Féidearthachtaí as Cuimse
Infinite Possibilities

MS Defender for Endpoint Workshop

Using Power Automate to isolate a machine from the network when a threat is detected in Windows Defender for Endpoint

Alan Pike **IT Security Officer**

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Workshop Outline

1. Overview
2. What you will need to have to implement this in O365
3. Tagging – automating this process
4. Roles & Device Groups
5. Power Automate setup
6. Things to be aware of

Live Demo

WDATP- Machine isolated: [redacted] - severity: Medium - Blanchardstown Device Tag

Reply | Reply All | Forward

IR

Incident Response

To Alan Pike; [redacted]

Sun 20/02/2022 13:39

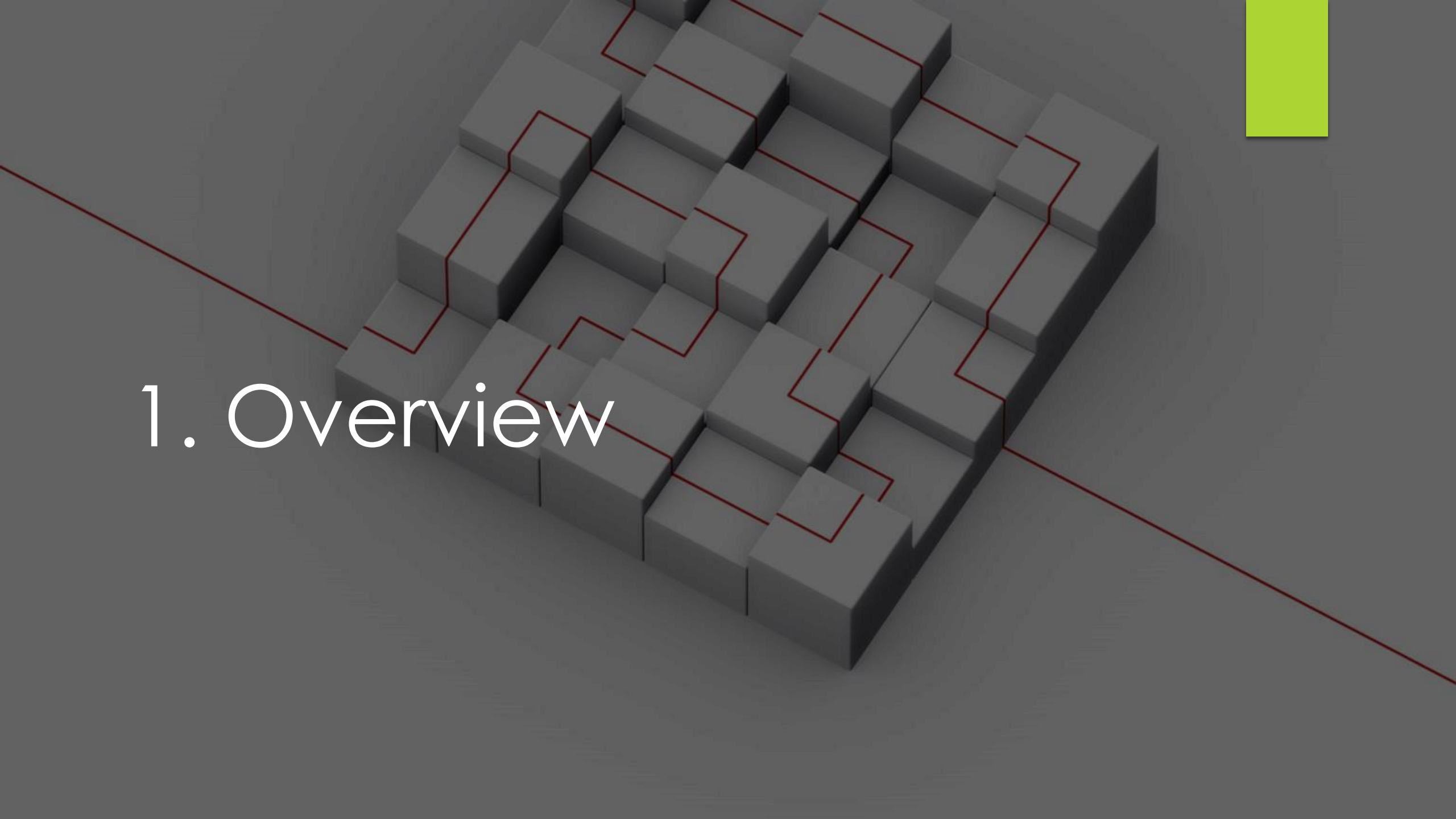
This message was sent with Low importance.

This is to notify that the machine [redacted]) is isolated by WDATP due to a Medium severity alert. This device is tagged as a Blanchardstown Campus Device within the Defender portal

Device Information:

OS Platform: Windows10
OS Version:
Machine Last IP address: 192.168.0.9
Last External IP: 78.17.[redacted]
Machine Risk Score: Informational
Machine Health Status: Active

Alert Information:
Alert Status: New
Alert Title: 'Conti' ransomware was detected
Alert Classificaiton:
Alert Description: Ransomware use common methods to encrypt files using keys that are known only to attackers. As a result, victims are unable to access the contents of the encrypted files. Most ransomware display or drop a ransom note—an image or an HTML file that contains information about how to obtain the attacker-supplied decryption tool for a fee. To target documents or other files that contain user data, some ransomware look for files in certain locations and files with certain extension names. It is also common for ransomware to rename encrypted files so that they all use the same extension name. This detection might indicate that the malware was stopped from delivering its payload. However, it is prudent to check the machine for signs of infection.
Alert Category: Ransomware
Alert Threat Family Name: Conti
Alert Detection Source: WindowsDefenderAv



