

DEFENDER MASTERCLASS LAB

Power Automate Integration with Microsoft
Defender for Endpoint

ABSTRACT

This lab document contains a step-by-step guide to create a Teams Adaptive card when a new Alert is generated by Microsoft Defender for Endpoint.

Jack Lewis

Written for Microsoft Defender Masterclass Series – a series of events for Microsoft Partners created by James Graham

Getting Started

Please ensure you have completed the lab prerequisites:

<https://github.com/JamesGrahamMSFT/DefenderMasterclass1/blob/main/Labs%20-%20Getting%20started.pdf>

The getting started guide provides step by step instructions to create a demo tenant. You can then use this demo tenant to complete this lab.

Create a workflow that notifies you in Teams when a new Defender Alert appears

Overview:

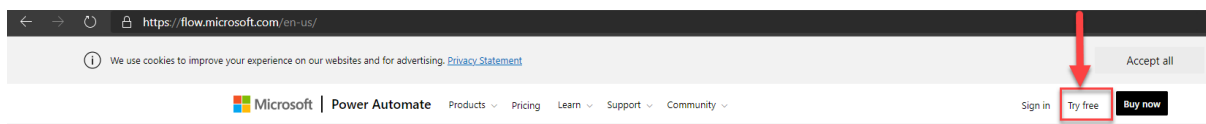
This lab will walk you through the process of creating a Power Automate Flow that notifies you when a new alert appears in your Microsoft Defender tenant, and then allows you, via the Adaptive Cards in Teams, to assign the alert, isolate the machine, or view more information about the alert.

Lab Steps:

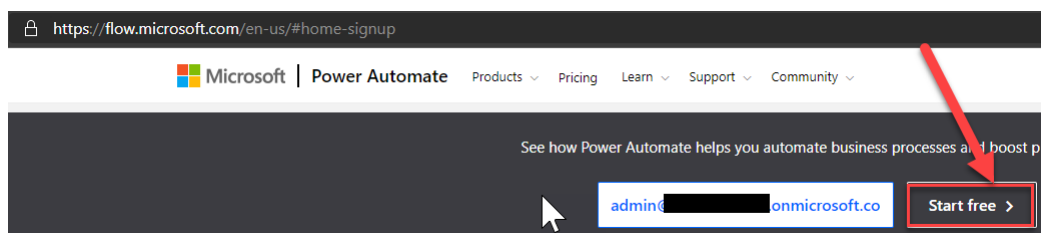
1) Create a flow with the Defender for Endpoint Connector

In this initial step we will create a Power Automate Cloud Flow that will run every time an alert is added into Microsoft Defender for Endpoint.

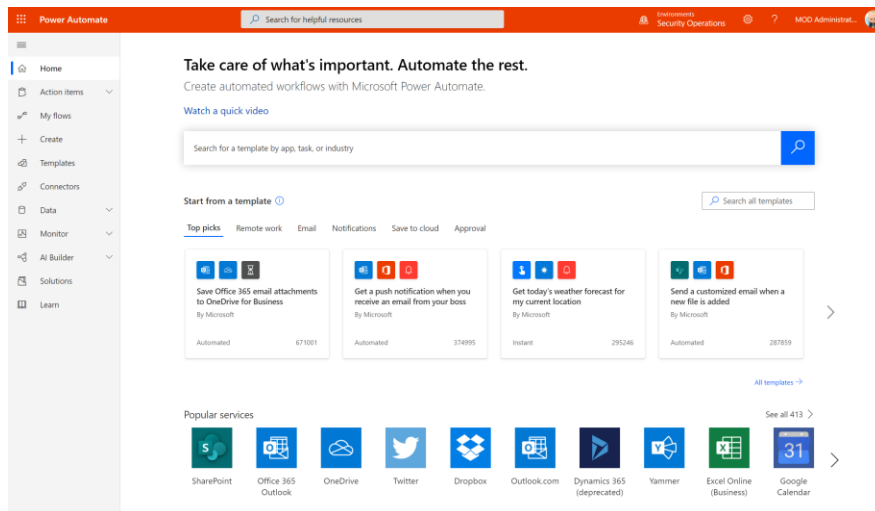
1. Navigate to <https://flow.microsoft.com> – login using your tenant credentials.
2. If you do not have a licence – follow steps 3 - 5 below if not skip to step 5 – if you're not sure, just skip to Step 6.
3. ONLY COMPLETE IF YOU DO NOT HAVE A FLOW LICENCE. Select the “Try Free” option



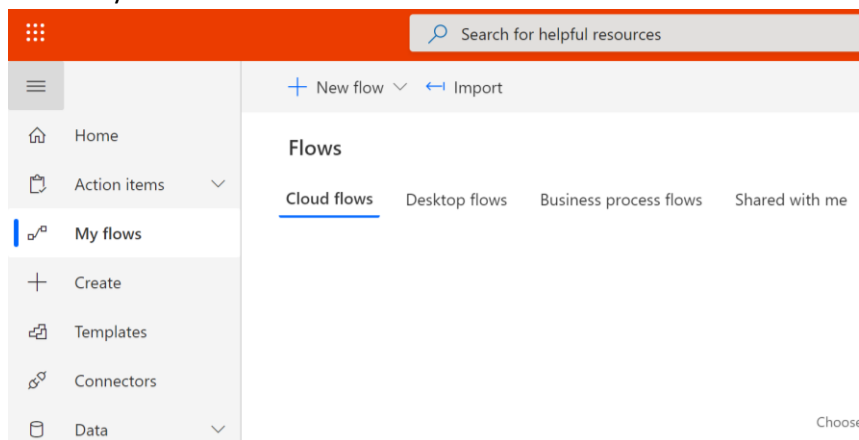
4. Enter your admin account and Click “Start Free” option



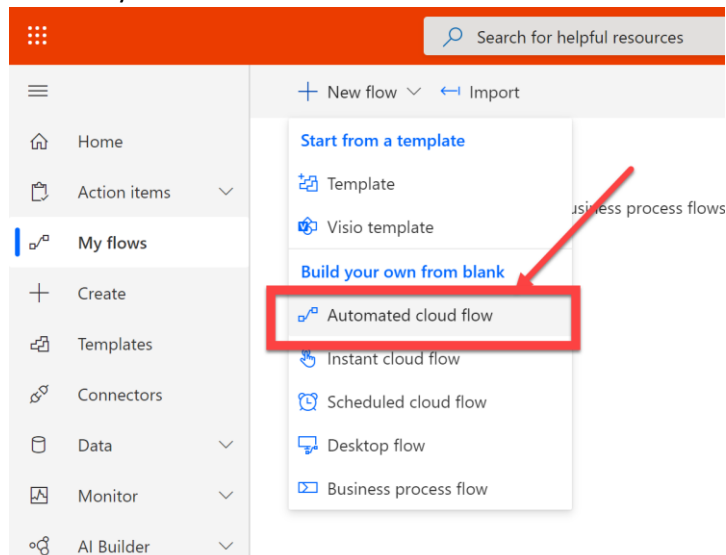
5. If asked to sign in please do so then you will be redirected to the flow page below:



6. Select My flows from the left hand menu.



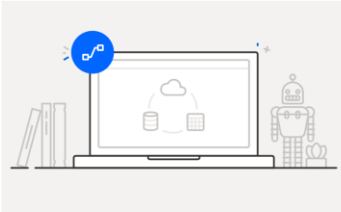
7. On the My flows screen – click on New and select Automated cloud flow



8. On the Build an automated cloud flow dialog –

- provide a name, e.g., Microsoft Defender for Endpoint – Alert – Notify Teams.
- In the 'Choose your flow's trigger' input, enter 'WDATP' and then select the Microsoft Defender ATP Trigger (Trigger when new WDATP Alert occurs).
- Select Create

Build an automated cloud flow



Free yourself from repetitive work just by connecting the apps you already use—automate alerts, reports, and other tasks.

Examples:

- Automatically collect and store data in business solutions
- Generate reports via custom queries on your SQL database

1 Flow name
Microsoft Defender for Endpoint - Alert - Notify Teams

2 Choose your flow's trigger *
WDATP

3 Triggers - Trigger when new WDATP al...
Microsoft Defender ATP

4

Skip Create Cancel

9. Click Sign in

Microsoft Defender ATP

Sign in to create a connection to Microsoft Defender ATP.

Sign in

Connect with Service Principal

10. Sign in with your Microsoft Defender administrator account

Sign in to your account - [Guest] - Microsoft Edge

https://login.microsoftonline.com/common/oauth2/authorize...

Microsoft

Pick an account

Jack Lewis
Signed in

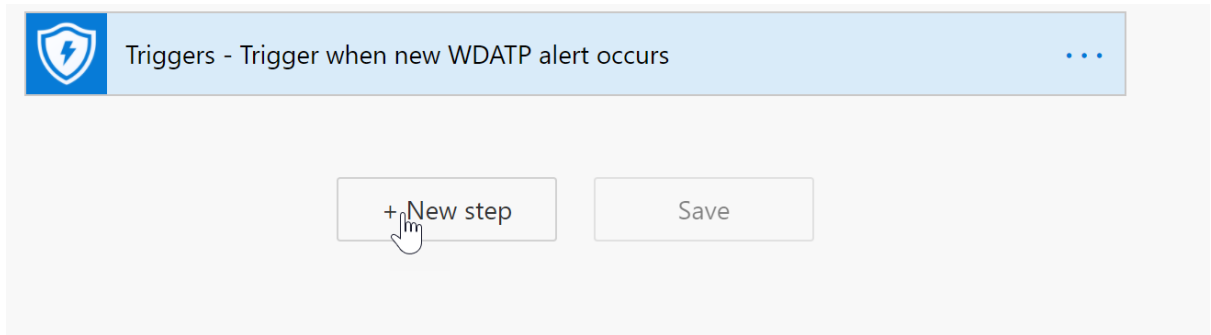
Use another account

You have now successfully created a flow that will run every time a new alert is created in Microsoft Defender for Endpoint. We now need to configure the Teams notification actions.

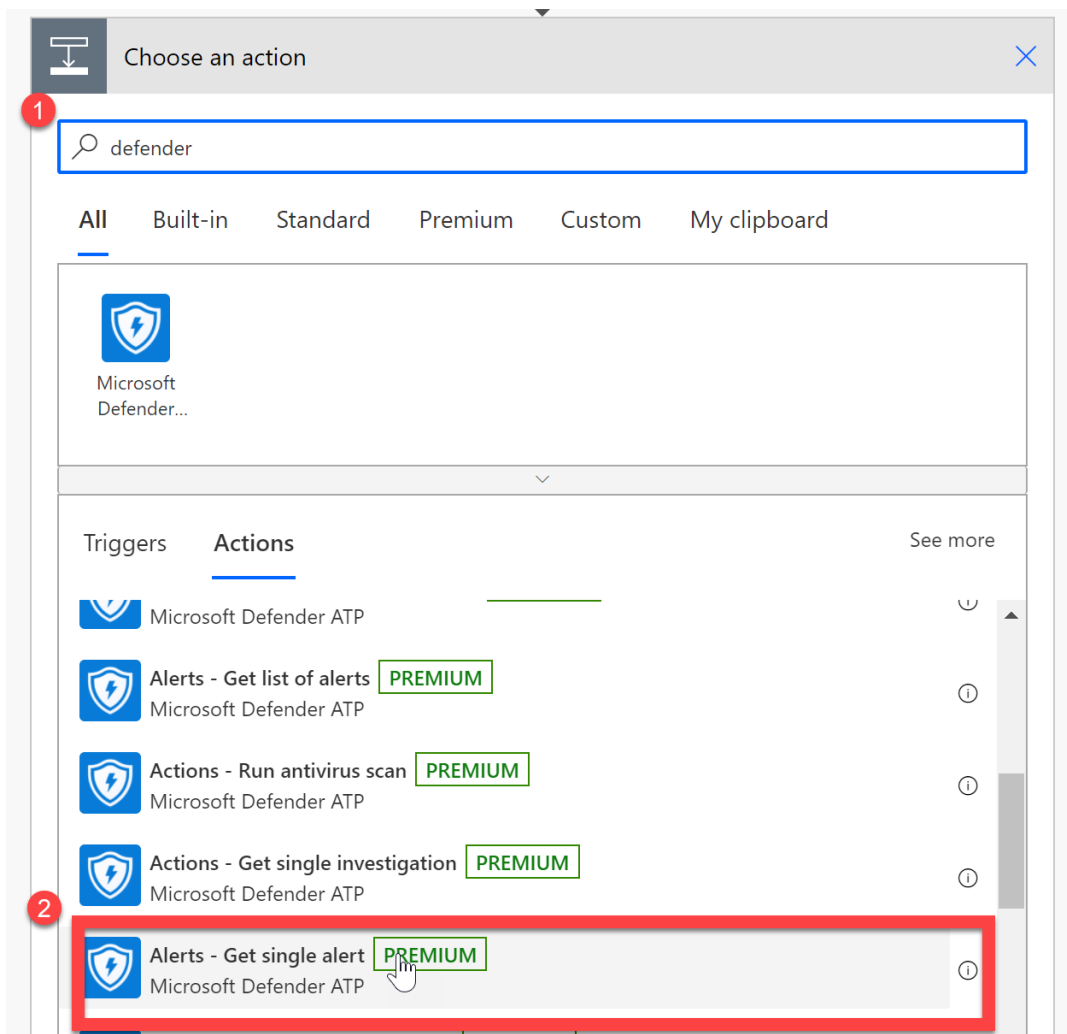
2) Send notifications to Teams

We will now create the initial actions and the steps required in the flow to send an adaptive card in Teams to an end-user when an alert in Defender is triggered.

