompted proceed with the **web client.**

Graphical user interface, application, Teams

Description automatically generated

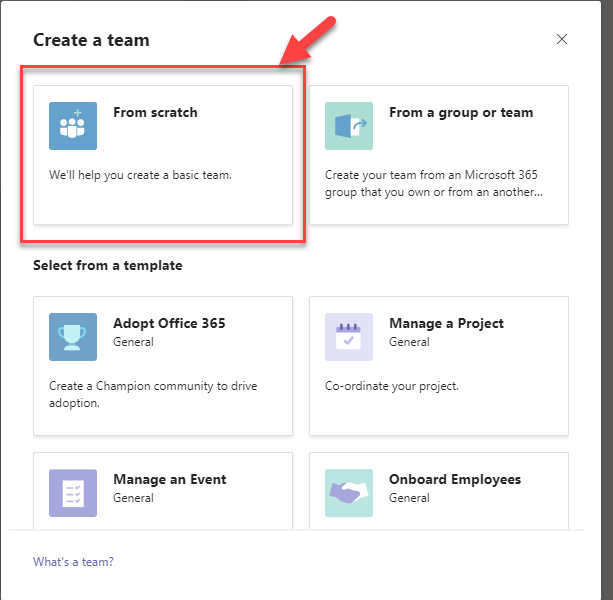
1. We’re going to create a Power App in order to provision a Table within Microsoft Dataverse. This table will be used to store persistent data related to the alerts that appear in Microsoft Defender ATP.
2. First step is to create a new Team (if using an existing Team, skip to step 7) – via the Teams blade, click on Join or create a team

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, Teams

Description automatically generated



1. Make the team private:

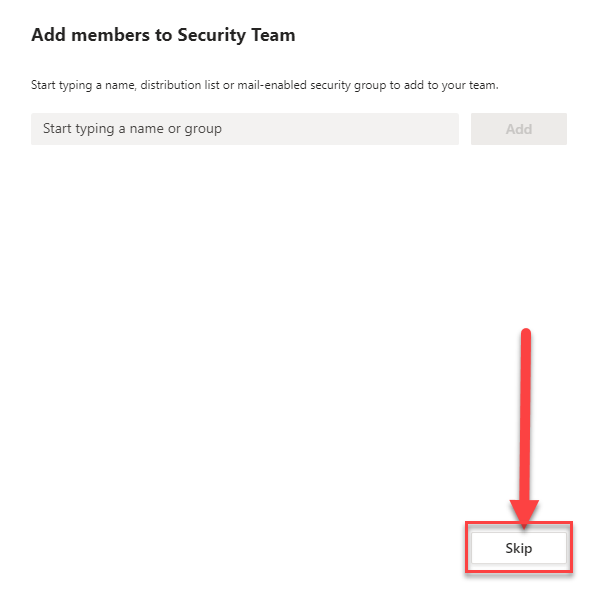
Graphical user interface, application

Description automatically generated

1. Give it a name, e.g. Security Team and then click on Create.

Graphical user interface, application, Teams

Description automatically generated



1. On the Team left hand menu, click on the … to bring up the apps blade:

Graphical user interface, application, Teams

Description automatically generated

1. Perform a search for Power Apps.

Graphical user interface, application, Teams

Description automatically generated

1. Click on Power Apps – click Add if prompted (depends if already added to Teams).
2. On the Power Apps blade – click on Create an App.

Graphical user interface, application, Teams

Description automatically generated

1. On the Create an app dialog – use the drop down to select the Team created in step 6.

Graphical user interface, application, Teams

Description automatically generated

1. Once done, click on Create.

Graphical user interface, application, Teams

Description automatically generated

1. The App will now be provisioned. A Dataverse Environment (that will contain your Dataverse Table and Power Automate Flows) is now being created.
2. Once completed – you will be asked to name your app:

Graphical user interface, application, PowerPoint

Description automatically generated

1. Provide a name for the App, e.g. MD Alerts. Click on Save.

Graphical user interface, text, application, email

Description automatically generated

1. Once done, click on Create new table:

Graphical user interface, application, Word

Description automatically generated

1. Provide a name for the table, e.g. table\_alert. Click Create when done.
2. You will now be presented with an empty table – we’ll use this to store the alerts received from Defender for Endpoint.