1. Overview

Overview

Over 7300 Windows Devices

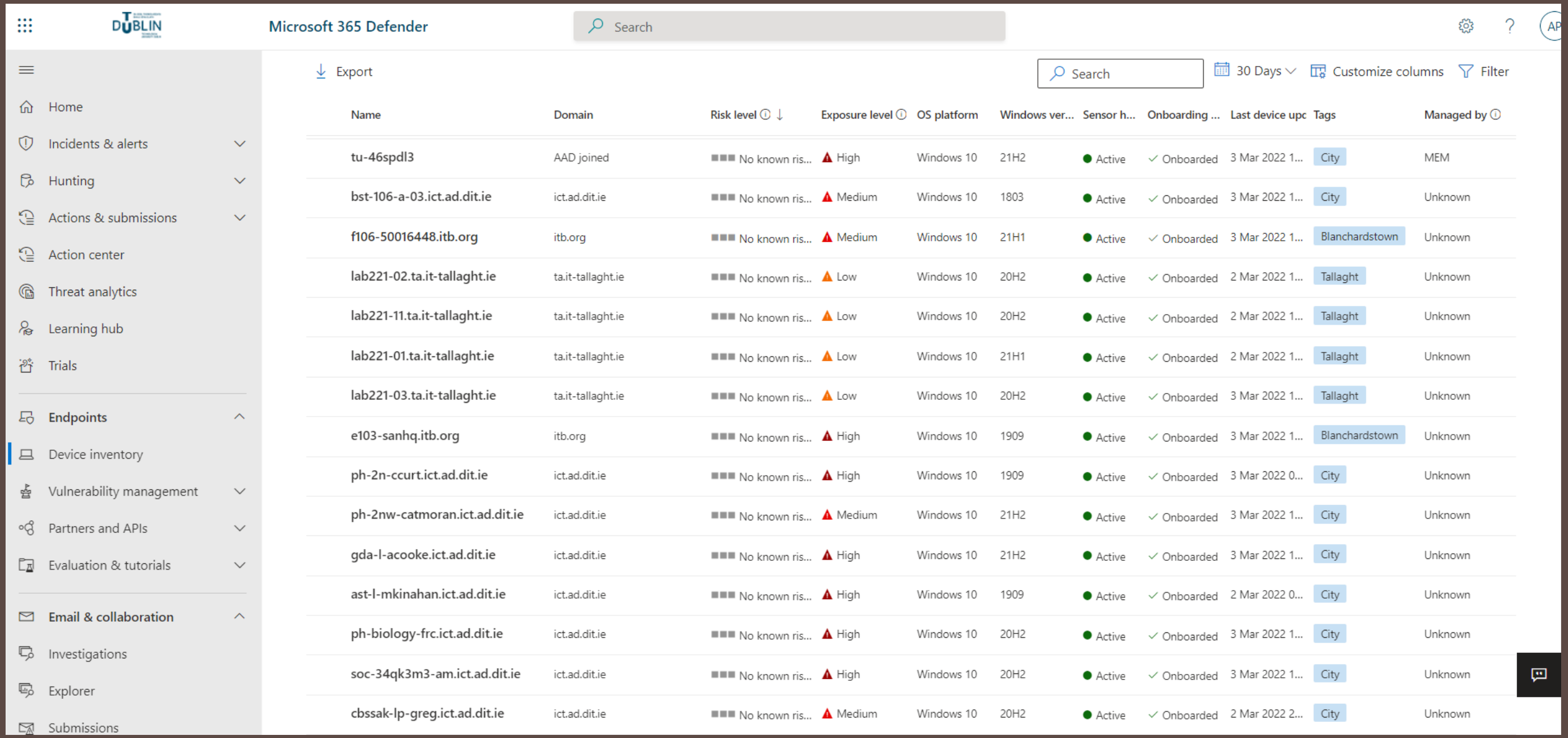
3 Campuses with 3 helpdesks

Automatically tag devices

Domain Joined & Intuned devices

Notify relevant helpdesk

Isolate devices based on Alert Severity


Microsoft 365 Defender
Search
Export
Search
30 Days
Customize columns
Filter
Home
Incidents & alerts
Hunting
Actions & submissions
Action center
Threat analytics
Learning hub
Trials
Endpoints
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Email & collaboration
Investigations
Explorer
Submissions
Name | Domain | Risk level | Exposure level | OS platform | Windows ver... | Sensor h... | Onboarding ... | Last device upc | Tags | Managed by
tu-46spdl3 | AAD joined | No known ris... | High | Windows 10 | 21H2 | Active | Onboarded | 3 Mar 2022 1... | City | MEM
bst-106-a-03.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | Medium | Windows 10 | 1803 | Active | Onboarded | 3 Mar 2022 1... | City | Unknown
f106-50016448.itb.org | itb.org | No known ris... | Medium | Windows 10 | 21H1 | Active | Onboarded | 3 Mar 2022 1... | Blanchardstown | Unknown
lab221-02.ta.it-tallaght.ie | ta.it-tallaght.ie | No known ris... | Low | Windows 10 | 20H2 | Active | Onboarded | 2 Mar 2022 1... | Tallaght | Unknown
lab221-11.ta.it-tallaght.ie | ta.it-tallaght.ie | No known ris... | Low | Windows 10 | 20H2 | Active | Onboarded | 2 Mar 2022 1... | Tallaght | Unknown
lab221-01.ta.it-tallaght.ie | ta.it-tallaght.ie | No known ris... | Low | Windows 10 | 21H1 | Active | Onboarded | 2 Mar 2022 1... | Tallaght | Unknown
lab221-03.ta.it-tallaght.ie | ta.it-tallaght.ie | No known ris... | Low | Windows 10 | 20H2 | Active | Onboarded | 3 Mar 2022 1... | Tallaght | Unknown
e103-sanhq.itb.org | itb.org | No known ris... | High | Windows 10 | 1909 | Active | Onboarded | 3 Mar 2022 1... | Blanchardstown | Unknown
ph-2n-ccurt.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | High | Windows 10 | 1909 | Active | Onboarded | 3 Mar 2022 0... | City | Unknown
ph-2nw-catmoran.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | Medium | Windows 10 | 21H2 | Active | Onboarded | 3 Mar 2022 1... | City | Unknown
gda-l-acooke.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | High | Windows 10 | 21H2 | Active | Onboarded | 3 Mar 2022 1... | City | Unknown
ast-l-mkinahan.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | High | Windows 10 | 1909 | Active | Onboarded | 2 Mar 2022 0... | City | Unknown
ph-biology-frc.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | High | Windows 10 | 20H2 | Active | Onboarded | 3 Mar 2022 1... | City | Unknown
soc-34qk3m3-am.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | High | Windows 10 | 20H2 | Active | Onboarded | 3 Mar 2022 1... | City | Unknown
cbssak-lp-greg.ict.ad.dit.ie | ict.ad.dit.ie | No known ris... | Medium | Windows 10 | 20H2 | Active | Onboarded | 2 Mar 2022 2... | City | Unknown

Search > Devices > tu-4k0kp73

tu-4k0kp73

No known risks · Active · Data sensitivity:TU Dublin... · City

Manage tags · Go hunt · Isolate device · Restrict app execution · ...

Device summary

Tags

Data sensitivity:TU Dublin... · City

Security Info

Open incidents
0

Active alerts
0

Exposure level
Medium

Risk level
None

Overview · Alerts · Timeline · Security recommendations · Software inventory · ...

Active alerts

180 days

Risk level: No known risks

We don't see new malicious activity on this device

Security assessments

Exposure level: Medium

65 active security recommendations

Discovered vulnerabilities (197)

Critical (1) · High (86) · Medium (108) · Low (2)

See all recommendations

Logged on users

30 days

1 logged on user

Most frequent: alan.pike

Least frequent: alan.pike

See all users

Search > Devices > tu-4k0kp73

tu-4k0kp73

No known risks · Active · Data sensitivity:TU Dublin... · City

Manage tags · Go hunt · Isolate device · Restrict app execution · ...

Device summary

Tags

Data sensitivity:TU Dublin... · City

Security Info

Open incidents
0

Active alerts
0

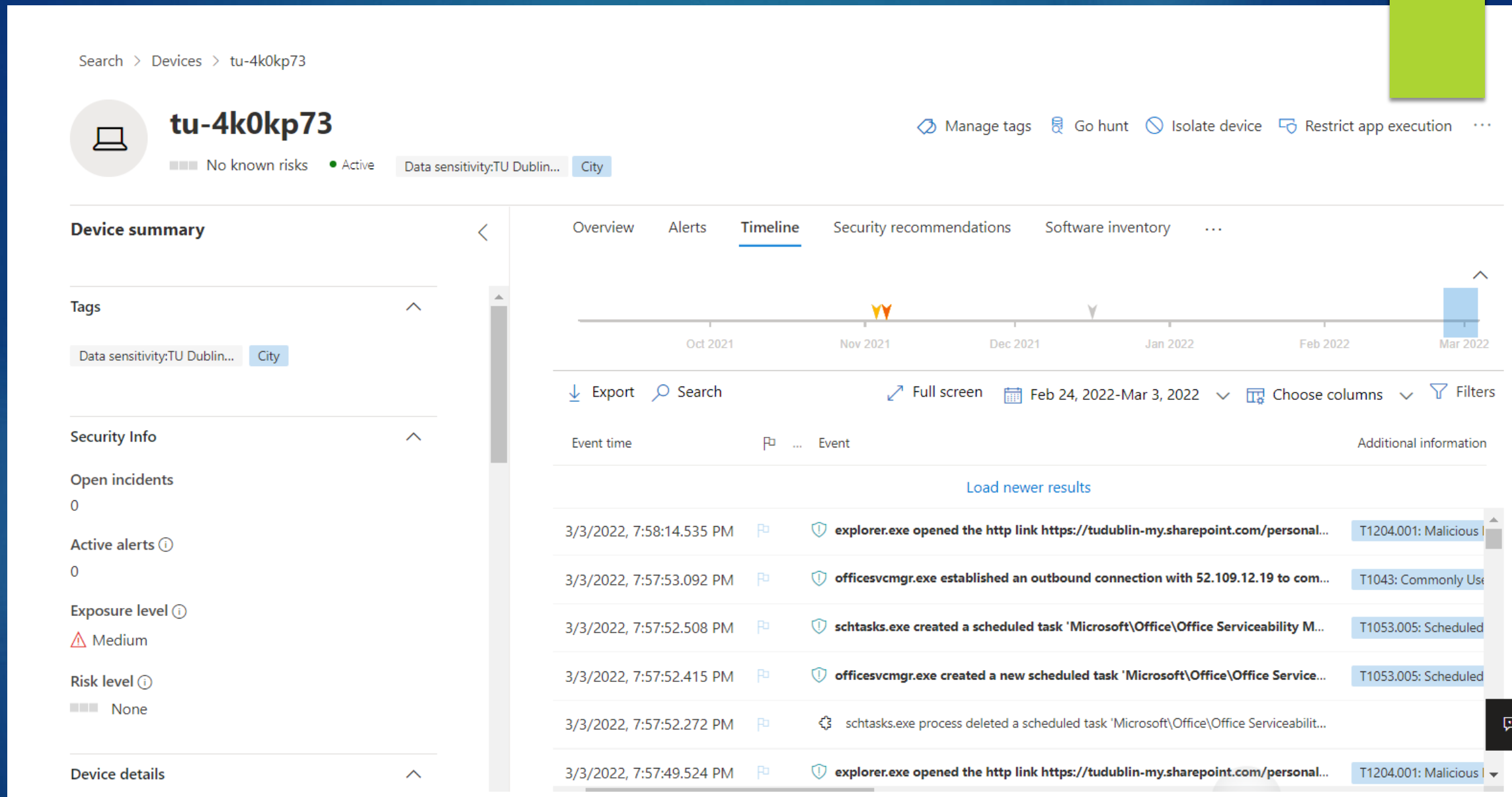
Exposure level
Medium

Risk level
None

Overview | Alerts | Timeline | Security recommendations | Software inventory | ...

Page 1 · Choose columns · 30 items per page · Filters

Title	Ta...	Severity	Status	Linked by	Category
'Phonzy' malware was prevented		Informational...	Resolved		Malware
'CVE-2015-5122' exploit malware was prevented		Low	Resolved		Exploit
'ShellCode' exploit malware was prevented		Low	Resolved		Exploit
'Aicat' exploit malware was prevented		Low	Resolved		Exploit
'CVE-2014-0515' exploit malware was prevented		Low	Resolved		Exploit
Meterpreter post-exploitation tool		Medium	Resolved		Suspicious acti
'Obfuscator' hacktool was prevented		Low	Resolved		Malware
'Pklotide' malware was prevented		Informational...	Resolved		Malware



Search > Devices > tu-4k0kp73

tu-4k0kp73

No known risks · Active · Data sensitivity:TU Dublin... · City

Manage tags · Go hunt · Isolate device · Restrict app execution · ...

Device summary

Tags

Data sensitivity:TU Dublin... · City

Security Info

Open incidents
0

Active alerts
0

Exposure level
Medium

Risk level
None

Overview | Alerts | Timeline | **Security recommendations** | Software inventory | ...

Export · 65 items · Search · Filter · Customize columns

Filters: Status: Active +1

Security recommendation	Weaknesses	Related component
Update Fortinet Forticlient	1	Fortinet Forticlient
Update Google Chrome	21	Google Chrome
Update Mozilla Firefox to version 97.0.1.0	174	Mozilla Firefox
Update Portswigger Burp Suite	1	Portswigger Burp Suite
Enable Automatic Updates	1	Application (Microsoft Office)
Enable 'Hide Option to Enable or Disable Updates'	1	Application (Microsoft Office)
Disable 'Continue running background apps when Google Chrome is closed'	1	Application (Google Chrome)
Turn on Microsoft Defender Application Guard managed mode	1	Security controls (Application Guard)

Severity

Alert severity	Description
High (Red)	Alerts commonly seen associated with advanced persistent threats (APT). These alerts indicate a high risk because of the severity of damage they can inflict on devices. Some examples are: credential theft tools activities, ransomware activities not associated with any group, tampering with security sensors, or any malicious activities indicative of a human adversary.
Medium (Orange)	Alerts from endpoint detection and response post-breach behaviors that might be a part of an advanced persistent threat (APT). This includes observed behaviors typical of attack stages, anomalous registry change, execution of suspicious files, and so forth. Although some might be part of internal security testing, it requires investigation as it might also be a part of an advanced attack.
Low (Yellow)	Alerts on threats associated with prevalent malware. For example, hack-tools, non-malware hack tools, such as running exploration commands, clearing logs, etc., that often do not indicate an advanced threat targeting the organization. It could also come from an isolated security tool testing by a user in your organization.
Informational (Grey)	Alerts that might not be considered harmful to the network but can drive organizational security awareness on potential security issues.