1. Firstly, we need to get more information about the alert. Click new step

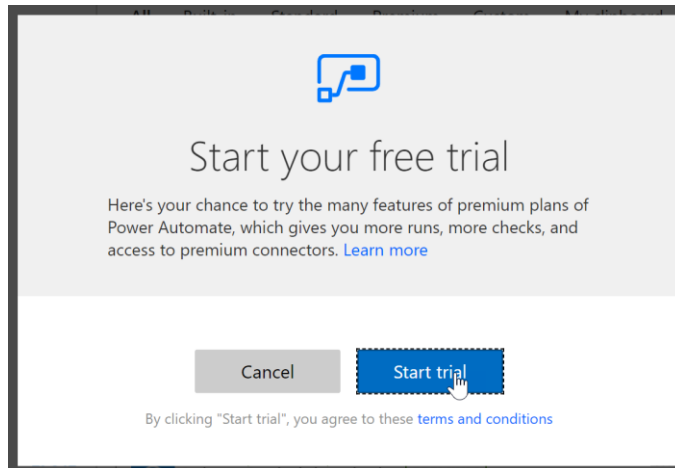


2. Search for 'Defender' in the dialog box, scroll down and then select 'Alerts – Get single alert'.

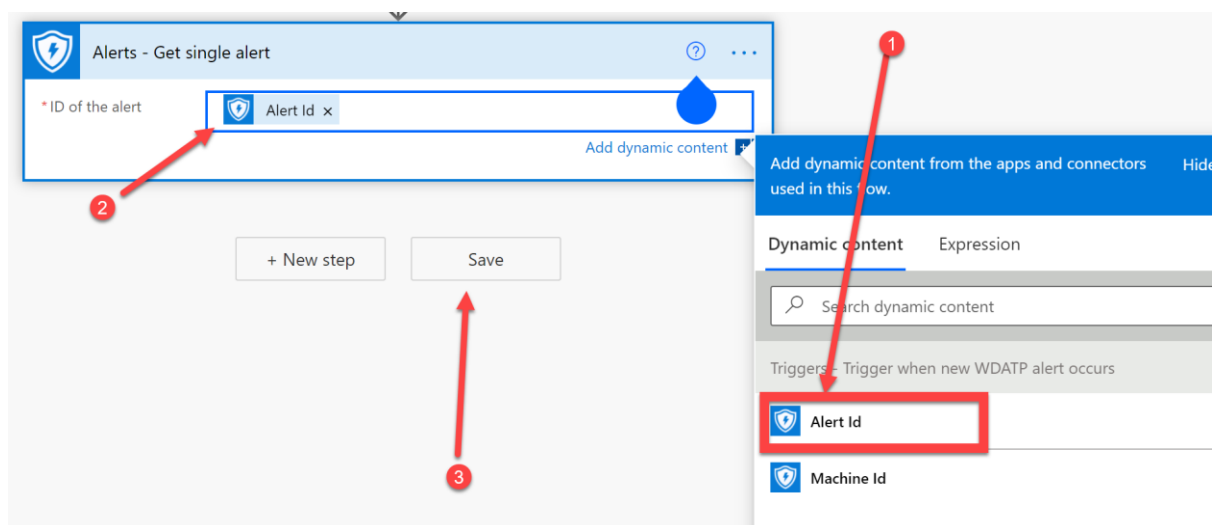


3. At this point, you may be asked to start a trial of Power Automate to access the Premium connectors. If so, sign up for the trial by clicking 'Start Trial'.

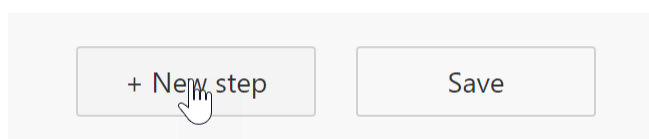
Note – The Microsoft Defender connector is a Premium connector and requires a Power Automate Premium license. If this is the first time creating a flow using a Premium connector in this tenant, you may be prompted to start a new trial of Power Automate Premium. If doing this in a demo environment and you are authorised, click on Start trial to receive a free 30-day trial.



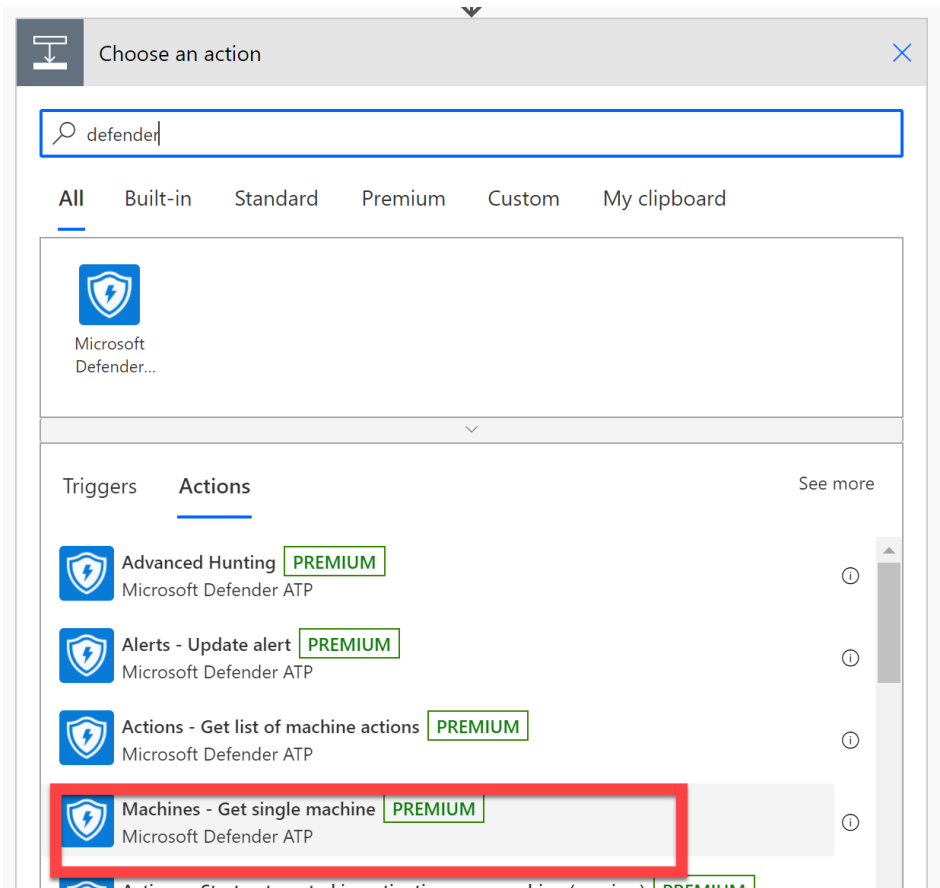
4. You will then need to use the Dynamic Content, from the Flow Trigger, to populate the ID of the Alert dialog box. Once your flow looks like the below, click Save.



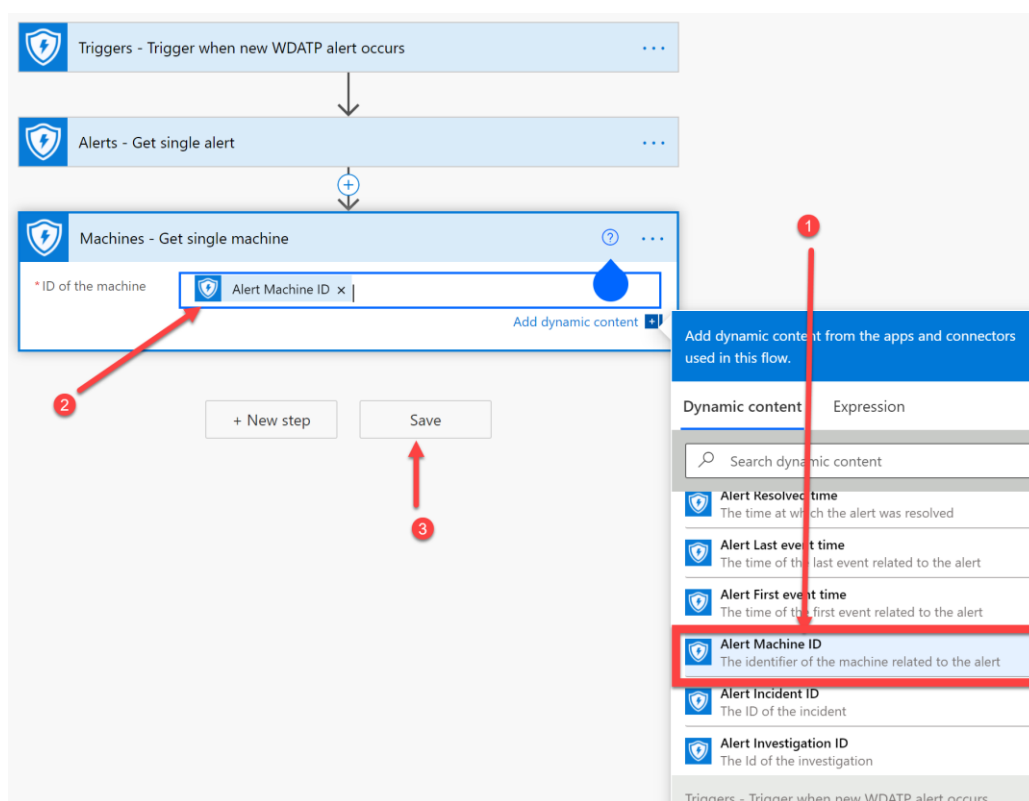
5. The previous step provides us with additional information about the Microsoft Defender alert, such as the name, severity, description, etc... We also need to know more information about the machine associated with the alert. Click New Step.



6. Search on Defender again and Select the 'Get single machine' action.



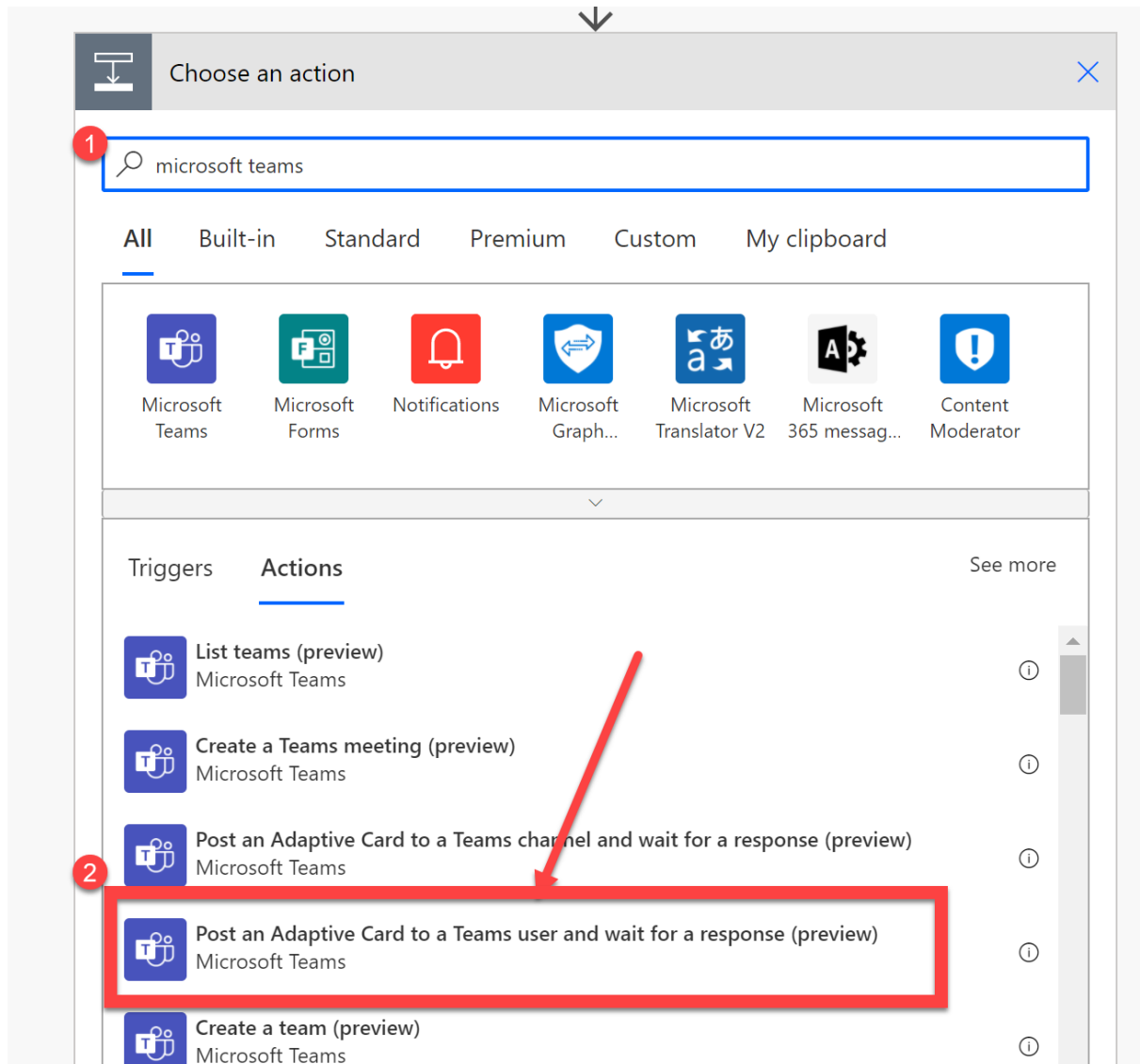
7. Populate the 'ID of the machine' dialog box with the 'Alert Machine ID' from the Dynamic Content. Click Save.