Graphical user interface, application

Description automatically generated

1. We need to rename the Name column to something more useful. Click the down arrow next to Name – and click on Edit column.

Graphical user interface, text, application

Description automatically generated

1. Rename it to ID – this will hold the unique alert ID. Click Save when done.
2. Click on Close in the bottom right corner.
3. Now click on Save -> and then click on Publish to Teams.

Graphical user interface, application

Description automatically generated

1. On the Add to channel dialog -> click on the + alongside General.

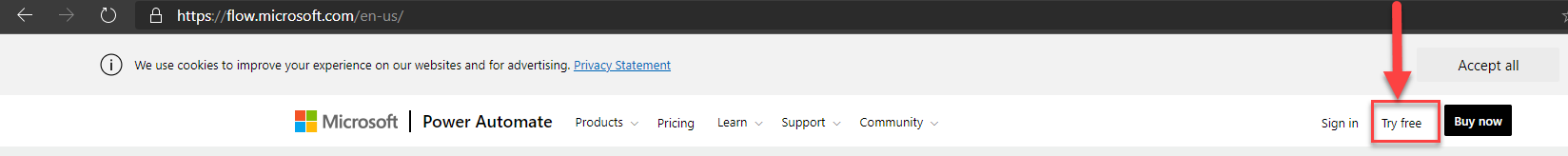
A picture containing rectangle

Description automatically generated

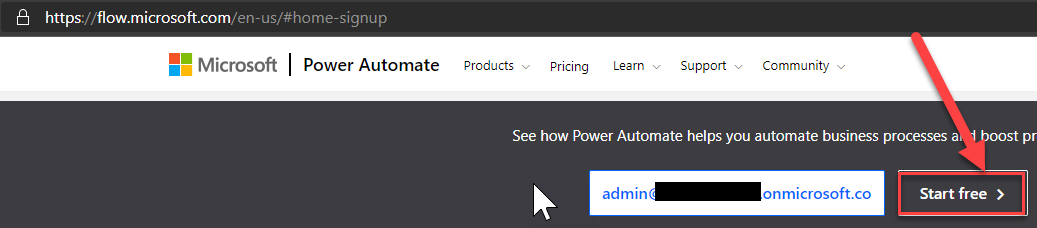
1. Then click on Save and close.

# Create a flow with the Defender for Endpoint Connector

1. Navigate to <https://flow.microsoft.com> – login using provided credentials
2. If you do not have a licence – follow steps 3 - 5 below if not skip to step 5
3. ONLY COMPLETE IF YOU DO NOT HAVE A FLOW LICENCE. Select the “Try Free” option



1. Enter your admin account and Click “Start Free” option



1. If asked to sign in please do so then you will redirected to the flow page below:

Graphical user interface, application

Description automatically generated

1. Make sure your environment is selected. If not, click on Environments and select the Team you created at the start.

Graphical user interface, application

Description automatically generated

1. Select My flows from the left hand menu.

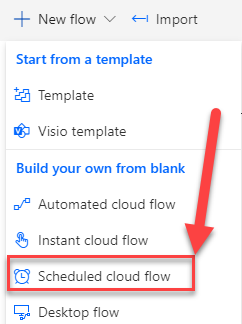
Graphical user interface, text, application

Description automatically generated

1. On the My flows screen – click on New and select + Scheduled – from blank (older tenants) or if you have a (updated tenant) choose New – Scheduled cloud Flow

Graphical user interface, application

Description automatically generated



1. On the Build a scheduled flow dialog – provide a name, e.g. New alerts flow
2. Adjust the schedule for the flow to run every hour.