High (Red)	Alerts commonly seen associated with advanced persistent threats (APT). These alerts indicate a high risk because of the severity of damage they can inflict on devices. Some examples are: credential theft tools activities, ransomware activities not associated with any group, tampering with security sensors, or any malicious activities indicative of a human adversary.
Medium (Orange)	Alerts from endpoint detection and response post-breach behaviors that might be a part of an advanced persistent threat (APT). This includes observed behaviors typical of attack stages, anomalous registry change, execution of suspicious files, and so forth. Although some might be part of internal security testing, it requires investigation as it might also be a part of an advanced attack.

High (Red)	Alerts commonly seen associated with advanced persistent threats (APT). These alerts indicate a high risk because of the severity of damage they can inflict on devices. Some examples are: credential theft tools activities, ransomware activities not associated with any group, tampering with security sensors, or any malicious activities indicative of a human adversary.
Medium (Orange)	Alerts from endpoint detection and response post-breach behaviors that might be a part of an advanced persistent threat (APT). This includes observed behaviors typical of attack stages, anomalous registry change, execution of suspicious files, and so forth. Although some might be part of internal security testing, it requires investigation as it might also be a part of an advanced attack.

Defender will block most threats, isolation gives us ability to prevent the spread of malware or the ability of threat actors to move laterally

Tagging is important as it allows more granular actions depending on tag and actions within powerautomate

This does not require a SIEM.

2. What you will need to implement this in O365

What you will need

- All users to have an A5/E5 license
  - Or
- Defender for Endpoint Plan 2 * (see next slide)

- All devices onboarded into Defender for Endpoint
- Tagging in place on all devices
  - An Azure app with the appropriate level of permission on the Graph API to apply tagging to devices
- Powerautomate script in place, along with another App in place to initiate the isolation of devices* (can be the same as the app above)

Defender for Endpoint Plan 1 vs Plan 2

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL blocking	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
API's, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts **		✓

3. Tagging

Different methods to apply tags to devices in Defender for Endpoint:

- Manually tag via the Defender portal
- Apply tags via group policy
- Apply tags using SCCM (for domain joined devices)
- Apply tags using a PowerShell script from an Azure automation account

Different methods to apply tags to devices in Defender for Endpoint:

- **Manually tag via the Defender portal**
- Apply tags via group policy
- Apply tags using SCCM (for domain joined devices)
- Apply tags using a PowerShell script from an Azure automation account

workshop-pc-vm-01

Informational · Active · Data sensitivity:null

Manage tags | Go hunt | Isolate device | ...

Device summary

This device has a configuration enforcement error:
Windows version is outdated, update the device with latest security fixes.

Tags

Data sensitivity:null

Security Info

Open incidents
1

Active alerts
1

Overview | Alerts | Timeline | Security recommendations | ...

Active alerts
180 days

Risk level: Informational

1 active alert in 1 incident

Informational (1)

Security assessments

Exposure level: High

57 active security recommendations

Discovered vulnerabilities (304)

Critical (5) High (216) Medium (83)

See all recommendations

Logged on users
30 days

1 logged on user

Most frequent: hea.user1

Least frequent: hea.user1

See all users

Different methods to apply tags to devices in Defender for Endpoint:

- Manually tag via the Defender portal
- **Apply tags via group policy**
- **Apply tags using SCCM (for domain joined devices)**
- Apply tags using a PowerShell script from an Azure automation account

- **Apply tags via group policy**
- Machine will need line of sight of a Domain controller to have this tag applied

- **Apply tags using SCCM (for domain joined devices)**
- Device will need to have visibility of SCCM if pushing a script or compliance baseline to apply tag

Different methods to apply tags to devices in Defender for Endpoint:

- Manually tag via the Defender portal
- Apply tags via group policy
- Apply tags using SCCM (for domain joined devices)
- **Apply tags using a PowerShell script from an Azure automation account**

Apply tags using a PowerShell script from an Azure automation account

This script looks at the device groups in place on your Defender portal.

If a machine appears in a dynamic device group, it will have an appropriate tag applied

The order/rank of the groups is important

Device Groups in TU Dublin

Organize devices into groups, set automated remediation levels, and assign administrators.

+ Add device group

Rank ↓	Device group	Devices	Remediation level
1	Tagged-City	7550	Full - remediate threats automatically
2	Tagged-BN	1403	Full - remediate threats automatically
3	Tagged-TA	999	Full - remediate threats automatically
4	City Devices (Domain Joined)	8	Full - remediate threats automatically
5	Blanchardstown Devices (Domain Joined)	0	Full - remediate threats automatically
6	Tallaght Devices (Domain Joined)	0	Full - remediate threats automatically
7	Intune laptops	294	Full - remediate threats automatically
Last	Ungrouped devices (default)	13172	Full - remediate threats automatically

Device Groups in TU Dublin

Organize devices into groups, set automated remediation levels, and assign administrators.

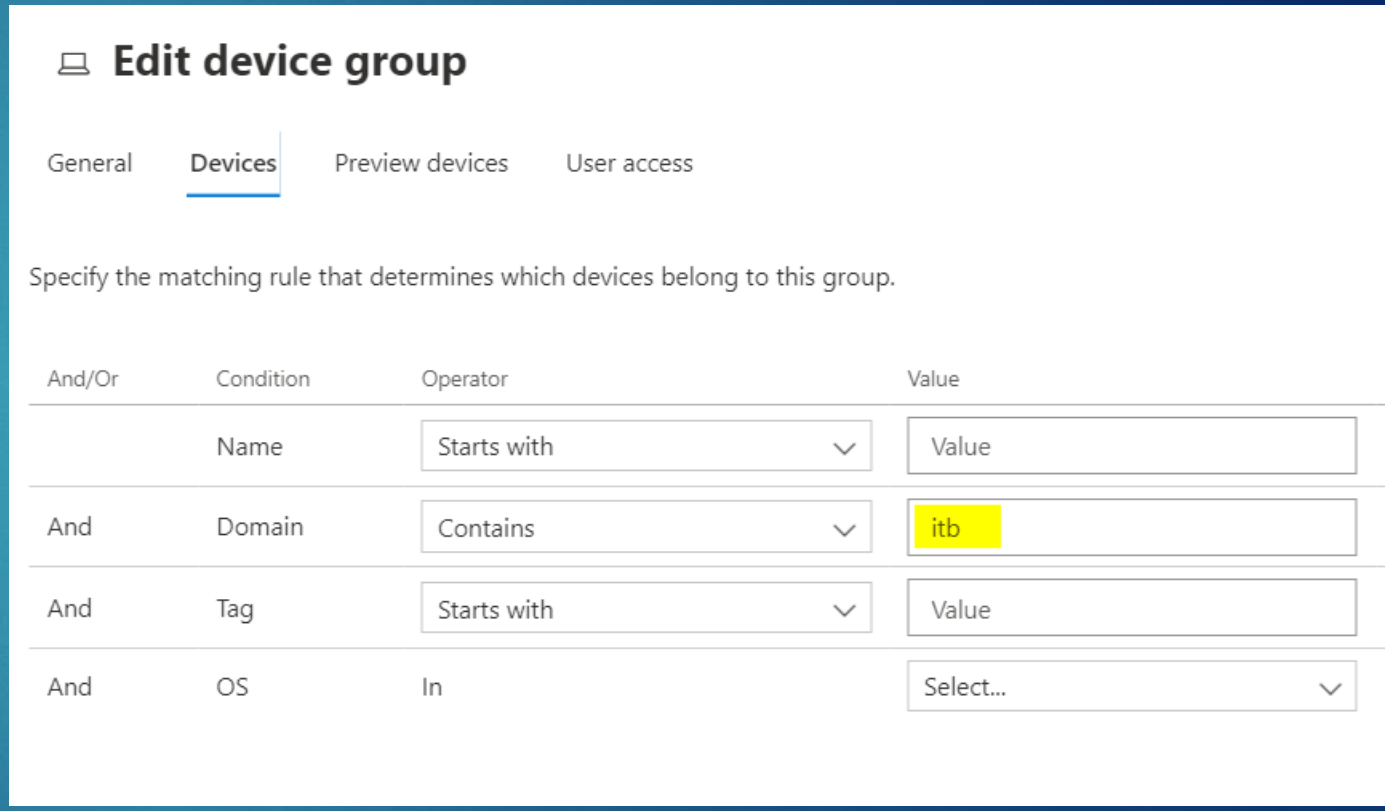
+ Add device group

Rank ↓	Device group	Devices	Remediation level
1	Tagged-City	7550	Full - remediate threats automatically
2	Tagged-BN	1403	Full - remediate threats automatically
3	Tagged-TA	999	Full - remediate threats automatically
4	City Devices (Domain Joined)	8	Full - remediate threats automatically
5	Blanchardstown Devices (Domain Joined)	0	Full - remediate threats automatically
6	Tallaght Devices (Domain Joined)	0	Full - remediate threats automatically
7	Intune laptops	294	Full - remediate threats automatically
Last	Ungrouped devices (default)	13172	Full - remediate threats automatically

Apply tags using a PowerShell script from an Azure automation account

We use a dynamic query to check for the domain name of the device.