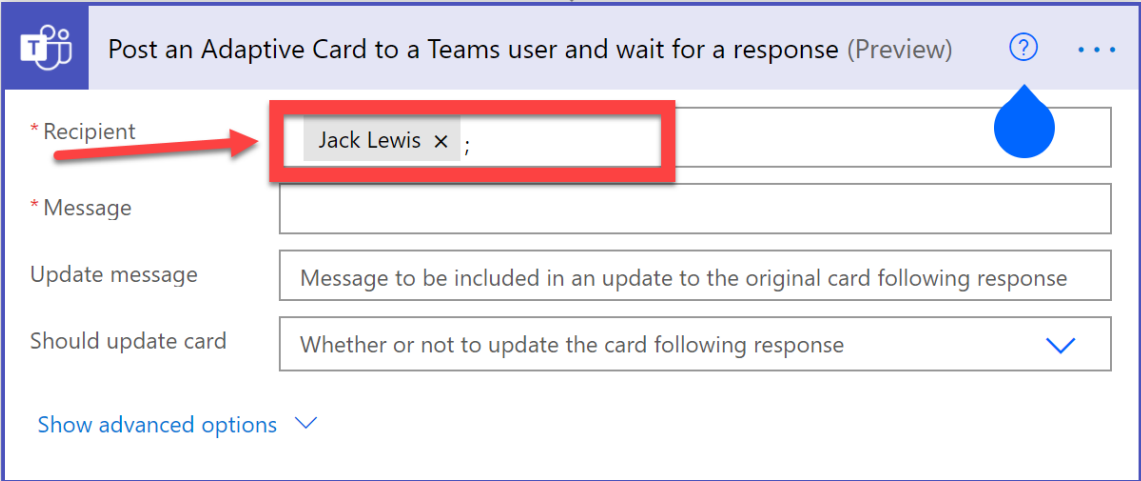
8. We now have all of the information we need about the alert and the associated machine to allow us to send a high-quality notification into Teams. Click new step.



9. In the dialog box, search for 'Microsoft Teams' and then select 'Post an Adaptive Card to a Teams user and wait for a response' **NOTE: MAKE SURE YOU SELECT USER AND NOT CHANNEL!**



10. In the 'Recipient' dialog box, enter yourself, as this will allow you to receive the notifications when this Flow is triggered.



Post an Adaptive Card to a Teams user and wait for a response (Preview) ? ...

* Recipient Jack Lewis x ;

* Message

Update message Message to be included in an update to the original card following response

Should update card Whether or not to update the card following response ✓

Show advanced options ▾

11. We will now need to populate the Message dialog box, with the Teams Adaptive Card. The adaptive card allows us to format the alert into a useable card, that also allows us to invoke actions. For example, in the adaptive card we will build and use in this flow, we will be able to assign the alert to an individual, isolate the machine or view more details about the specific alert. Firstly, you will need to copy and paste the following into the Message dialog box:

```
{
  "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
  "type": "AdaptiveCard",
  "version": "1.2",
  "body": [
    {
      "type": "ImageSet",
      "images": [
        {
          "type": "Image",
          "size": "Medium",
          "url": "https://betanews.com/wp-content/uploads/2017/01/win-defender.jpg"
        }
      ]
    },
    {
      "type": "TextBlock",
```

```

    "text": "New Microsoft Defender Alert",
    "size": "Large",
    "weight": "Bolder",
    "wrap": true
  },
  {
    "type": "TextBlock",
    "text": "ALERT DESCRIPTION",
    "isSubtle": true,
    "wrap": true
  },
  {
    "type": "ActionSet",
    "actions": [
      {
        "type": "Action.ShowCard",
        "title": "Assign Alert",
        "card": {
          "type": "AdaptiveCard",
          "body": [
            {
              "type": "Input.ChoiceSet",
              "id": "alertassign",
              "value": "${r}",
              "choices": [
                {
                  "title": "Joni Sherman",
                  "value": "jonis@"
                },
                {
                  "title": "Adele Vance",

```

```

        "value": "adelev@"
    }
],
    "style": "expanded",
    "isVisible": true
}
],
"actions": [
    {
        "type": "Action.Submit",
        "title": "Assign Alert",
        "data": {
            "x": "alertassign"
        }
    }
]
}
},
{
    "type": "Action.Submit",
    "title": "Isolate Machine",
    "data": {
        "x": "isolate"
    }
},
{
    "type": "Action.OpenUrl",
    "title": "View Details",
    "url": "https://securitycenter.windows.com/alerts/DETAILURL/details"
}
]

```

```

    }
  ]
}

```

12. Your flow action will then look like this, please press Save.

```

data : {
  "x": "isolate"
},
{
  "type": "Action.OpenUrl",
  "title": "View Details",
  "url": "DETAILURL"
}
]
}

```

Update message

Message to be included in an update to the original card following response

Should update card

Whether or not to update the card following response ▼

[Show advanced options](#) ▼

+ New step

Save

13. We now need to make some adjustments to the message, let's start with the Alert Description. Find the text **ALERT DESCRIPTION** and replace it with something similar to the following: Here we have used the dynamic content to list out the Alert ID, Severity of the alert, the alert description and the associated machine name... but feel free to use whatever you want!

```

{
  "type": "TextBlock",
  "text": "Alert ID:  Alert Alert ID ×, Severity:
 Alert Alert seve... ×, Description:  Alert Description ×,
Machine Name:  Machine Comp... × "

```

```

"text": " Alert ID: Alert Alert ID , Severity:
Alert Alert seve... , Description: Alert Description ,
Machine Name: Machine Comp... ,
    "isSubtle": true,
    "wrap": true
  },
  {
    "type": "ActionSet",
    "actions": [
      {
        "type": "Action.ShowCard",
        "title": "Assign Alert",
        "card": {
          "type": "AdaptiveCard",
          "body": [
            {
              "type": "Input.ChoiceSet",
              "id": "alertassign",
              "value": "${r",
              "choices": [
                {
                  "title": "Joni Sherman",
                  "value": "jonis@"
                },
                {
                  "title": "Adele Vance",
                  "value": "adelev@"
                }
              ]
            },
            {
              "type": "Text",
              "text": "Assign Alert"
            }
          ],
          "style": "expanded",
          "isVisible": true
        }
      }
    ]
  }

```

14. We can now focus our attention on the assign function, which will assign the alert to an individual in the Microsoft Defender portal. To do this, we will need to edit the choices available within the adaptive card. To do this, we will need to complete the values in the choices, by completing the UPN. Here is what my completed values look like:

```

"choices": [
  {
    "title": "Joni Sherman",
    "value": "jonis@gmfta.com"
  },
  {
    "title": "Adele Vance",
    "value": "adelev@gmfta.com"
  }
]

```

At this point you can add additional choices, by replicating what exists within the curly braces. Just make sure you remember to add a , after each closing curly brace (except for the final choice you make available), for example here is what an additional choice would look like:

```

"choices": [
  {
    "title": "Joni Sherman",
    "value": "jonis@gmfta.com"
  },
  {
    "title": "James Graham",
    "value": "james@gmfta.com"
  },
  {
    "title": "Jack Lewis",
    "value": "jack@gmfta.com"
  },
  {
    "title": "Adele Vance",
    "value": "adelev@gmfta.com"
  }
],

```

- Finally, we need to update the DETAILURL so that it populates it with the correct URL for the Alert, should you want to view more details before assigning the alert or isolating the machine. To do this we need to replace the DETAILURL value with the 'Alert Alert ID' Dynamic Content

```

{
  "type": "Action.OpenUrl",
  "title": "View Details",
  "url": "https://securitycenter.windows.com/alerts/

```

Alert Alert ID × /details"

```

}
}
}
}
}

```

Add dynamic content +

Message to be included in an update to the original card following response

Whether or not to update the card following response ▼

ions ▼

+ New step
Save

Add dynamic content from the apps and connectors used in this flow.

Dynamic content

Expression

Machine OS build
The OS build of the machine

Machine RBAC group ID
The ID of the RBAC group to which the machine belongs

Machine Is AAD joined
A flag indicating whether the machine is joined to AAD

Alerts - Get single alert

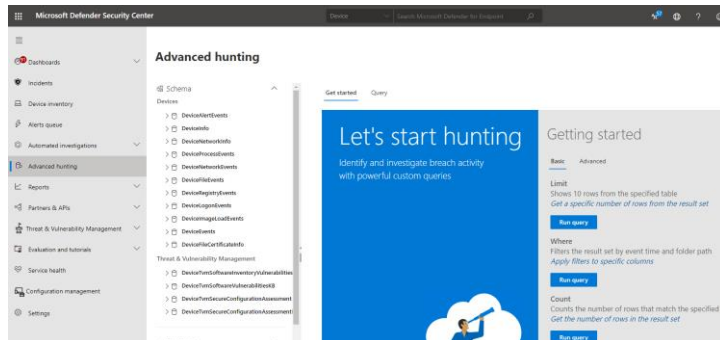
Alert Alert ID
Alert identifier

16. Once complete. Click Save. We will now test the flow to make sure it is behaving as expected.

3) Test out the Flow

To test the flow, we need to generate a new alert in Microsoft Defender for Endpoint (MDE). Typically, you'd need to achieve this by running an attack scenario on an onboarded client, however for the purpose of this lab (and to save time), we'll trigger an alert using a custom detection rule against the data that already resides in the tenant.

1. Login to <https://securitycenter.microsoft.com> with your tenant admin credentials.
2. Navigate to Advanced Hunting.

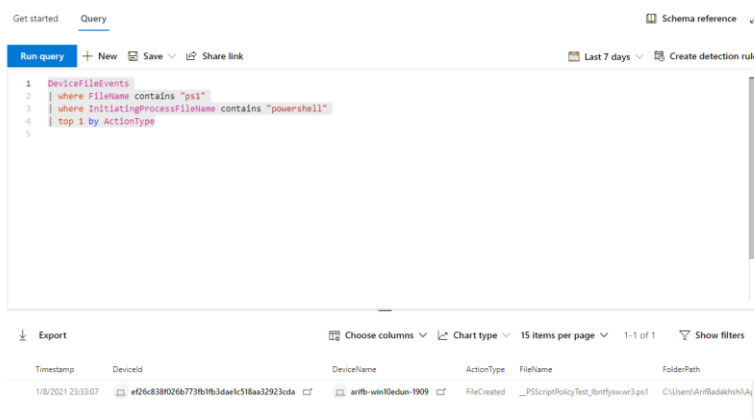


3. Create a new query.
4. We'll create something simple using the DeviceFileEvents schema.
5. Copy/Paste the following query:

DeviceFileEvents

```
| where FileName contains "ps1"  
| where InitiatingProcessFileName contains "powershell"  
| top 1 by ActionType
```

6. Run the query to see the result – you should receive a single resulting ps1 file. If not, perhaps widen the filter parameters until you get at least 1 result.



7. Click on Create detection rule.

✓ [Create detection rule](#)

8. Complete Alert details as follows:

Alert details

Provide the name of the alert and the information displayed with it.

Detection name *

Detection test

Frequency * ⓘ

Every 24 hours

Alert title *

Flow test alert

Severity *

Medium

Category *

Execution

MITRE techniques

Select MITRE techniques

Description *

Detected a ps1 file - this means your flow is working.

Recommended actions

Provide remediation recommendations for responders

Next

9. Click next.
10. On the Action page – click next.
11. On the summary page - Click on Create.
12. The rule should run once upon creation; however, you can manually trigger a run within Settings -> Customer detections. Simply select your rule and hit run.
13. Navigate to Alert view and you should now see your custom alert – it may not be at the top of the queue (as we're querying older data). Click on the Alert to prove it was created by your custom detection rule.

Details

Flow test Alert

Medium **New**

[See in timeline](#)
[Link to another incident](#)
[Assign to me](#)
...