Graphical user interface, application

Description automatically generated

1. Click on Create.
2. You will now arrive in the flow editor screen. Click on + New Step.

Graphical user interface, application, Teams

Description automatically generated

1. In the search bar – type Defender, scroll down the Actions and select Alerts – Get list of alerts (Premium).

Graphical user interface, text, application

Description automatically generated

1. Note – The Microsoft Defender connector is a Premium connector and requires a Power Automate Premium license. if this is the first time creating a flow using a Premium connector in this tenant, you may be prompted to start a new trial of Power Automate Premium. If doing this in a demo environment and you are authorised, click on Start trial to receive a free 30-day trial.
2. If required – Sign into Defender for Endpoint following the on-screen prompt and consent on behalf of your organisation to the required permissions.
3. Once completed – click on Show advanced options.

Graphical user interface, text, application, email

Description automatically generated

1. In the Returns first results field – type 10.

Graphical user interface, text, application, email

Description automatically generated

1. This will return the most recent 10 alerts from Defender for Endpoint.
2. To check this is working – you can save the flow and run a quick test.

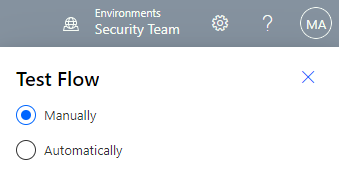
Graphical user interface, application

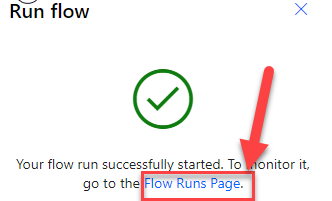
Description automatically generated

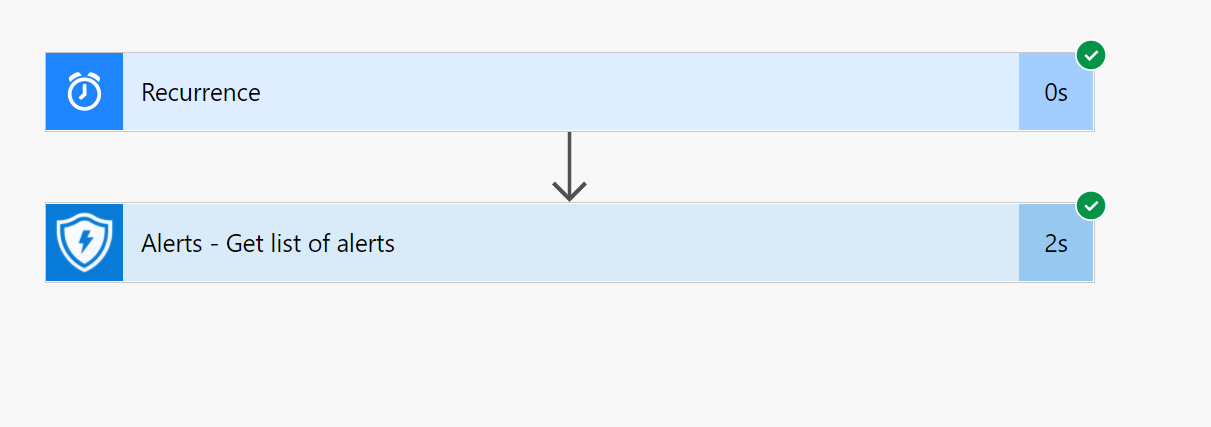
1. Click on Test – Click on I’ll perform the trigger action and click on Test