If a new machine is domain joined in Blanchardstown, it will appear in this group



Apply tags using a PowerShell script from an Azure automation account

- Script is in place to run every evening from Azure automation account
- PowerShell script will apply a “Blanchardstown” tag to any devices found in this group
- This is where the rank/order of the groups comes into play

Apply tags using a PowerShell script from an Azure automation account

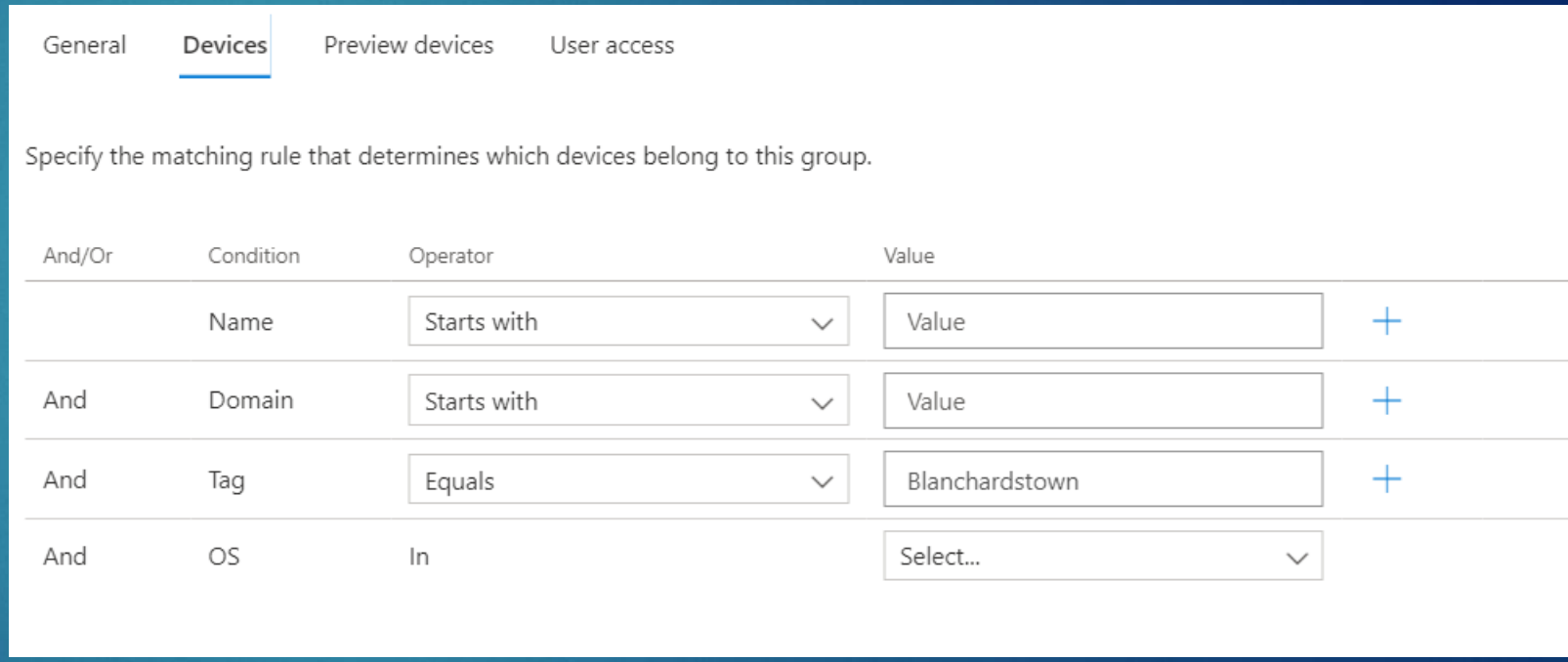
Rank ↓	Device group	Devices	Remediation level
1	Tagged-City	7550	Full - remediate threats automatically
2	Tagged-BN	1403	Full - remediate threats automatically
3	Tagged-TA	999	Full - remediate threats automatically
4	City Devices (Domain Joined)	8	Full - remediate threats automatically
5	Blanchardstown Devices (Domain Joined)	0	Full - remediate threats automatically
6	Tallaght Devices (Domain Joined)	0	Full - remediate threats automatically
7	Intune laptops	294	Full - remediate threats automatically
Last	Ungrouped devices (default)	13172	Full - remediate threats automatically

Apply tags using a PowerShell script from an Azure automation account

Rank ↓	Device group	Devices	Remediation level
1	Tagged-City	7550	Full - remediate threats automatically
2	Tagged-BN	1403	Full - remediate threats automatically
3	Tagged-TA	999	Full - remediate threats automatically
4	City Devices (Domain Joined)	8	Full - remediate threats automatically
5	Blanchardstown Devices (Domain Joined)	0	Full - remediate threats automatically
6	Tallaght Devices (Domain Joined)	0	Full - remediate threats automatically
7	Intune laptops	294	Full - remediate threats automatically
Last	Ungrouped devices (default)	13172	Full - remediate threats automatically

Apply tags using a PowerShell script from an Azure automation account

Tagged-BN uses the following rule to determine which devices belong to this group



Apply tags using a PowerShell script from an Azure automation account

These groups are delegated out to the various IT staff within the 3 campuses (using Roles)

For example, only IT staff within City can view devices tagged with the "City" tag

We can also use these tags in the powerautomate script to determine where alerts are sent

Rank ↓	Device group	Devices
1	Tagged-City	7550
2	Tagged-BN	1403
3	Tagged-TA	999

Apply tags using a PowerShell script from an Azure automation account

This is fairly straight forward for domain joined devices, as we can specify the name of the domain the machine is a member of, which will dynamically add them to a device group

Script runs in the evening, device is tagged accordingly.

Device is then moved to one of the 3 “tagged groups”

Apply tags using a PowerShell script from an Azure automation account

But…what about intuned devices?
These are not in a specific domain

Rank ↓	Device group	Devices	Remediation level	Descr...
1	Tagged-City	7768	Full - remediate threats automatically	
2	Tagged-BN	1510	Full - remediate threats automatically	
3	Tagged-TA	1100	Full - remediate threats automatically	
4	City Devices (Domain Joined)	13	Full - remediate threats automatically	City Cam...
5	Blanchardstown Devices (Do...	1	Full - remediate threats automatically	blanchar...
6	Tallaght Devices (Domain Joi...	0	Full - remediate threats automatically	Tallaght ...
7	Intune laptops	342	Full - remediate threats automatically	Intune la...
Last	Ungrouped devices (default)	13490	Full - remediate threats automatically	Devices t...

Apply tags using a PowerShell script from an Azure automation account

Within Azure, each intuned device will appear as a device listed against a particular user.

When a user signs in (whether it be autopiloted device or manually joined to intune), the device is registered under their own account

In TUDublin, all users a directory sync'd from 1 of 3 on prem AD forests

We populate a number of attributes for each user, which allows us to make dynamic user groups, based on where the users on-prem AD account is sync'd from

Apply tags using a PowerShell script from an Azure automation account

Each site in populates the CompanyName attribute (Company attribute from on prem AD) with the campus the user is located

```
City                                :
CompanyName                         : City
ConsentProvidedForMinor             :
Country                             :
CreationType                        :
Department                          : Information Services
DirSyncEnabled                      : True
DisplayName                         : Alan Pike
FacsimileTelephoneNumber            :
GivenName                           : Alan
IsCompromised                       :
```

Apply tags using a PowerShell script from an Azure automation account

The script will check devices in the "intuned devices" group that do not have a tag in place.

If these devices have been registered with a user, it will get the details of primary user of that device (e.g. Alan Pike).

Using the graph API, it will obtain the company attribute of this user (e.g. City)

It will apply this value as the tag to the device.

This ensures we have 1 groups for all devices in City, whether they be domain joined or intuned devices

Apply tags using a PowerShell script from an Azure automation account

For security reasons….

The script will connect to the Graph API using a service principal.

A secret is created in the Azure App, and this is securely stored in the automation account

Apply tags using a PowerShell script from an Azure automation account

Secure the secret of the Service principal by storing the secret as an encrypted variable

```
##CONFIG
$tenantId = "766317cb-[redacted]"
$clientId = Get-AutomationVariable -Name 'TaggingClientID'
$appsecret = Get-AutomationVariable -Name 'TaggingSecret'
```

tud-eun-p-automation-tagging | Variables

Automation Account

Search (Ctrl+/)

Process Automation

- Runbooks
- Jobs
- Hybrid worker groups
- Watcher tasks

Shared Resources

- Schedules
- Modules
- Python packages
- Credentials
- Connections
- Certificates
- Variables

Add a variable | Refresh

Search variables...

Name	Type	Value	Last modified
TaggingClientID	String	3cb7103c-	11/15/2021, 12:
TaggingSecret	Unknown (encrypted)	**********	11/15/2021, 12:

Apply tags using a PowerShell script from an Azure automation account

Script is available on github

https://github.com/alanptud/Defender_Tagging

4. Roles and Device Groups

Custom Roles

Access to Microsoft Defender for Endpoint features can be controlled by creating custom roles.
These roles define what level of access someone has within Microsoft Defender for Endpoint

Role
Microsoft Defender for Endpoint administrator (default)
Microsoft Defender for Endpoint - Read Only
Microsoft Defender for Endpoint - Alert Investigations
Microsoft Defender for Endpoint - Remediate Actions