Manage alert ^

① Classify this alert
True alert
False alert

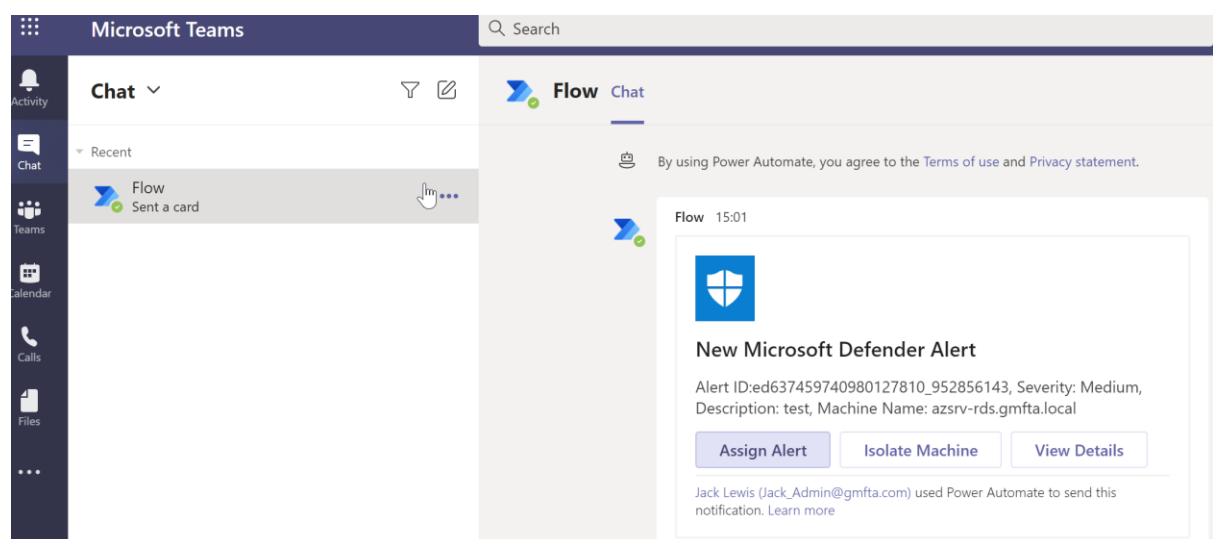
Status New v

Classification Select classification... v

Alert details ^


Incident	Multi-stage incident involving Execution & Exfiltration on one endpoint (open in Microsoft 365 Defender)
Detection source	Custom detection
Category	Execution
First activity	Jan 8, 2021, 11:33:07 PM
Last activity	Jan 8, 2021, 11:33:07 PM
Generated on	Jan 11, 2021, 5:05:48 PM
Assigned to	(Unassigned)

- See the Detection source is Customer detection.
- Your flow should now trigger based on a new Alert being generated. In a separate browser tab pen <https://teams.microsoft.com/> and login as the account that you defined as the recipient in step 2.10 of this lab. After a minute (or 3) you should receive a Teams message from the Flow bot. The message will look something like the following



16. Click on the Assign Alert button in the card, select a user with one of the radio settings, and then click the bottom Assign Alert button.

Flow 15:01



New Microsoft Defender Alert

Alert ID:ed637459740980127810_952856143, Severity: Medium, Description: test, Machine Name: azsrv-rds.gmfta.local

1

Assign Alert

Isolate Machine

View Details

2

☒ Joni Sherman

☐ James Graham

☐ Jack Lewis

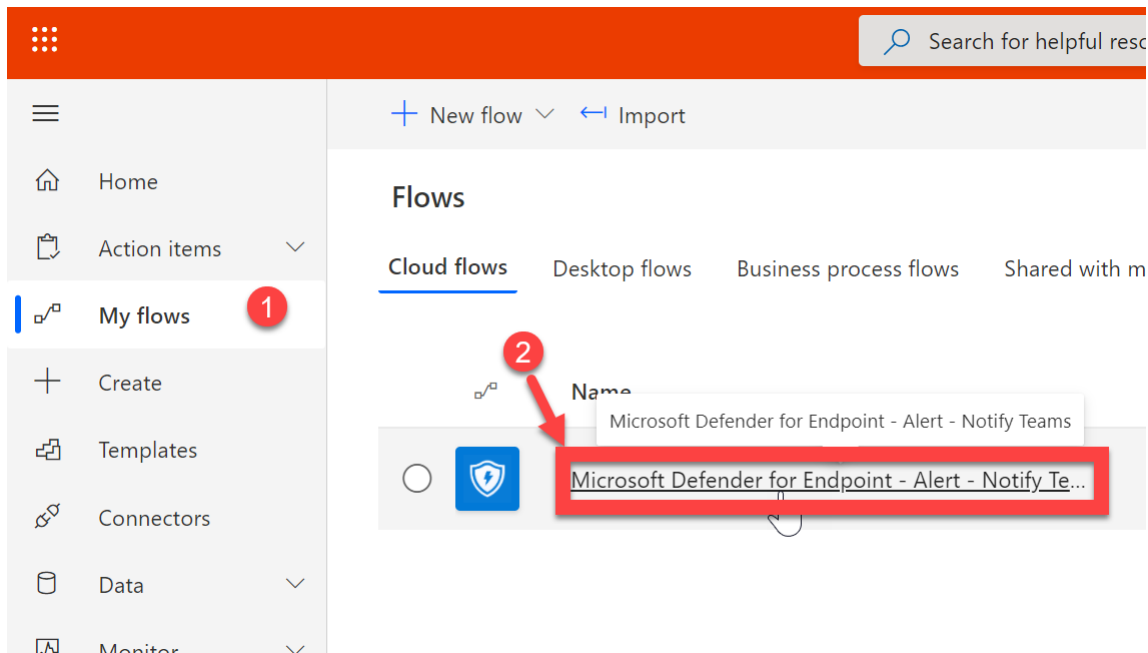
☐ Adele Vance

3

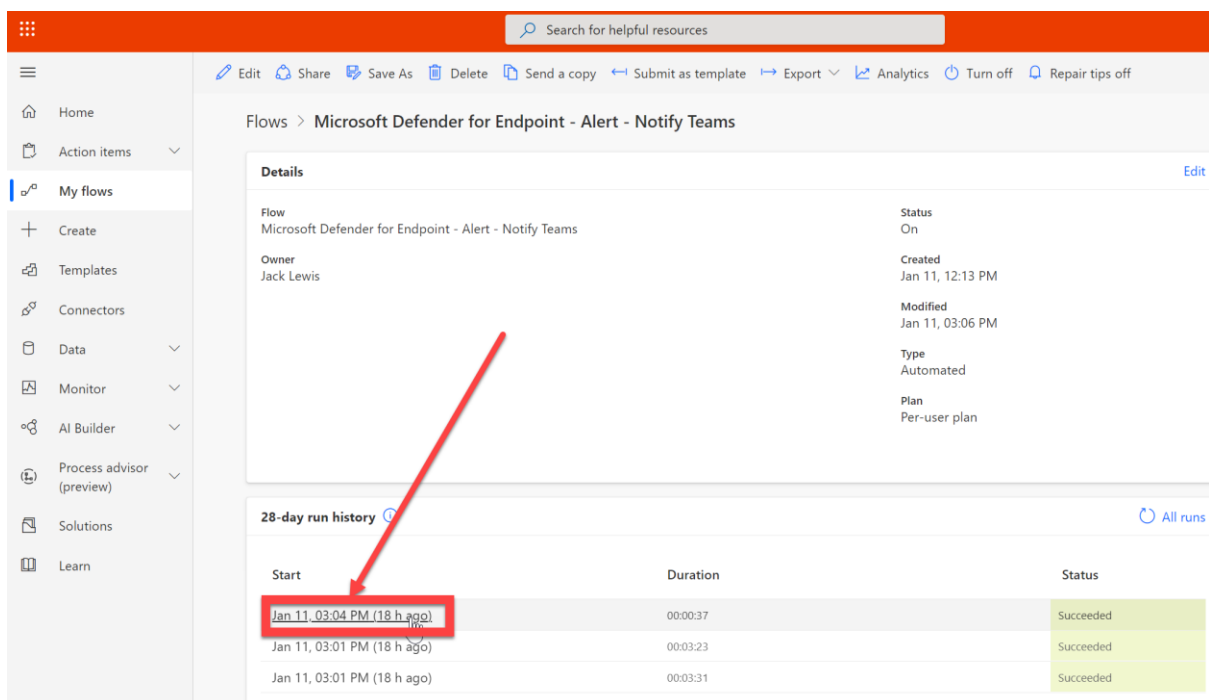
Assign Alert

Jack Lewis (Jack_Admin@gmfta.com) used Power Automate to send this notification. [Learn more](#)

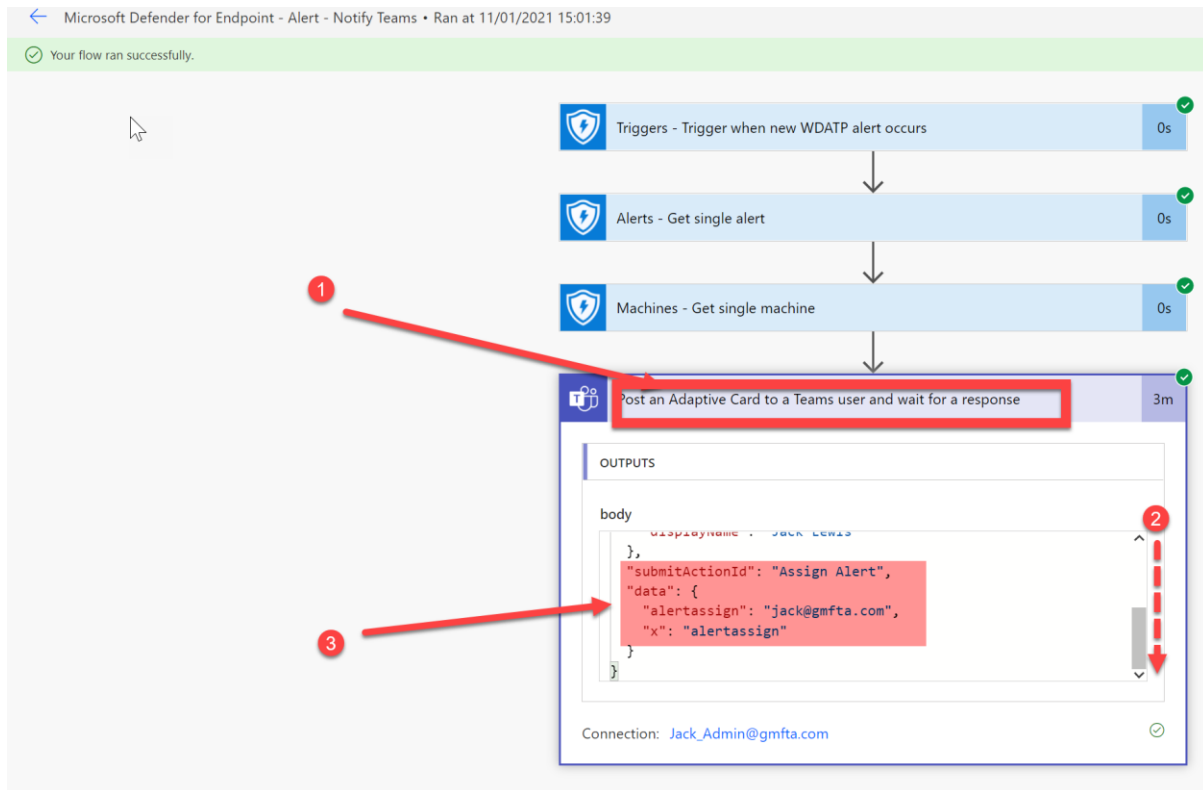
17. You will find that currently by clicking on the actions, nothing happens in the Defender portal. We will configure the Adaptive Card actions and the associated API calls in the next section of this lab, but before then, let's review the flow that ran as a result of you creating an alert. To do this, navigate back to flow.microsoft.com, click on My Flows and then click on the name of the Flow that we created during this lab. **DO NOT CLICK ON EDIT, MAKE SURE YOU CLICK ON THE NAME OF THE FLOW DEMONSTRATED IN THE IMAGE BELOW.**



18. Power Automate allows you to review the previously run flows (over the last 28 days), this is useful when you want to troubleshoot or debug any issues you are seeing with your flows, as you can see the responses to each of your actions, to discover where any issues may reside. Click on the latest flow run to review what has happened at each step.



19. Click on the Post an Adaptive Card to a Teams user and wait for a response step, scroll down the Output body and review the JSON data. You will find that the SubmitActionID attribute is telling us that we need to assign the alert, and that the alertassign attribute is telling us that it should be assigned to a specific user. We will use this in our next steps to configure a condition that looks at the response body data and makes decisions about alert assignment or machine isolation.