Graphical user interface, application

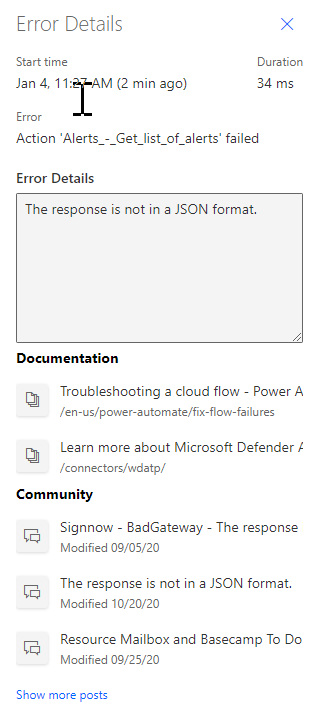
Description automatically generated (Old Tenant)

 (New Tenants)

1. Click on Run flow – you should’ve received a message on-screen with a green tick stating your flow run successfully started. Select the Flow Runs Page to see how this is working
2. – click done. If all is well you will green ticks against each step.



1. If you receive errors, you will need to drill into the step to learn why the step failed.
2. Expand the Alerts – Get list of alerts step and review the Outputs. **Assuming there are active alerts in Defender for Endpoint you should see a JSON output** showing the top 10 alerts in the tenant. You can scroll down to view the details. (The Error below occurs because the demo tenant has no alerts). If this occurs setup your environment to have a machine and



1. We have now confirmed that we can pull in Defender for Endpoint data into a flow and can now build out what we want to do with the data.

# Build out the Flow

1. Still within the flow environment – click on Edit in the top right corner.

A picture containing graphical user interface

Description automatically generated



1. Click on + New step.
2. Now we will create an array to store the alerts – this way we can store them, and then compare to ensure we only ever notify on new alerts.
3. In the Choose an action box – type variable in the search bar and select Initialize variable:

Graphical user interface, text, application, email

Description automatically generated

1. Change the type to Array and provide a name, e.g. Array\_Alerts -> We actually want this to be initialized prior to grabbing the Alerts -> so click on the Initialize variable box and drag it above the Alerts – Get list of alerts box.

Graphical user interface, application

Description automatically generated

1. Click on + New step – in the search bar type variable -> from the list select Append to array variable.

Graphical user interface, application

Description automatically generated

1. From the Name drop down – select your array name from step 5. In the Value -> select Alert Alert ID from the Dynamic content list. Graphical user interface, application

   Description automatically generated
2. Click Save.
3. We can now check that the alerts are being successfully stored in the Array that we have created.
4. Click on + New step.
5. In the search bar type compose – click on Compose in the Actions window.

Graphical user interface, text, application

Description automatically generated

1. Within the Inputs field of the Compose action – select the Array that we have created from the list of Dynamic content.

Graphical user interface, application

Description automatically generated

1. Then click on Save and Test the flow again to confirm the Array gets populated with the alerts. You should see data with the Compose action:

Graphical user interface, text, application

Description automatically generated

1. Click on Edit.
2. Now that we have the new Alerts in an Array we need to create another Array so we can run a comparison to ensure we’re only notifying on new Alerts.
3. Click on + New Step and perform a search on variable. Click on Initialize variable – set the Type to Array and provide a name, e.g. Dataverse\_AlertIDs.

A picture containing application

Description automatically generated

1. Click on + New Step and perform a search on Common Data Service. Click on Common Data Service (current environment) and click on List records within the actions list.

Graphical user interface, text, application

Description automatically generated

1. Within the Entity name drop down – search for the Common Data Service entity you created in step 17 of Part 1.

Graphical user interface, application

Description automatically generated

A picture containing application

Description automatically generated

1. Click on Save – Ignore the warning; this is because we don’t specify a filter, however we don’t need it here as we know the size of the dataset. For large datasets a filter would be required to ensure the flow is efficient.
2. Click on + New step.
3. Search on variable – select Append to array variable. From the name drop down box select the Array we created in step 16. Select the value field and then select ID from the list of Dynamic content.