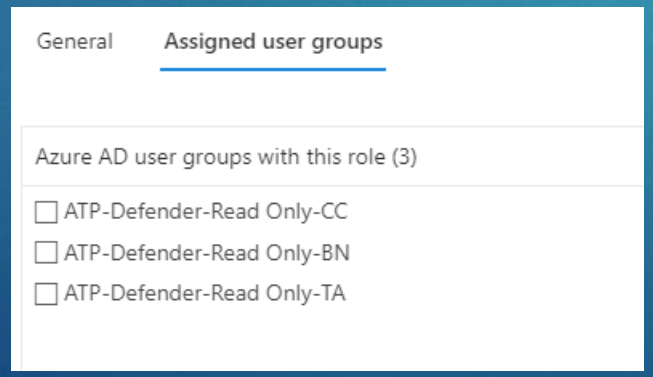
Custom Roles

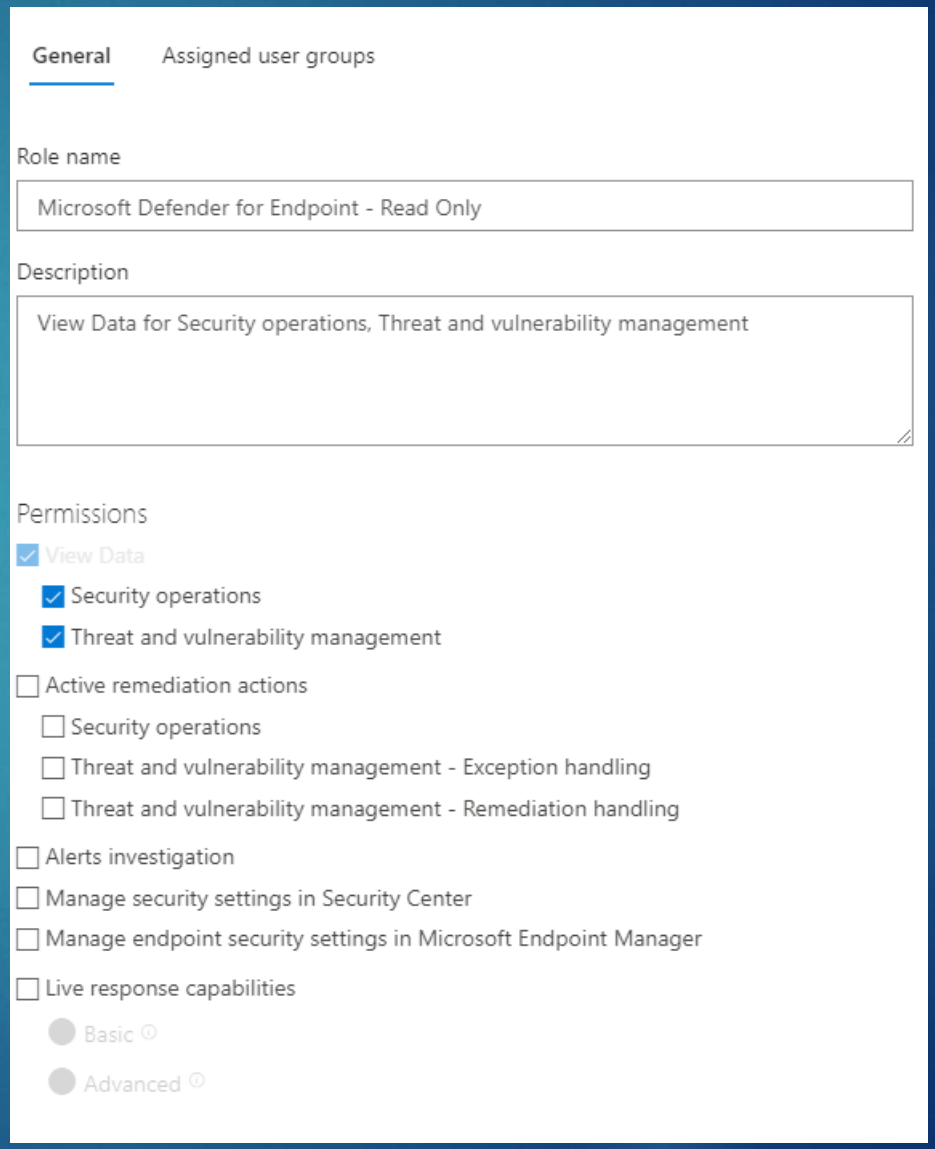
Read Only Role

Allow users to view data only

We give this to all IT staff in our organisation for their day-to-day account

Allows staff to click on a link on an email to view the alert ID (either from phone or laptop)





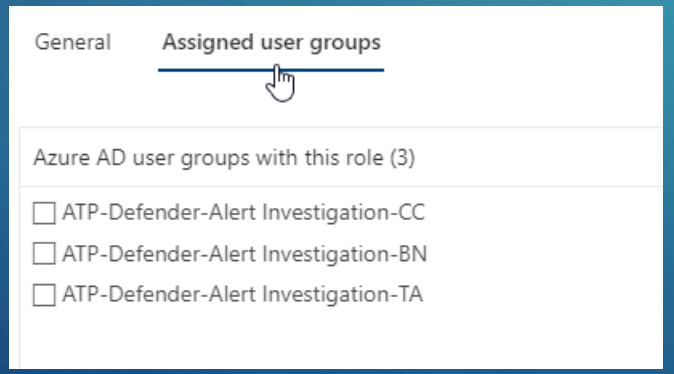
Custom Roles

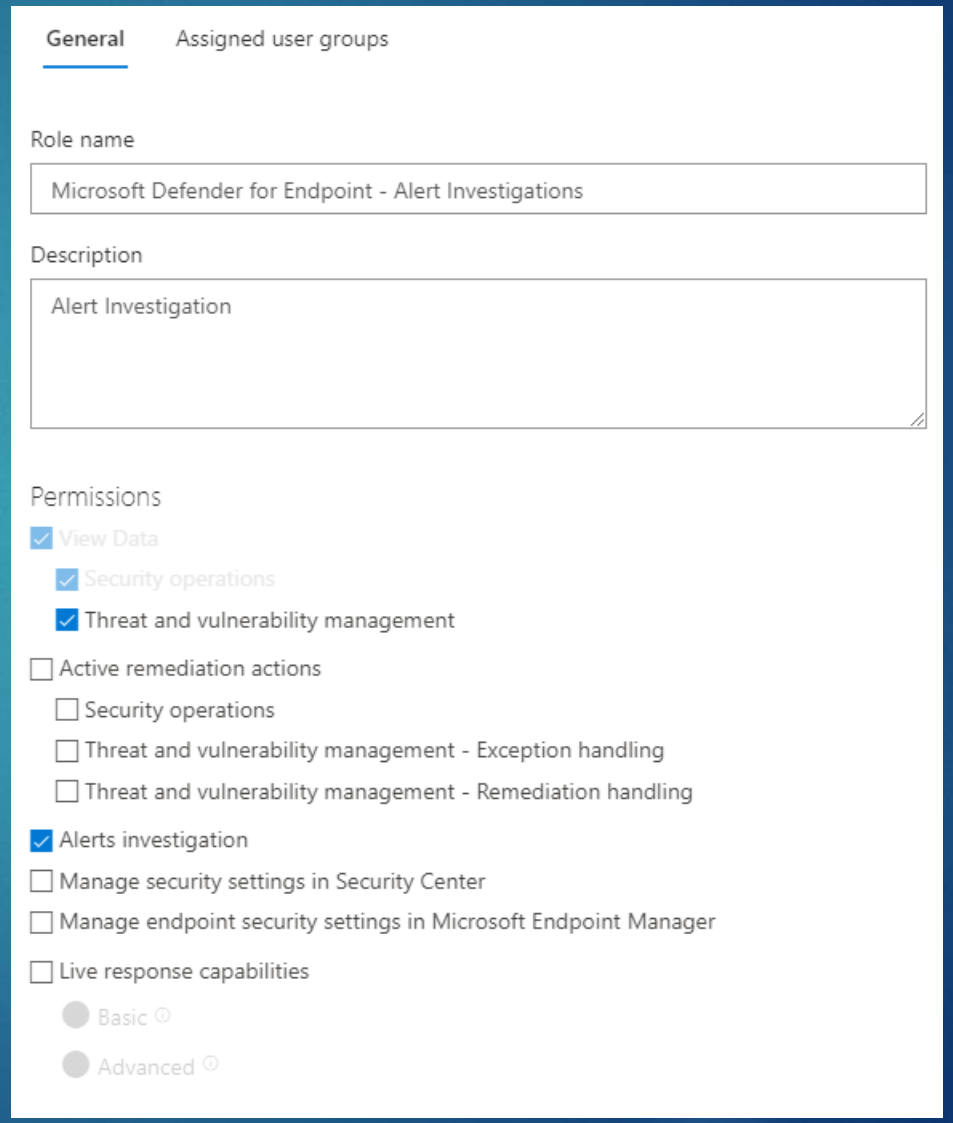
Alert Investigation Role

Includes the ability to read data

Also gives users access to manage investigations

We give this to all IT staff in our organisation, but they need to use a separate Cloud Admin account





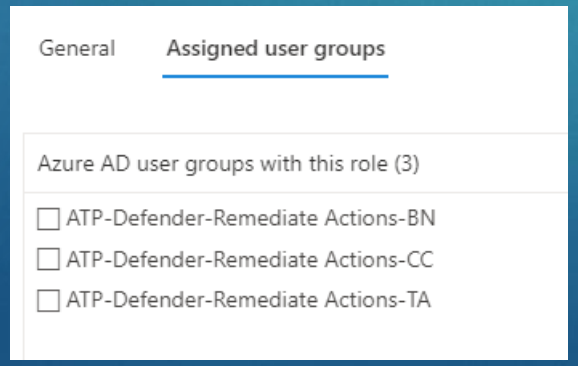
Custom Roles

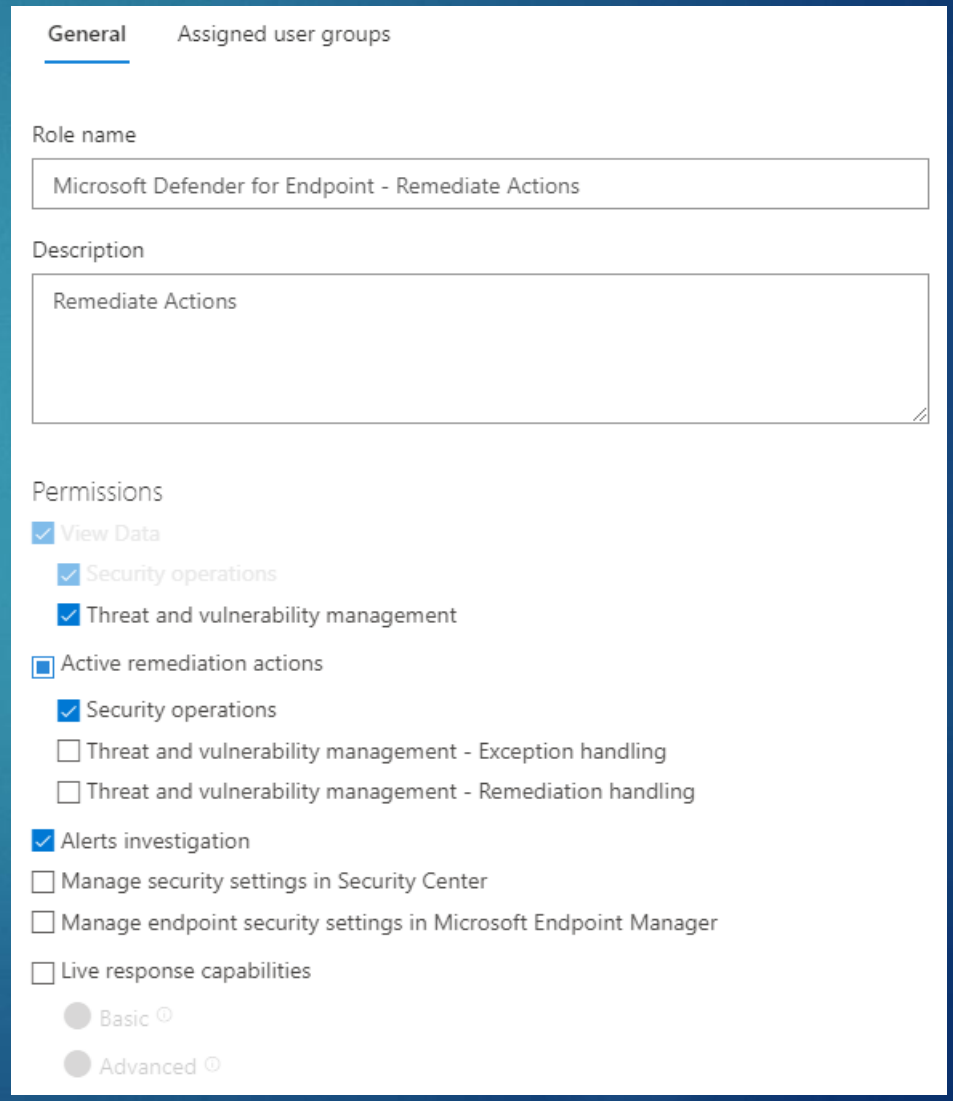
Remediate Actions

Includes the ability to read data and manage investigations

Also allows users to remediate actions, such as isolate machine, release from isolation