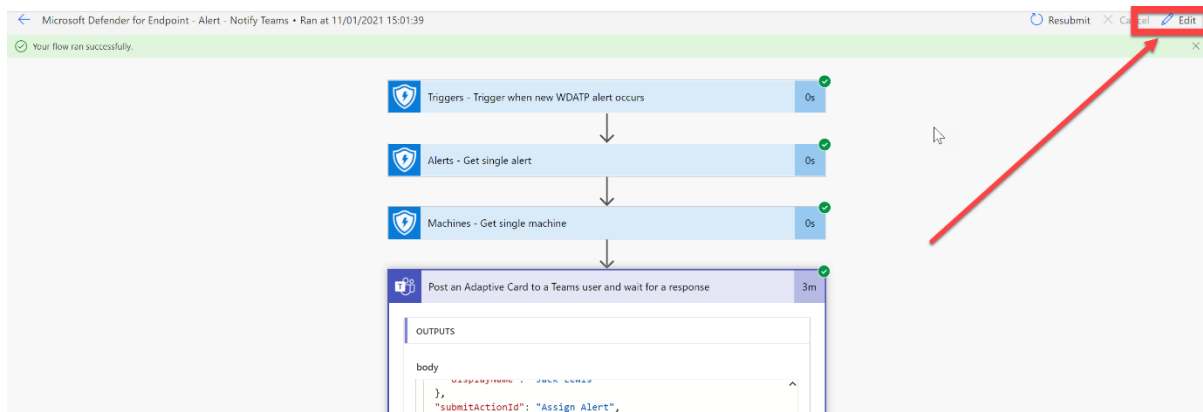


Now that we have tested the Flow and we understand how the Adaptive Card buttons and associated actions respond to the Flow, we can now configure the next steps in the flow to invoke certain actions within Microsoft Defender.

4) Configure the Adaptive Card Actions

Now that we have confirmed that the flow is triggering and alerting as expected, we need to configure the Adaptive Cards actions functionality, so that when you ask for a machine to be isolated, or an alert to be assigned, it happens in the Microsoft Defender portal. We will start by processing the response, and then we will use conditions to perform certain actions.

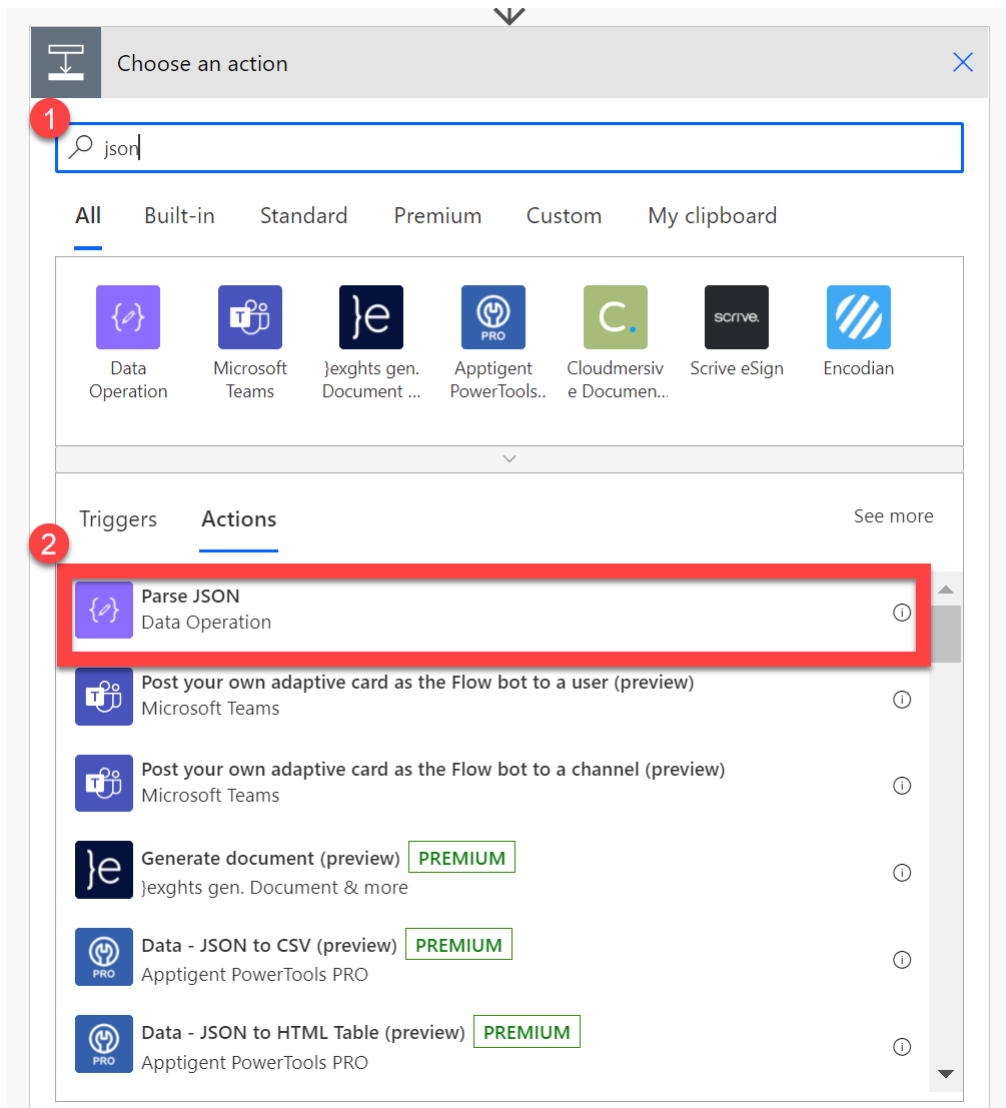
1) Go back into your flow, by clicking edit



2) Select New Step

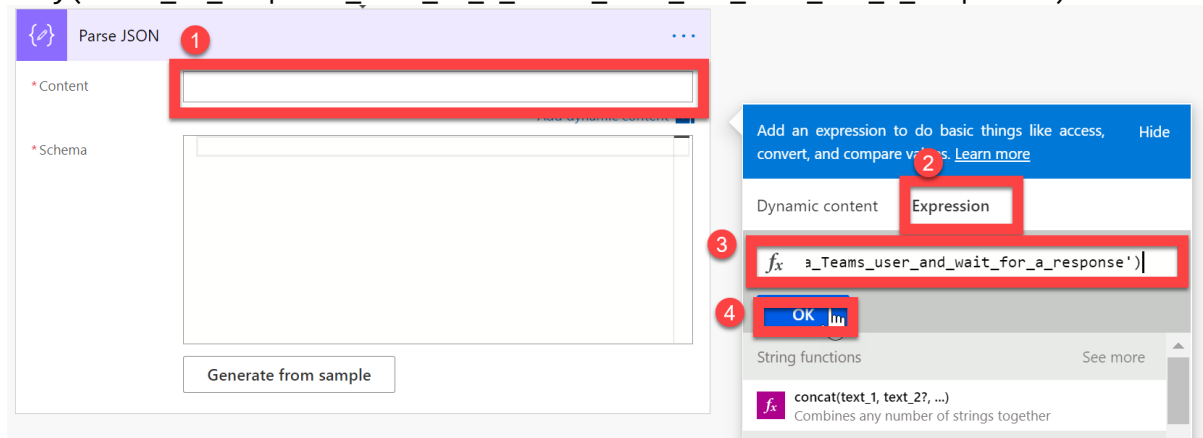


3) In the dialog box enter 'json', and then select the Parse JSON action.

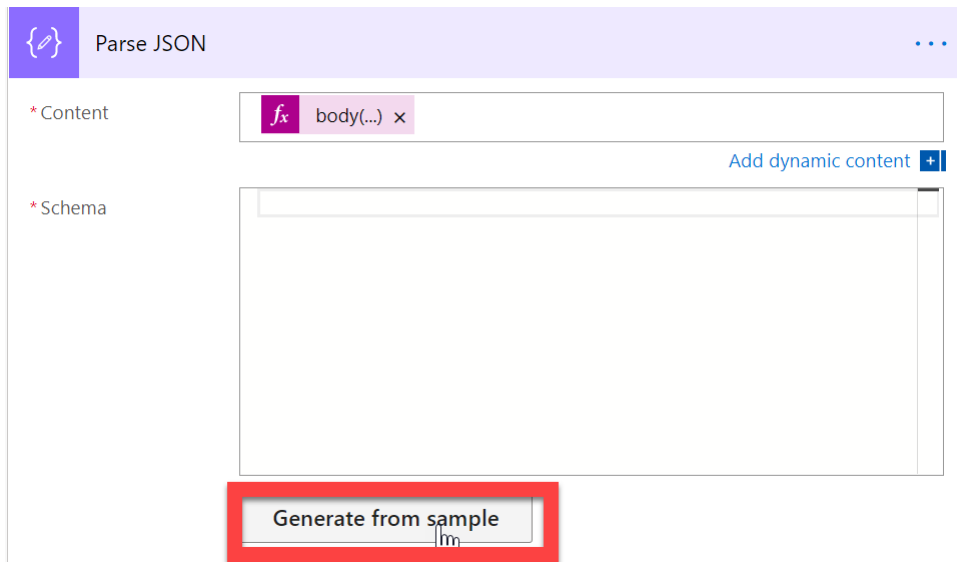


4) Select the Content input box, then select Expression and paste the below into the formula (fx) dialog box and click OK

body('Post_an_Adaptive_Card_to_a_Teams_user_and_wait_for_a_response')



5) Click Generate from sample



6) Paste the below into the dialog box and click Done

```
{
  "responseTime": "2021-01-11T15:05:09.7253401Z",
  "responder": {
    "objectId": "eb28b631-27e2-45ea-8c2c-e5269e6eea16",
    "tenantId": "5eb42099-961e-44fc-bf27-c97c06c9eb6e",
    "email": "Jack_Admin@gmfta.com",
    "userPrincipalName": "Jack_Admin@gmfta.com",
    "displayName": "Jack Lewis"
  },
  "submitActionId": "Assign Alert",
  "data": {
    "alertassign": "jonis@gmfta.com",
    "x": "alertassign"
  }
}
```

Insert a sample JSON Payload

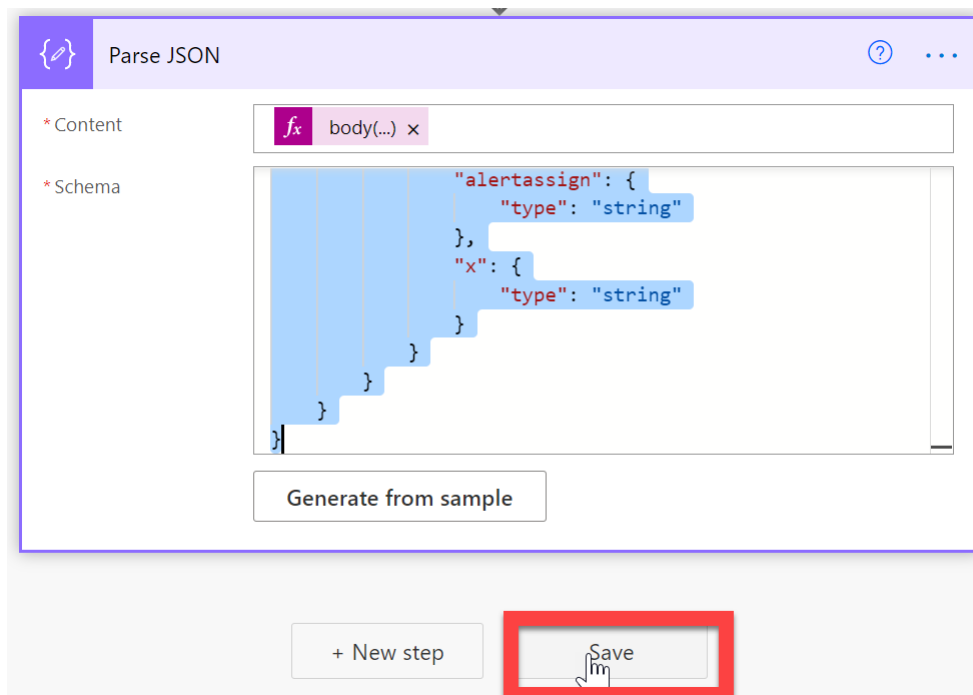


ⓘ Clicking 'Done' will overwrite your current schema

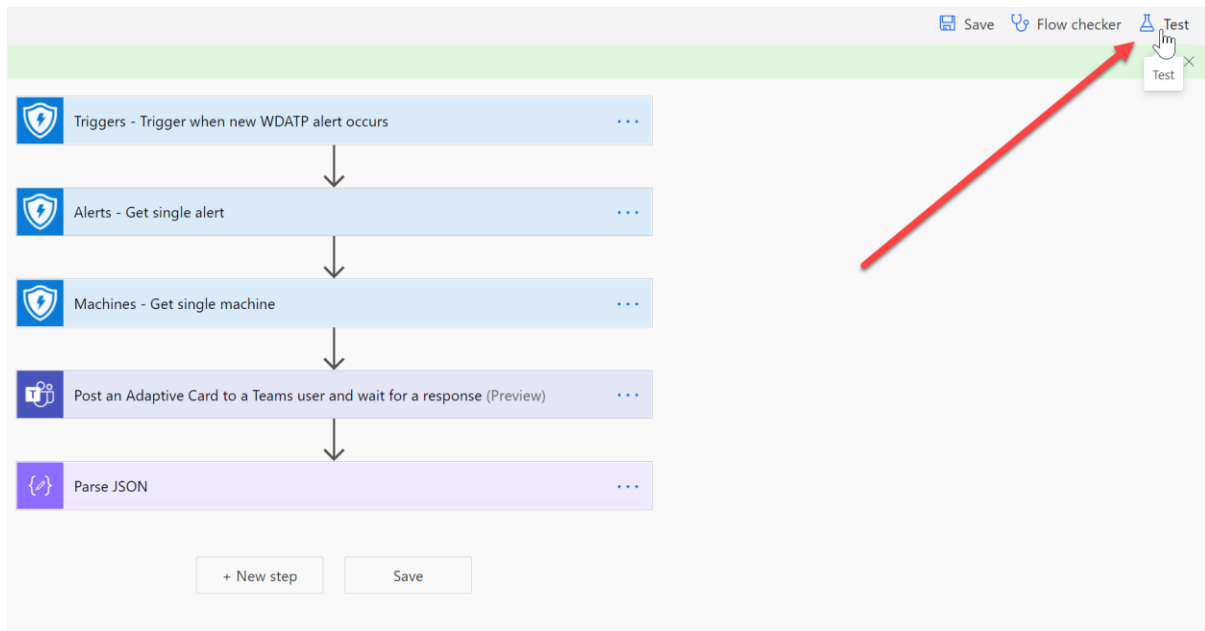
```
{  "userPrincipalName": "Jack_Admin@gmfta.com",  "displayName": "Jack Lewis"},  "submitActionId": "Assign Alert",  "data": {    "alertassign": "jonis@gmfta.com",    "x": "alertassign"  }}
```