Graphical user interface, application

Description automatically generated

1. Click on + New step.
2. Search for and select Compose. Within the Inputs box select the Dataverse Array.

Graphical user interface, application, Teams

Description automatically generated

1. Now that we have two arrays initialized we need to run a comparison of the IDs.
2. To compare the array values, we must loop through each entry and compare against the list of alert IDs we have already collected.
3. Click on + New step.
4. Perform a search for apply to each and select Apply to each from the Actions list.

Graphical user interface, application, email

Description automatically generated

1. Within the select an output box – select the Alerts\_Array from the list of Dynamic Content (we created this in Step 5 Part 2).
2. Within the Apply to each action box – click on Add an action.

Graphical user interface, application

Description automatically generated

1. Perform a search on condition and select Condition Control from the list of Actions.

Graphical user interface, application

Description automatically generated

1. Click on Save.
2. Return to the Condition and expand by clicking on it.
3. Within the Condition action – In the left hand value select the Dataverse Array we created in step 16 – change to the middle drop down box to Contains – and then in the right hand value click on Expression and scroll down for Item() and click OK.

Graphical user interface, application

Description automatically generated

1. So we now have a comparison for the Condition – if there is a match, then we have seen that alert before and therefore we don’t need to do anything – therefore leave the If yes section blank.
2. If there is a new Alert the Condition will not find a match and thus we must edit the If no Action. Within the If no action box, click on Add and action.

Graphical user interface, text, application

Description automatically generated

1. In the Choose an action dialog – select Common Data Service (this environment) and click on Create a new record from the list of Actions.
2. Within the Entity name – we must select the Common Data Service entity we created at the start, e.g. table\_alerts.
3. Within the ID box select the item() expression.

Graphical user interface, text, application

Description automatically generated

1. This will write each new alert to the table – this allows us to pull in the previously seen alerts every time the flow runs and perform the comparison against the alerts pulled from Defender for Endpoint. If you recall step 21 above – we pull in all of the values stored in the table\_alerts CDS entity and store in an array. We then compare each new alert pull from Defender for Endpoint against the entries in this array to see if we have/have not seen them before.
2. Save the flow.

# Send notifications to Teams

1. Under the existing If no part of the condition – click on Add an action.
2. For us to post details of the alert, other than just the Alert ID, we must pull in the additional details of the Alert from Defender for Endpoint.
3. In the Choose an action dialog box – search for Defender. From the list of Actions – select Alerts – Get single alert.

Graphical user interface, application

Description automatically generated

1. Within the ID of the alert box – add the Expression item(). This will pull the details of the alert based on the Alert ID we have.

A picture containing table

Description automatically generated

1. Now we can post a message to Teams.
2. Add an action under the previous action.
3. In the search box type Teams – click on Microsoft Teams. Within the list of Actions – select Post a message as the Flow bot to a user.

Graphical user interface, text, application

Description automatically generated

1. In the Recipient box use your credentials (send notification to yourself).
2. In the Message box – type:

Alert details:

Description - <add Alert Description from Dynamic Content>

Severity - <add Alert Alert severity from Dynamic Content>

1. In the Headline box – add Alert Title from Dynamic content.

Graphical user interface, text, application

Description automatically generated

1. Save the flow and test.
2. Go to Teams and review the new chat messages received.

Graphical user interface, text, application

Description automatically generated

1. You should have messages reporting alerts from Defender for Endpoint.
2. If you find the test did not successfully send messages it may be because you tested it earlier and wrote the alerts to the Dataverse entity. You can remove these records manually by navigating to teams.microsoft.com. Navigate to Power Apps and click on the Power App you created at the start.

Graphical user interface, application

Description automatically generated

1. Click on the ellipses and click on edit data.

Graphical user interface, application

Description automatically generated

1. Delete the table records to reset the seen Alerts.

Graphical user interface, text, application

Description automatically generated

1. Once emptied you can run the test again.

The flow will now automatically run every hour and report on any new alerts.

------ extra steps – add an Adaptive card. TBD -----------

Lab Complete.