We give this to subset of IT staff in our organisation, also requires a separate Cloud Admin account (protected with conditional access policies)





Device Groups

Ra... ↓	Device group	Devices	Remediation level	Description
1	Tagged-City	7768	Full - remediate threats automatica...	
2	Tagged-BN	1510	Full - remediate threats automatica...	
3	Tagged-TA	1100	Full - remediate threats automatica...	
4	City Devices (Domain Joined)	0	Full - remediate threats automatica...	City Campus Domain Joined Devices
5	Blanchardstown Devices (Domain Joine...	0	Full - remediate threats automatica...	blanchardstown domains
6	Tallaght Devices (Domain Joined)	0	Full - remediate threats automatica...	Tallaght Domain Joined Devices
7	Intune laptops	343	Full - remediate threats automatica...	Intune laptops with no Tag

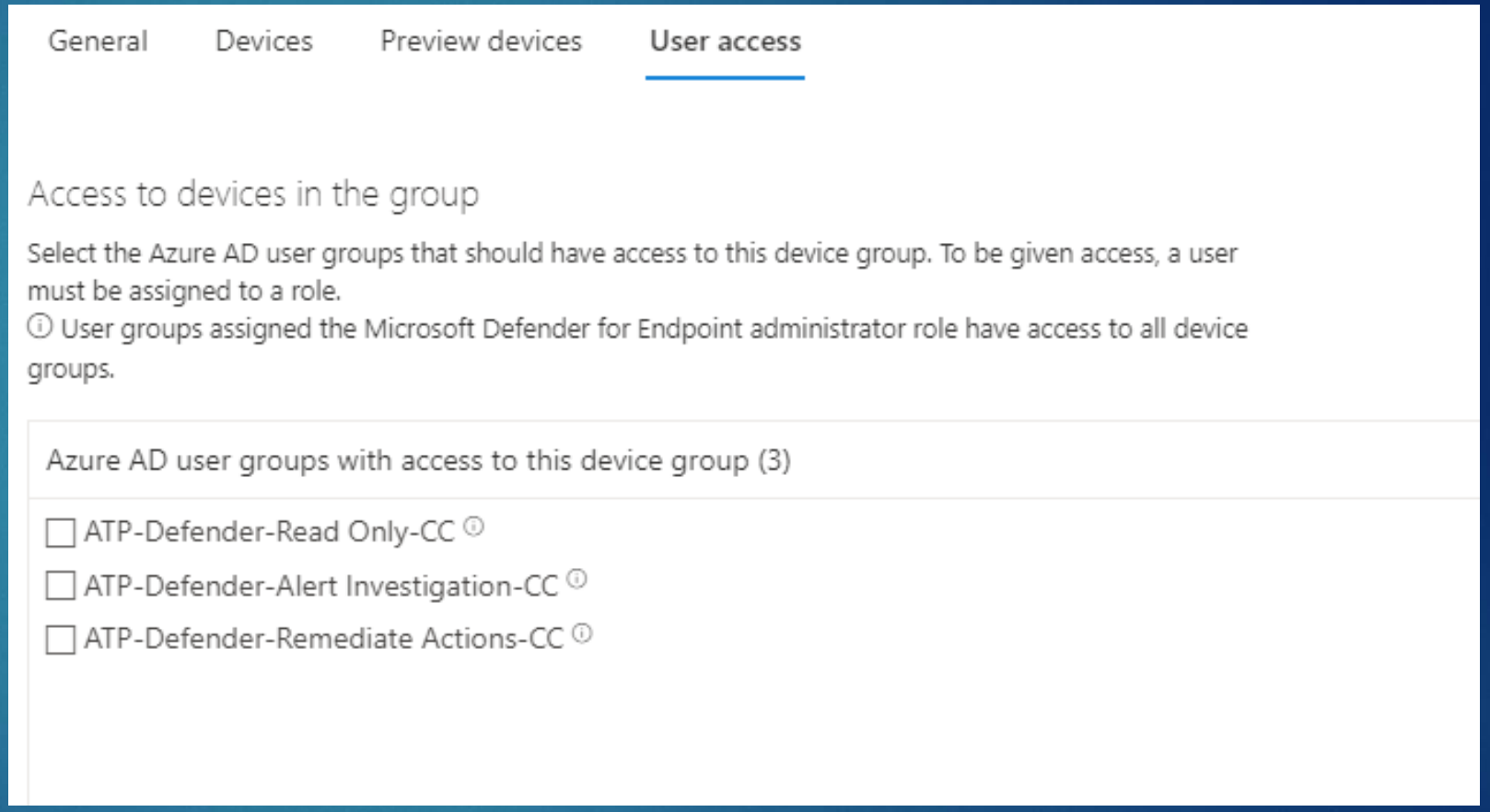
Device Groups

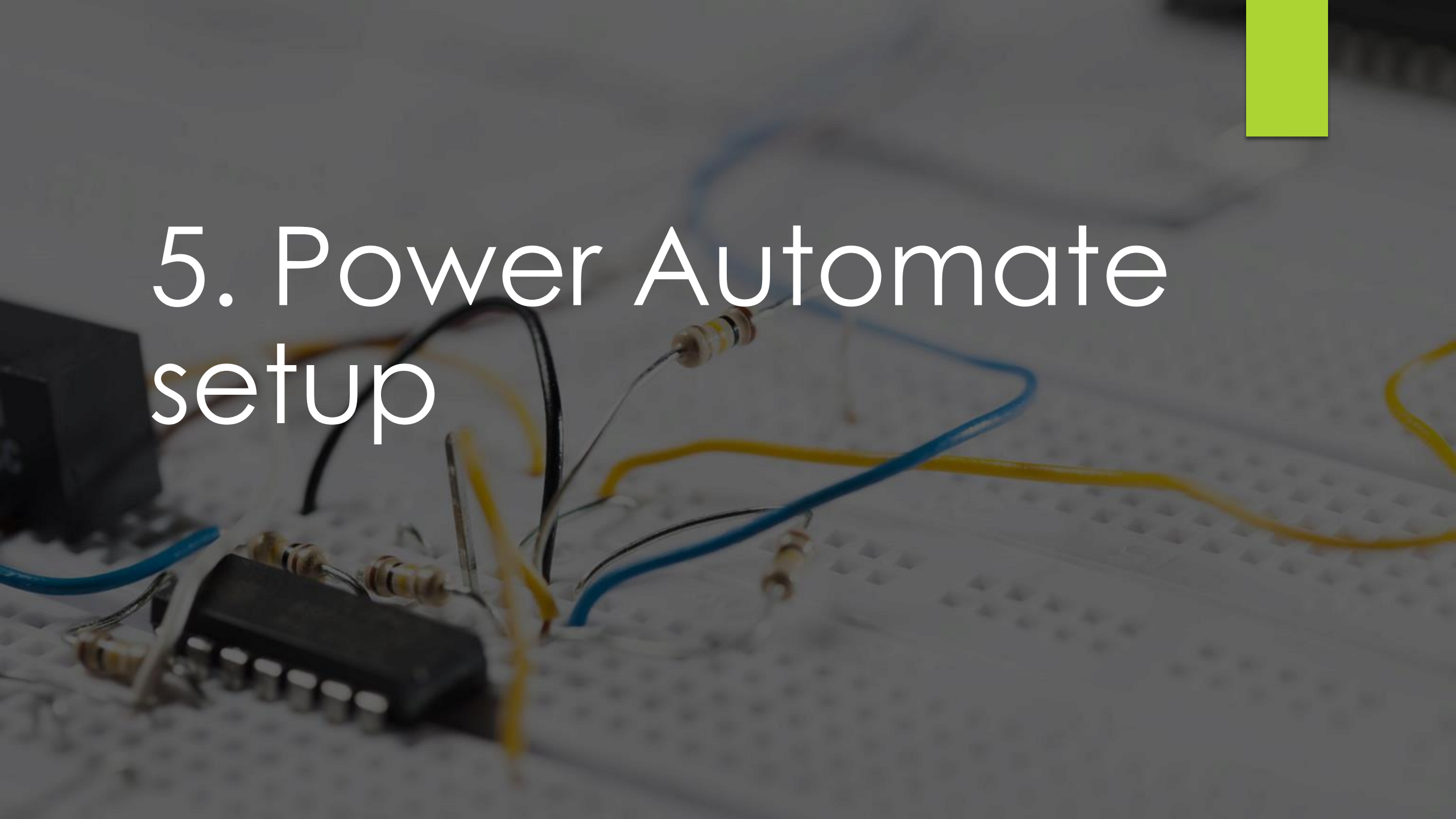
Ra... ↓	Device group	Devices	Remediation level	Description
1	Tagged-City	7768	Full - remediate threats automatica...	
2	Tagged-BN	1510	Full - remediate threats automatica...	
3	Tagged-TA	1100	Full - remediate threats automatica...	
4	City Devices (Domain Joined)	0	Full - remediate threats automatica...	City Campus Domain Joined Devices
5	Blanchardstown Devices (Domain Joine...	0	Full - remediate threats automatica...	blanchardstown domains
6	Tallaght Devices (Domain Joined)	0	Full - remediate threats automatica...	Tallaght Domain Joined Devices
7	Intune laptops	343	Full - remediate threats automatica...	Intune laptops with no Tag