Done

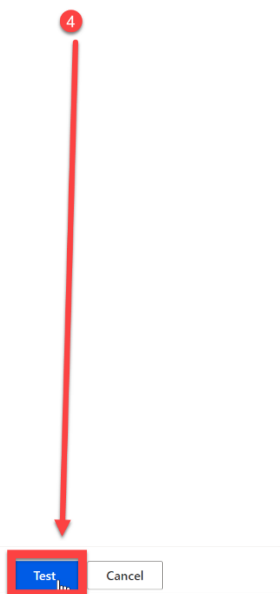
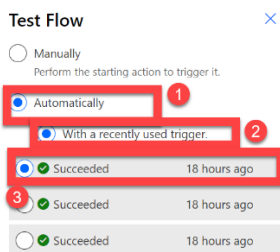
7) Click Save



8) As the flow has successfully run previously, we can reuse that data to test out our flow again. Click test




- 9) Select Automatically, then select With a recently used trigger, click on one of the radio buttons to use the previous flow trigger data, and then click Test



- 10) Your flow will then run and you can watch each step sequentially complete, when it gets to the Teams step, you will need to go back into Teams (teams.microsoft.com) and will need to respond to the adaptive card, in this example, click on Isolate Machine



Flow 09:38



New Microsoft Defender Alert

Alert ID:ed637459742575156562_-661060956, Severity: Medium,
Description: test, Machine Name: james-lvm-20h2

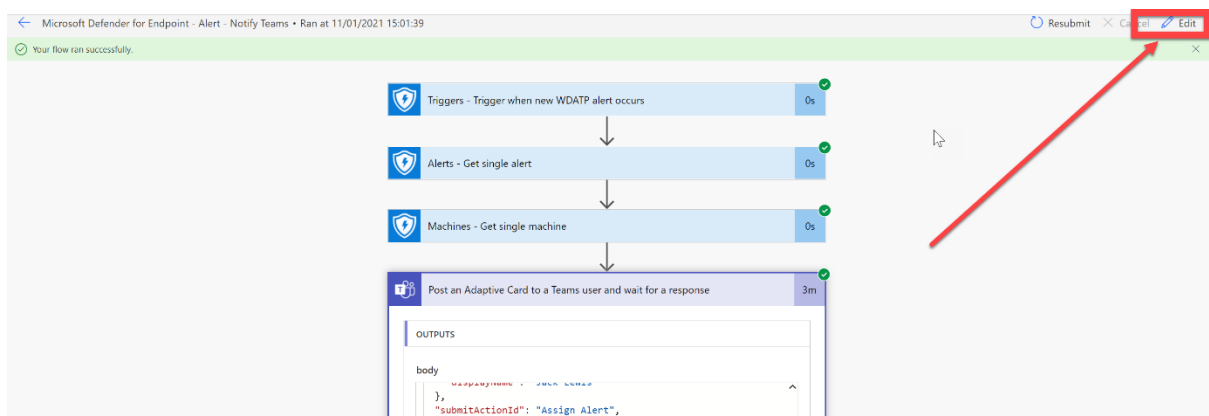
[Assign Alert](#) [Isolate Machine](#) [View Details](#)

Jack Lewis (Jack_Admin@gmfta.com) used Power Automate to send this notification. [Learn more](#)

- 11) Head back into the Flow tab, and you will see that the flow has successfully completed, click on the Parse JSON step and review the output. We will use this to allow us to make decisions in the following steps.



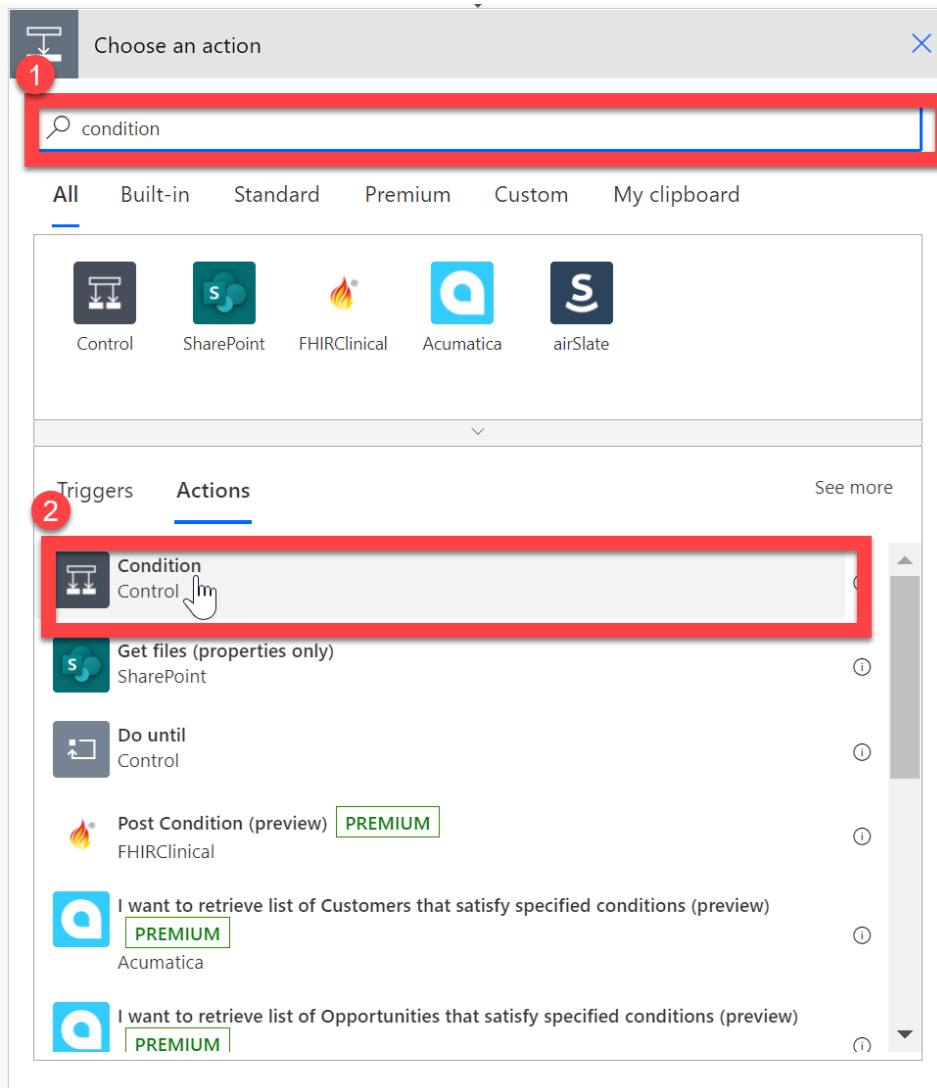
12) Go back into your flow, by clicking edit



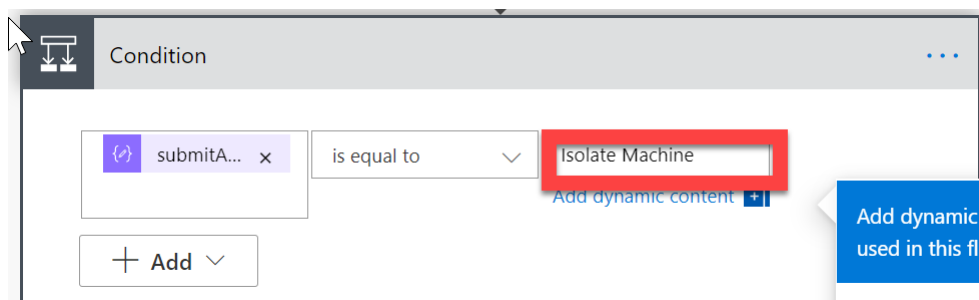
13) Select New Step



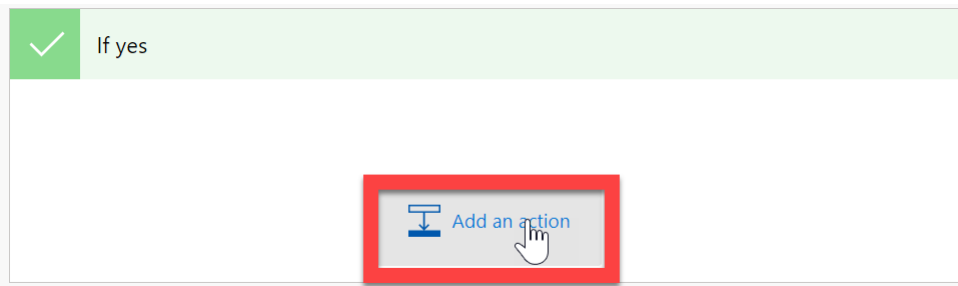
14) In the dialog box, search for condition and then select Condition



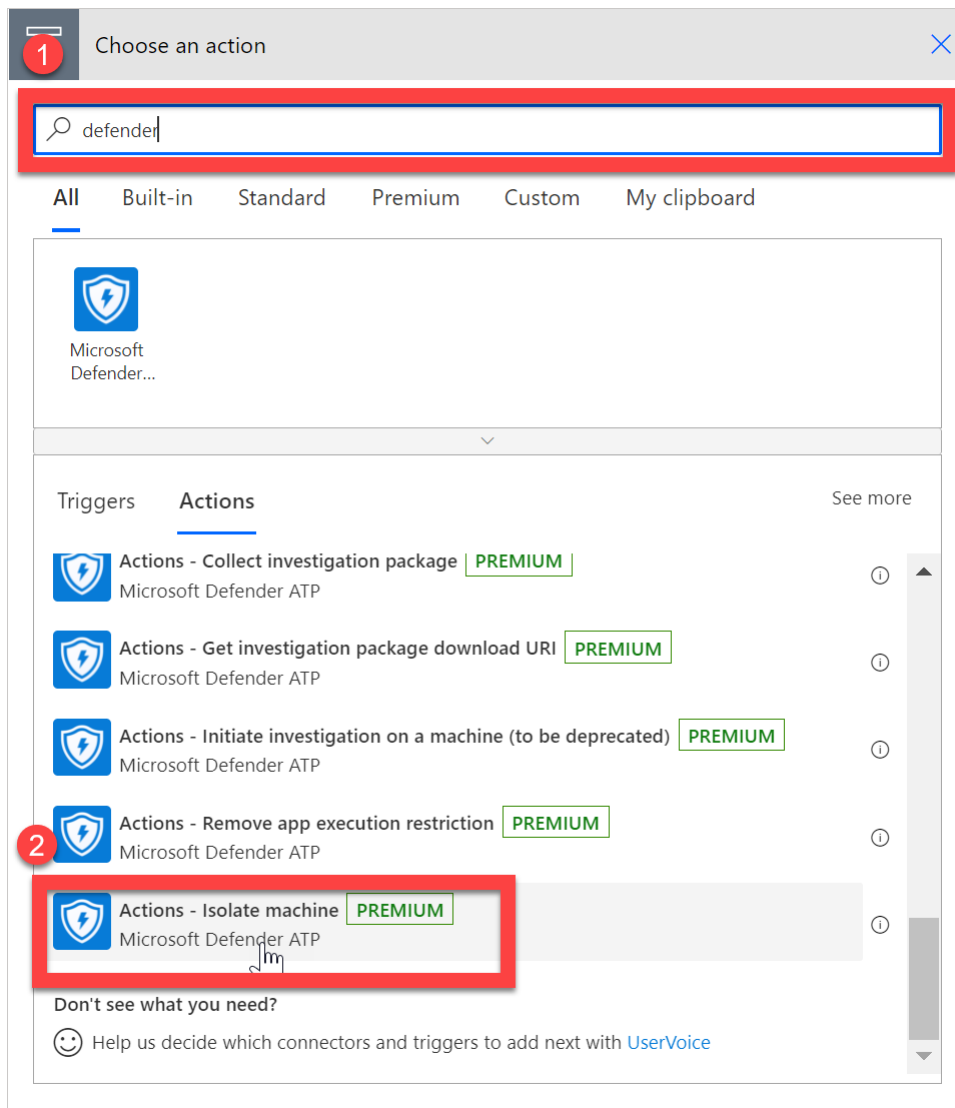
15) Within the condition – select submitActionId from the dynamic content. Make sure your operator is set to 'is equal to', and set the value Isolate Machine



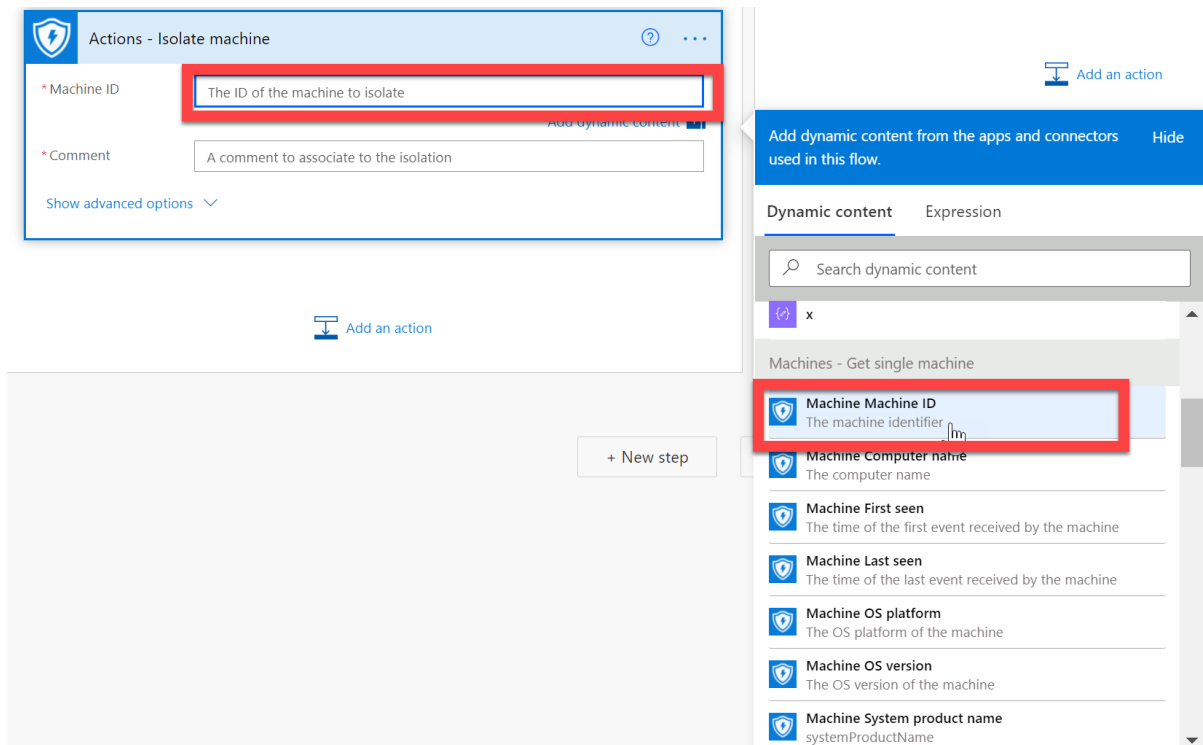
16) We will now build the actions for if the condition is evaluated to be true – in which case, we need to isolate the machine. Under If yes, click Add an action.



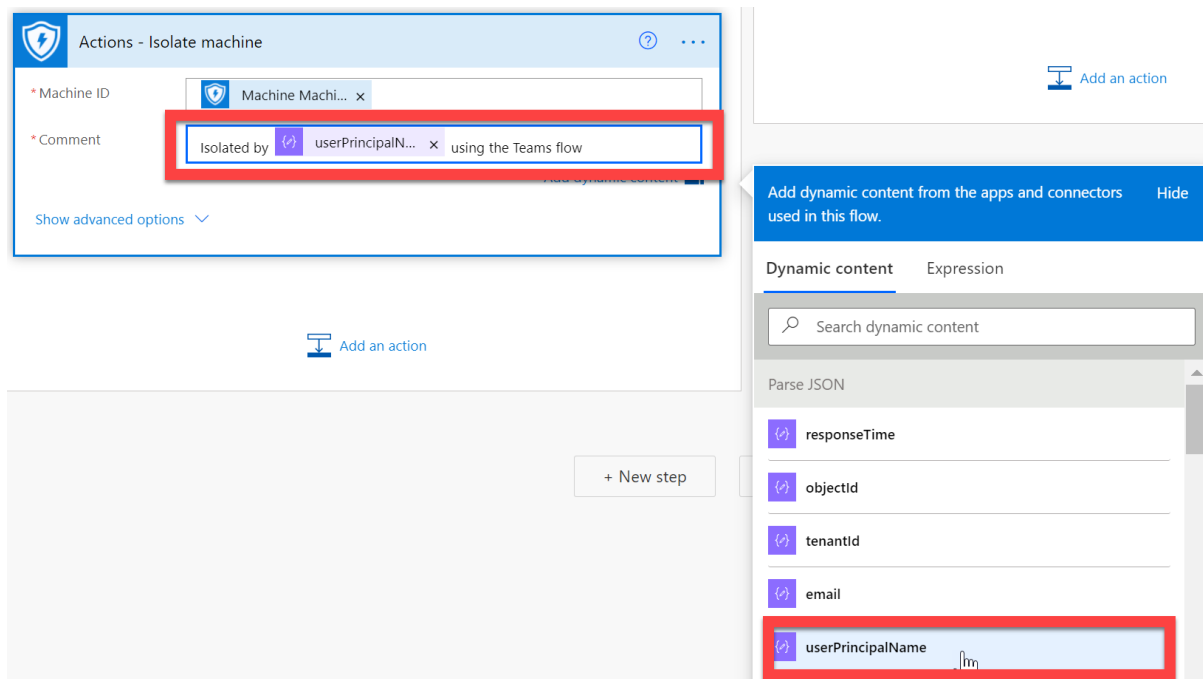
17) In the dialog box, search for defender and select Actions – Isolate machine



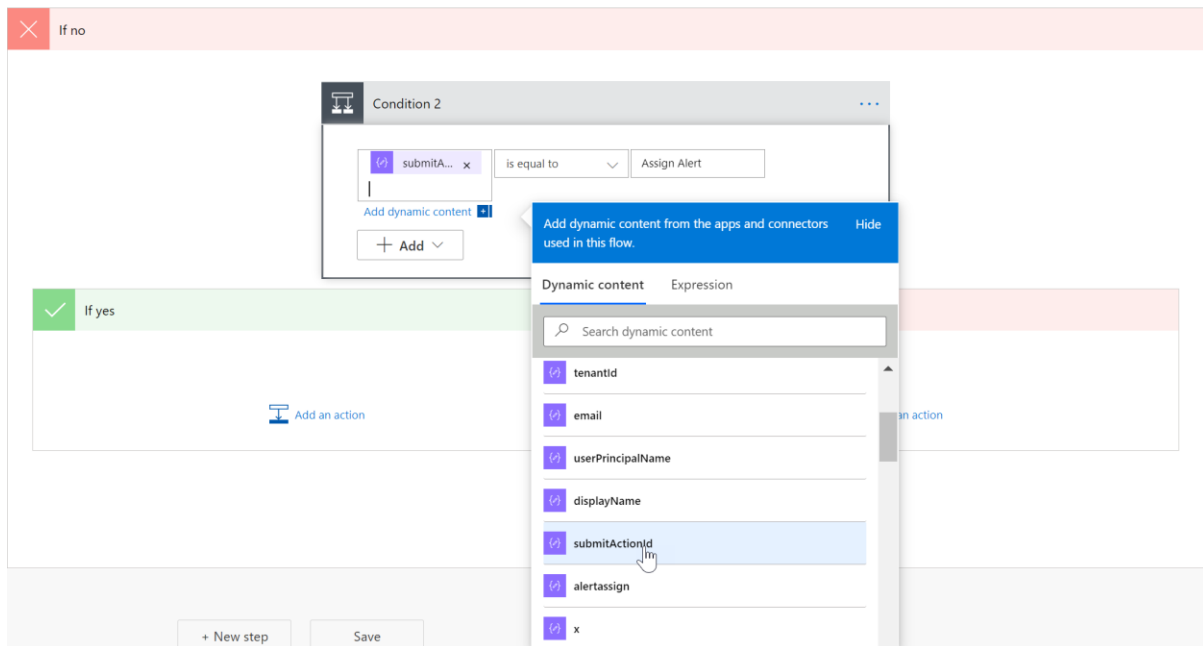
18) Select the Machine ID dialog box, and then select Machine Machine ID



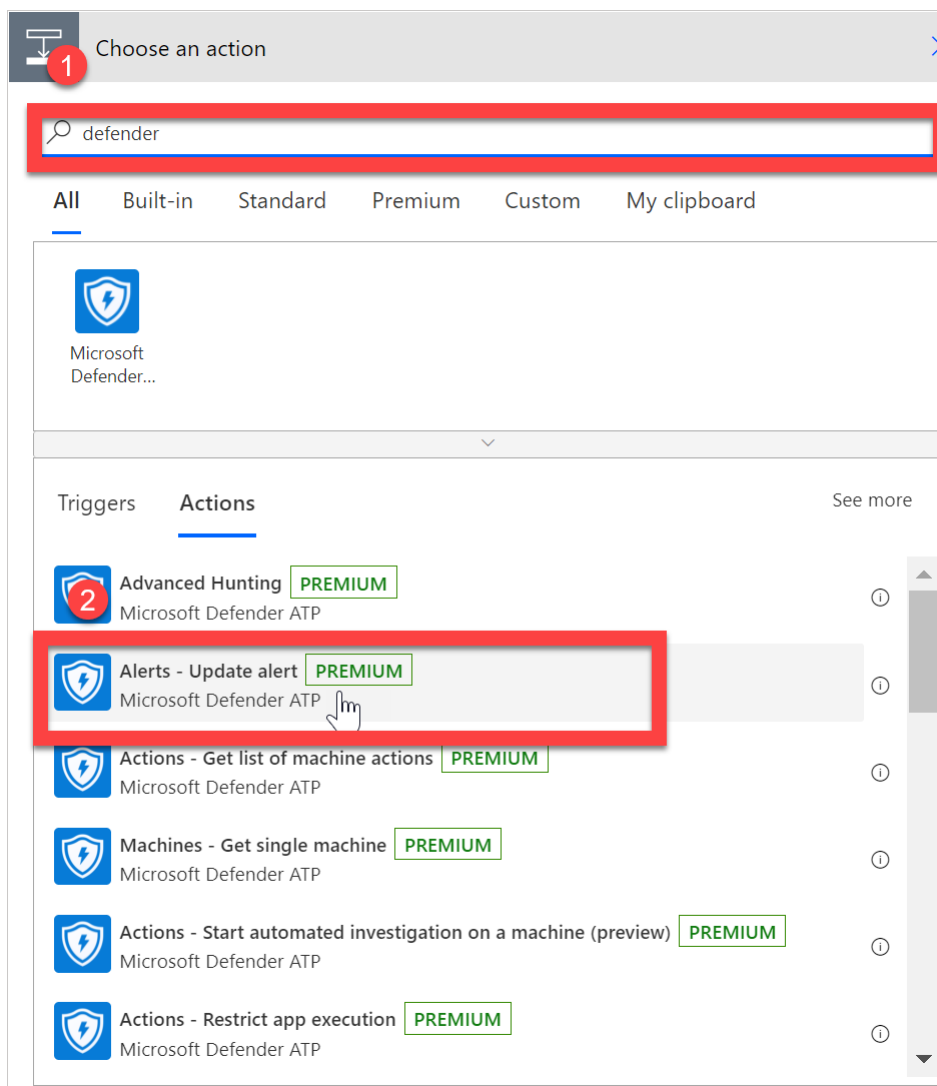
19) Select the comment dialog box and type something logical in here. For example, I've used the userPrincipalName dynamic content to allow me to write that the machine was isolated by a specific user, using the Teams flow.