Device Groups

Tagged-City Device group is only visible to users in the "CC" group (i.e. City Campus)

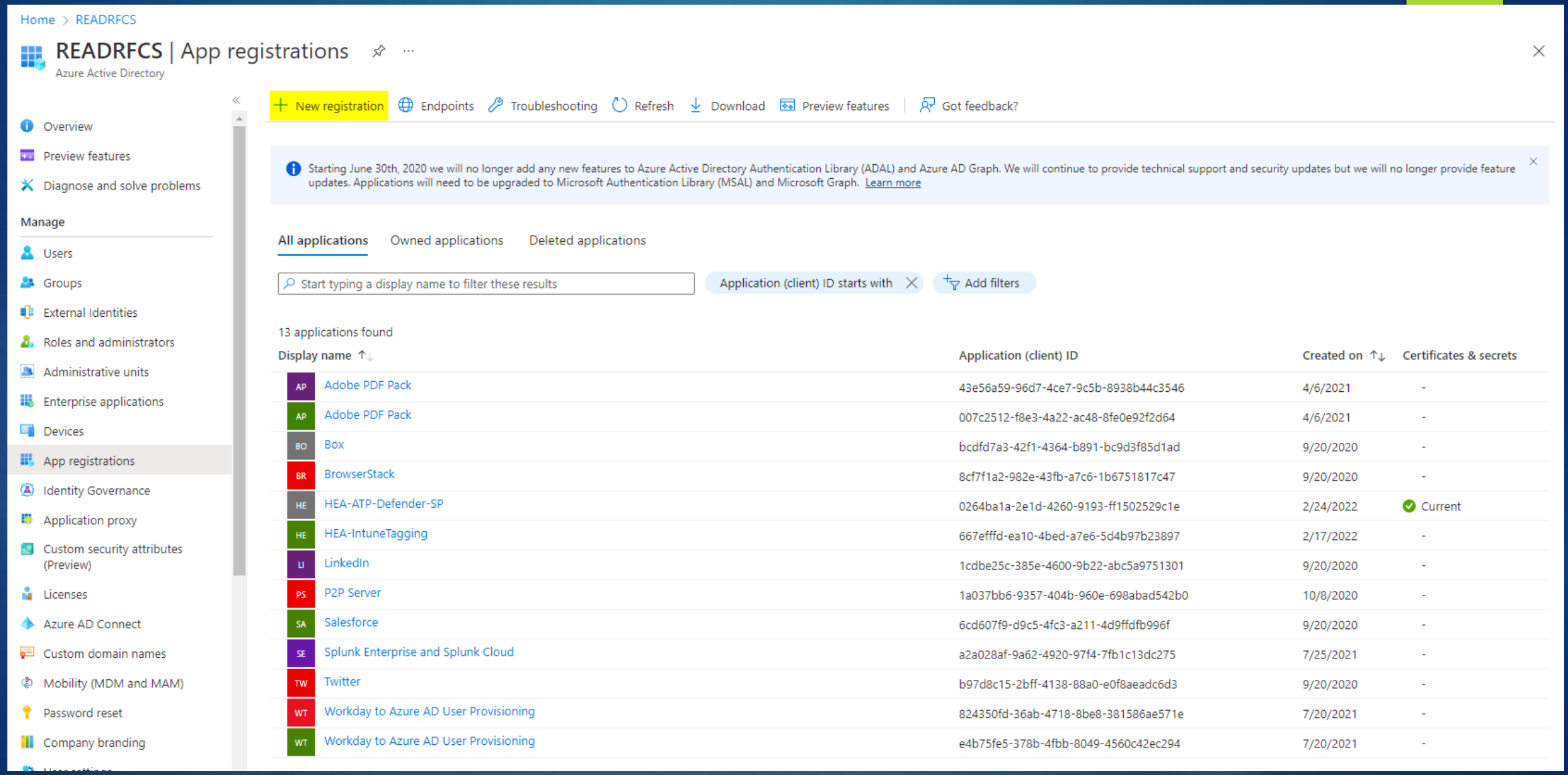
Keeps devices separate between different locations, departments, functional areas etc