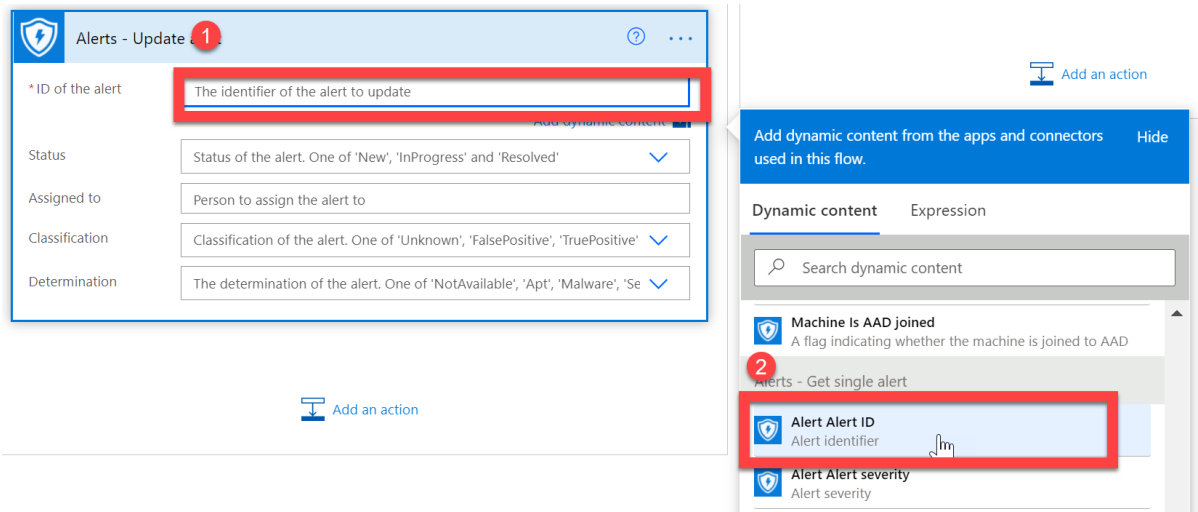
20) We now need to add a condition if the previous condition is evaluated to be false. You can do this by adding a new step under If no. We need to create a condition that evaluates if the submitActionID value is equal to Assign Alert. It should look like the below once complete. Refer to the previous steps to remind yourself how to add a condition if required.



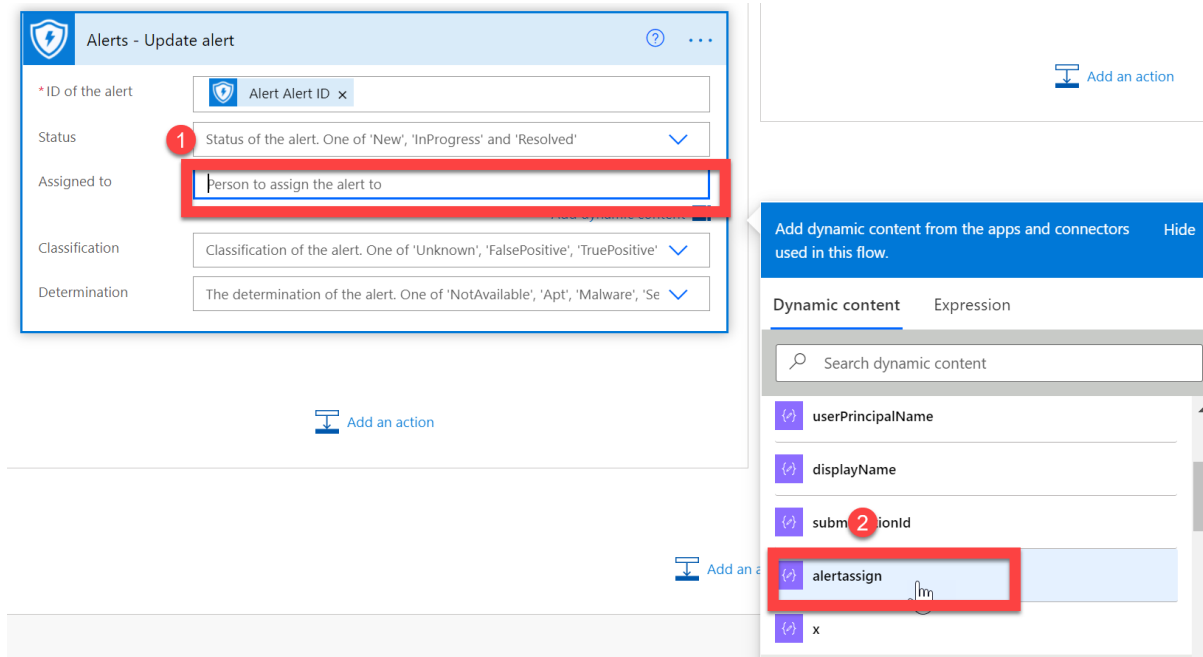
21) Under If yes, for this condition, add a Defender Alerts - Update Alert action



22) In the ID of the alert dialog box, select Alert ID from Dynamic Content (**NOTE: You will need to scroll down to find this, it will be under the Alerts – Get single alert section**)



23) In the Assigned to dialog box, select alertassign from Dynamic Content



24) You can now save your flow.

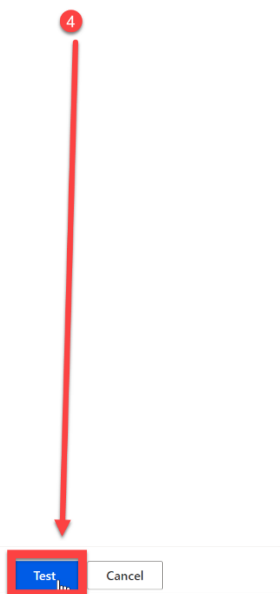
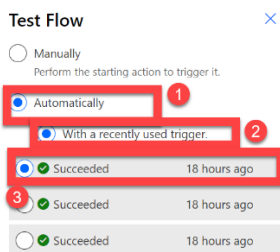
Congratulations! The logic of your flow is now complete. We now need to test the flow and see the results in the Microsoft Defender Security Centre Portal.

5) Run final flow testing and see the results in the Defender Security Centre Portal
We are nearly complete! We just need to run a final test to ensure the flow is behaving as expected.

1) As the flow has successfully run previously, we can reuse that data to test out our flow again. Click test



- 2) Select Automatically, then select With a recently used trigger, click on one of the radio buttons to use the previous flow trigger data, and then click Test




- 3) Your flow will then run and you can watch each step sequentially complete, when it gets to the Teams step, you will need to go back into Teams (teams.microsoft.com) and will need to

respond to the adaptive card, in this example, click on Assign Alert, and assign the alert to somebody.



Flow 15:01



New Microsoft Defender Alert

Alert ID:ed637459740980127810_952856143, Severity: Medium, Description: test, Machine Name: azsrv-rds.gmfta.local

1

Assign Alert

Isolate Machine

View Details

2

☒ Joni Sherman

☐ James Graham

☐ Jack Lewis

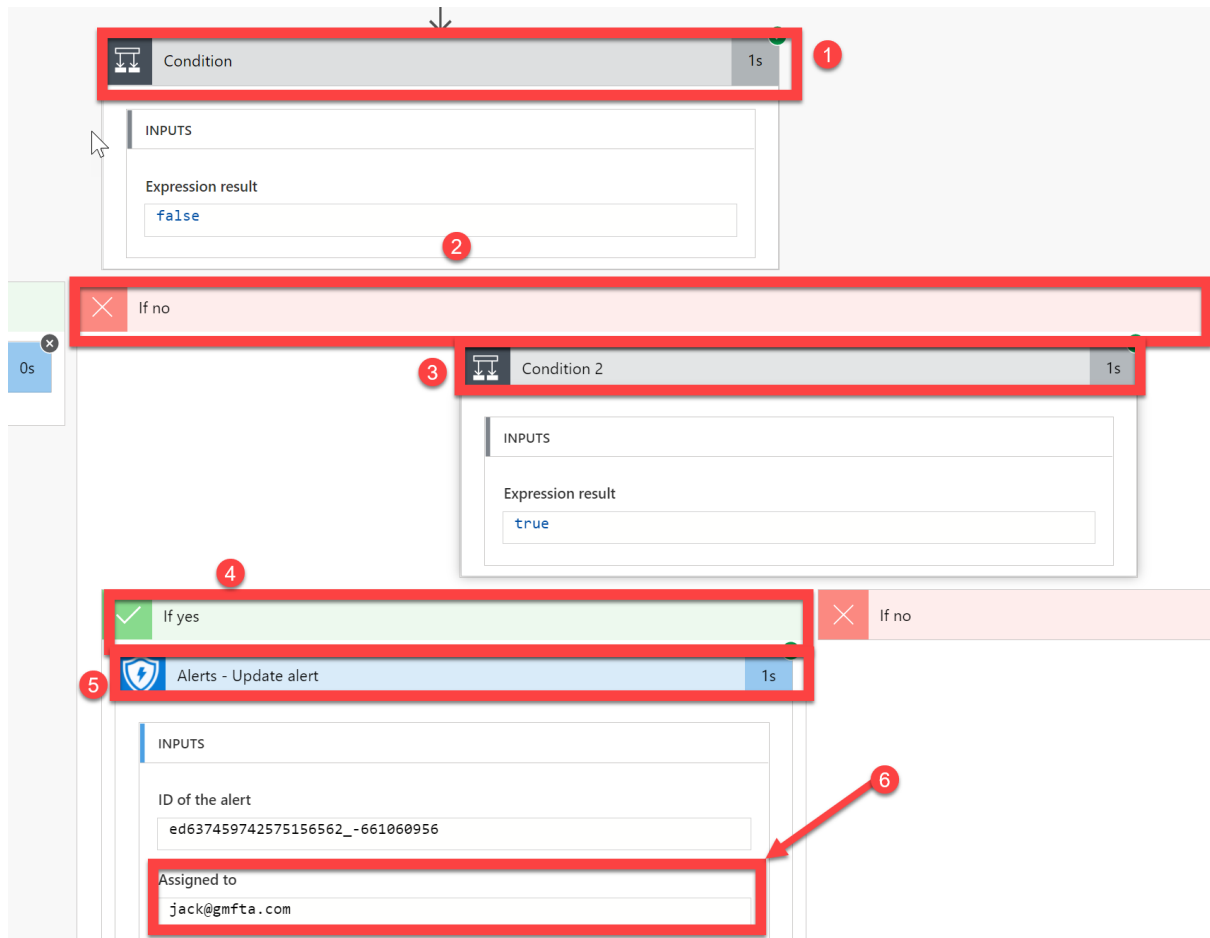
☐ Adele Vance

3

Assign Alert


Jack Lewis (Jack_Admin@gmfta.com) used Power Automate to send this notification. [Learn more](#)

- 4) Heading back into the Flow web app, you will see that the flow successfully completes after a few seconds, you can then expand out the condition step and the steps/actions below it to see that the alert has been assigned to the individual you selected



- 5) We can now confirm this in the defender portal, by heading back into the Teams web app and clicking on View Details

Flow 10:33



New Microsoft Defender Alert

Alert ID:ed637459742575156562_-661060956, Severity: Medium, Description: test, Machine Name:james-lvm-20h2

Assign AlertIsolate MachineView Details

☐ Joni Sherman

☐ James Graham

☒ Jack Lewis

☐ Adele Vance

Assign Alert

Jack Lewis (Jack_Admin@gmfta.com) used Power Automate to send this notification. [Learn more](#)

- 6) You can see in the Defender Security Centre Portal that the alert has been assigned to the selected individual

PS1 File Found

james-lvm-20h2

Risk level Medium

nt authority\system

ALERT STORY

[664]

[792] services.exe

[3412] MsSense.exe

[9664] SenselR.exe "OfflineSenseIR" "4172" "eyJDb211YW5kSWQ/OiILCjE3dubG9hZEEZpbGVBY3Rpb25..."

[6280] powershell.exe -ExecutionPolicy Bypass -NoProfile -NonInteractive -Command "& (\$Output..."

File create

PS1 File Found Medium New Detected

File modify

PS1 File Found Medium New Detected

Details

PS1 File Found

Medium New

[See in timeline](#) [Link to another incident](#)

Status

New

Classification

Select classification...

Alert details

Incident

PS1 File Found on one endpoint ([open in Microsoft 365 Defender](#))

Detection source

Custom detection

Category

Execution

First activity

Jan 11, 2021, 2:52:44 PM

Last activity

Jan 11, 2021, 3:26:43 PM

Generated on

Jan 11, 2021, 3:04:17 PM

Assigned to

jack@gmfta.com

Alert description

- 7) Now repeat the above steps, but instead Isolate the machine. You should see that the machine is isolated in the defender security centre portal.

Action center

Close

Device isolation

Submission time

Status

Jan 12, 2021, 11:27:19 AM

Device isolation pending

[Cancel action](#)

Device isolation submitted

by admin@MSDx848803.onmicrosoft.com on Jan 12, 2021, 11:27:19 AM

Isolated by admin@MSDx848803.onmicrosoft.com

Congratulations! You have now successfully completed this lab. We hope that you found this lab, and the associated lab materials useful. We look forward to seeing what you build as a result of attending this lab!

Lab Complete.