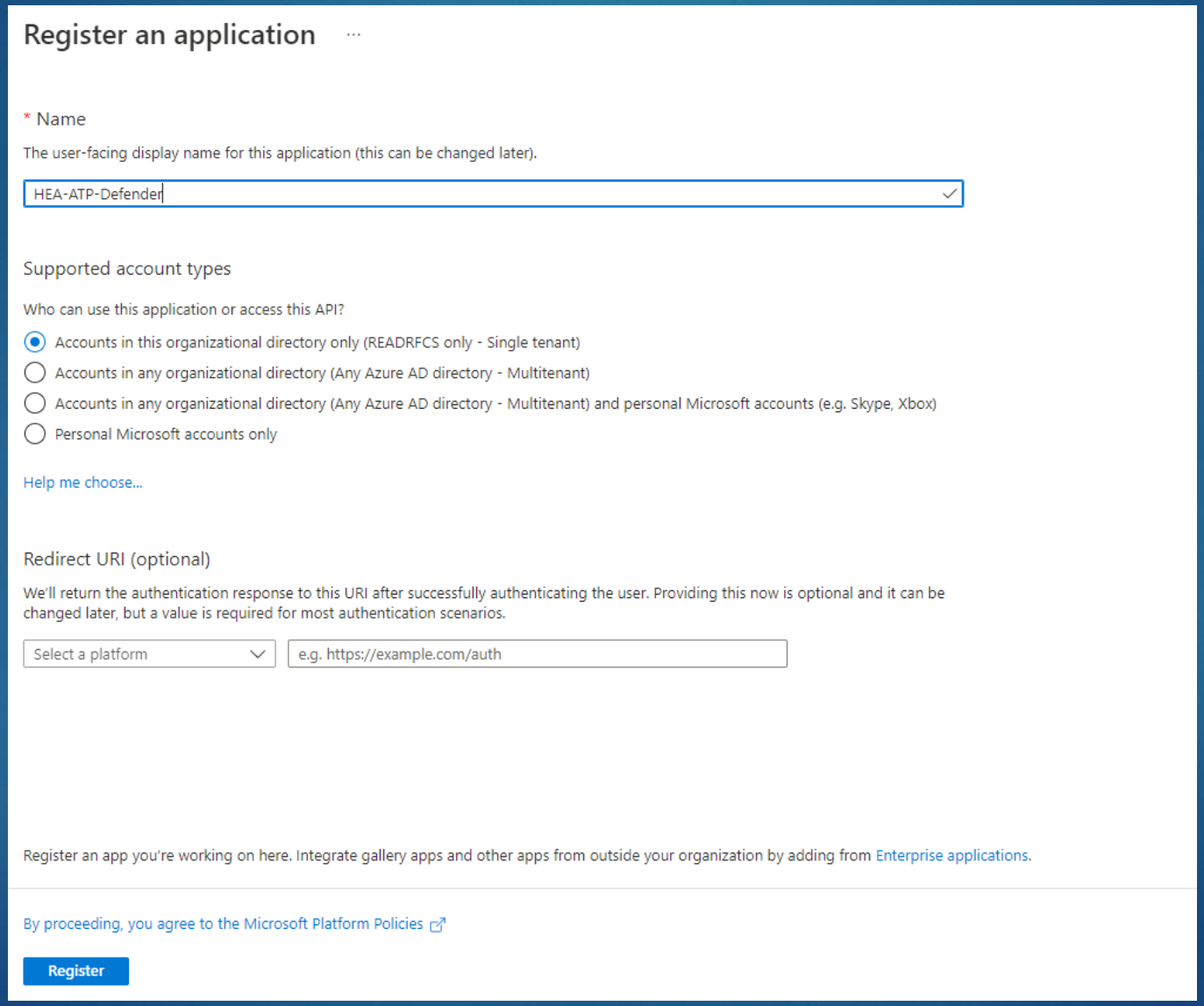


5. Power Automate setup

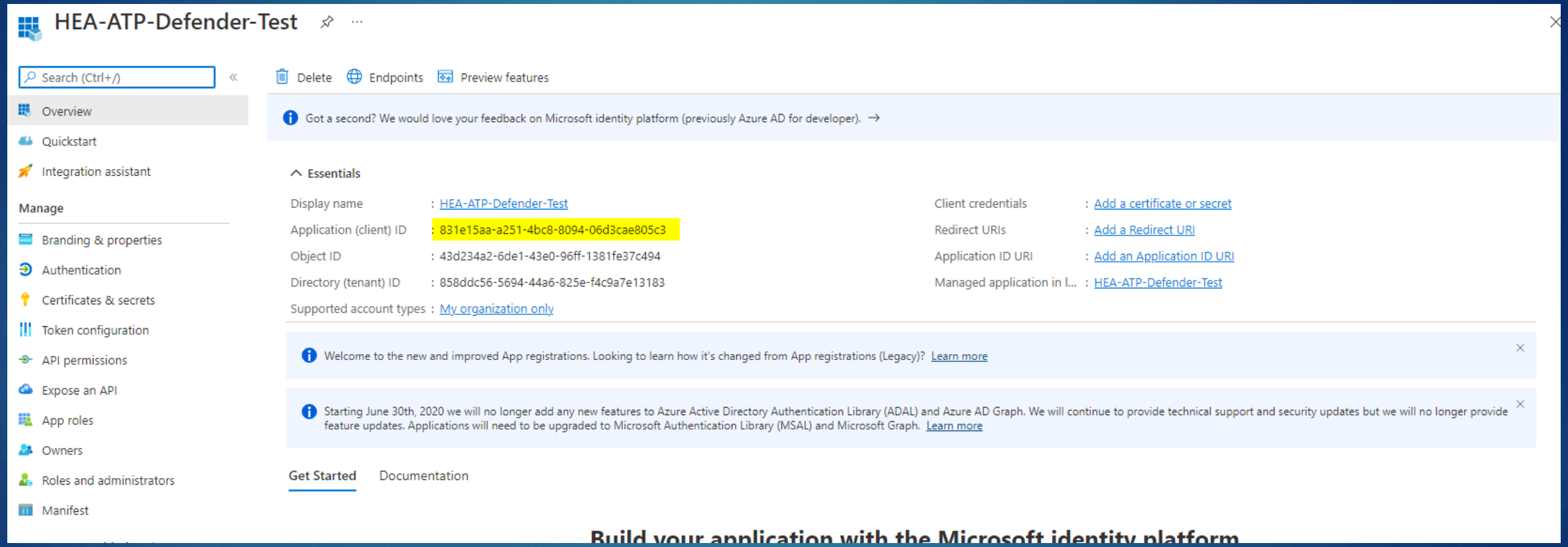
Firstly, Create an App in Azure…



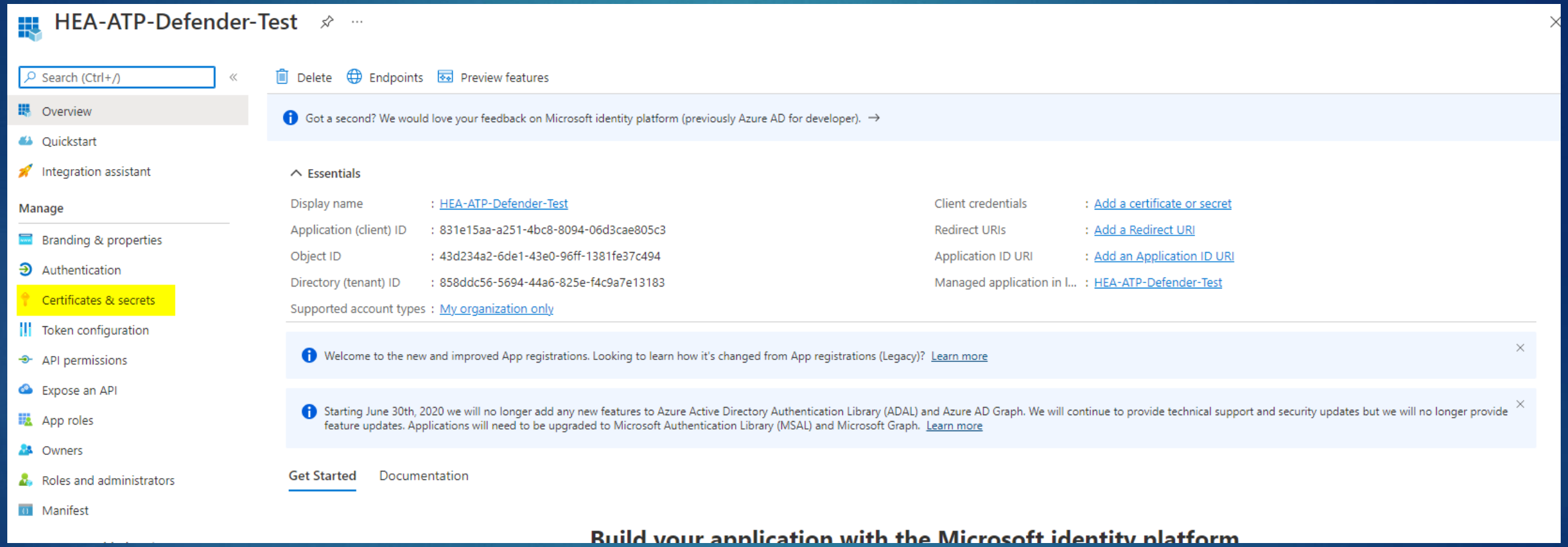
Firstly, Create an App in Azure…



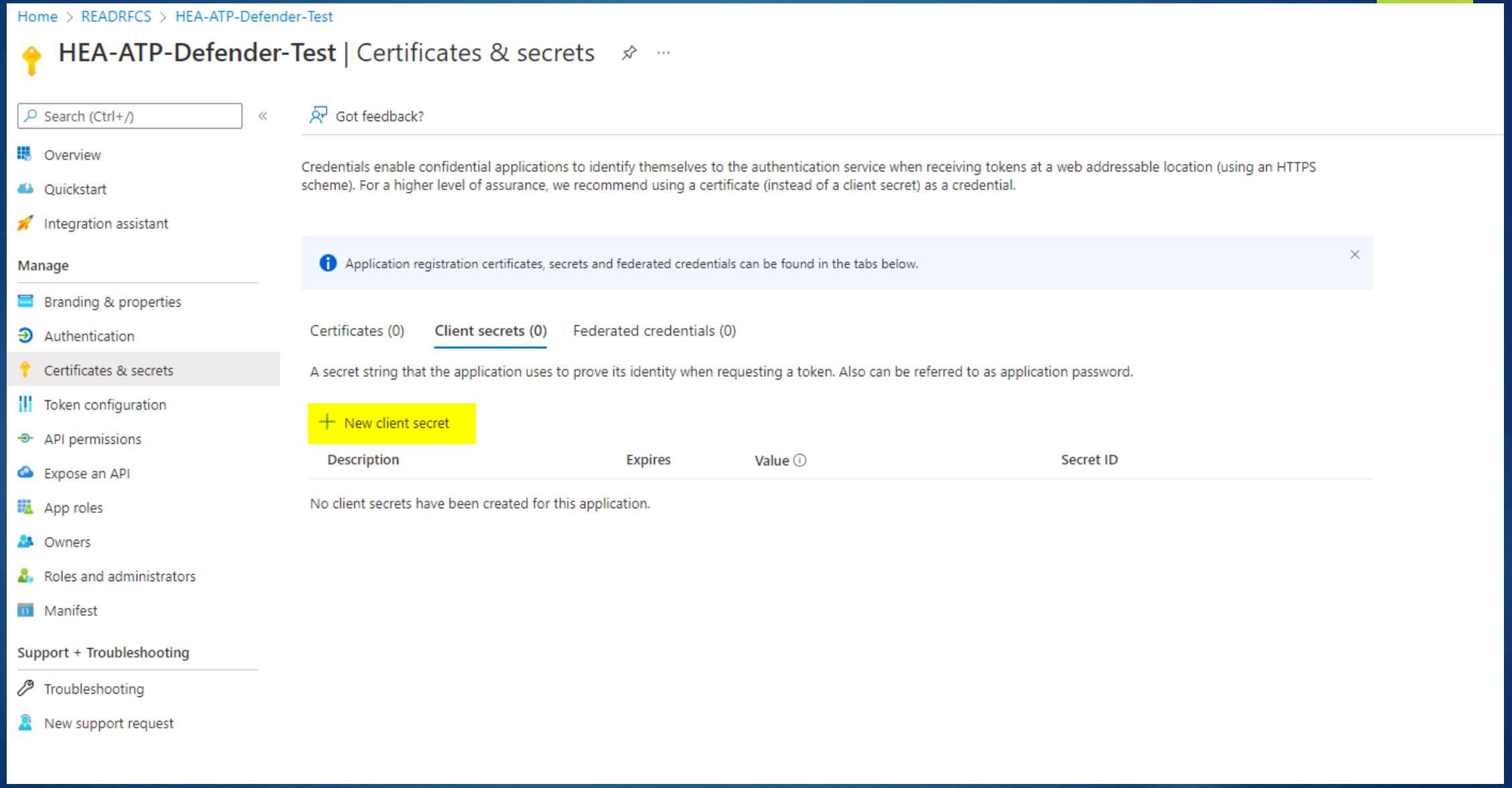
Take note of the ClientID…



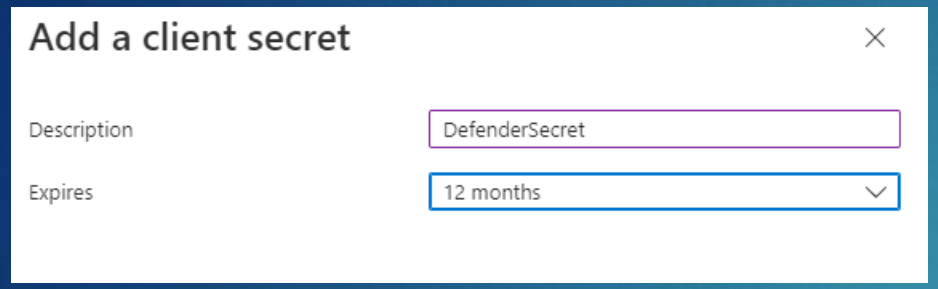
Create a Client Secret…

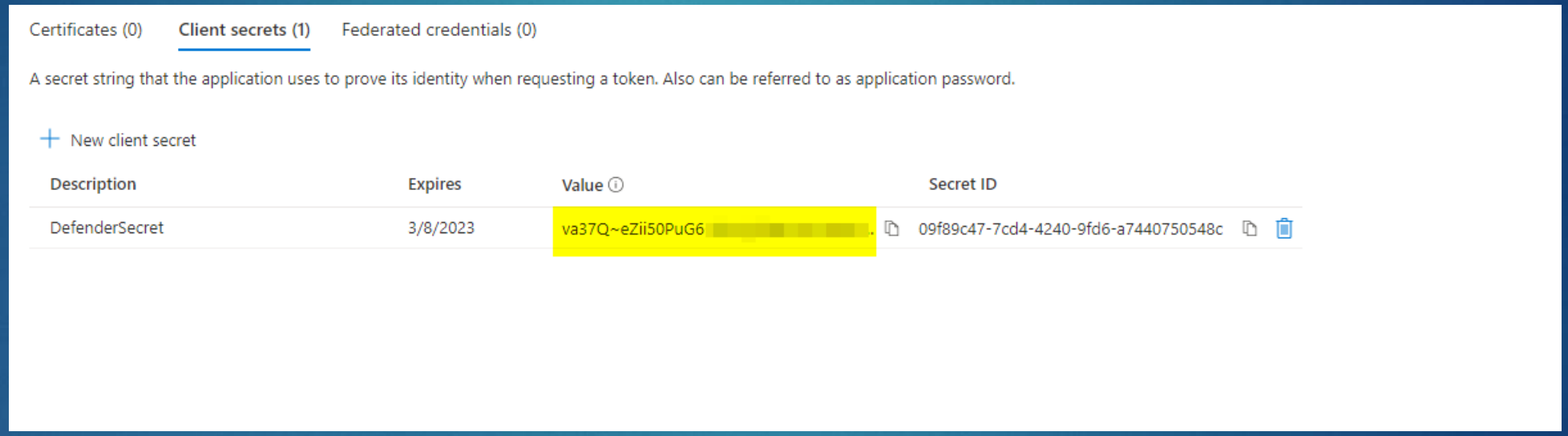


Create a Client Secret…

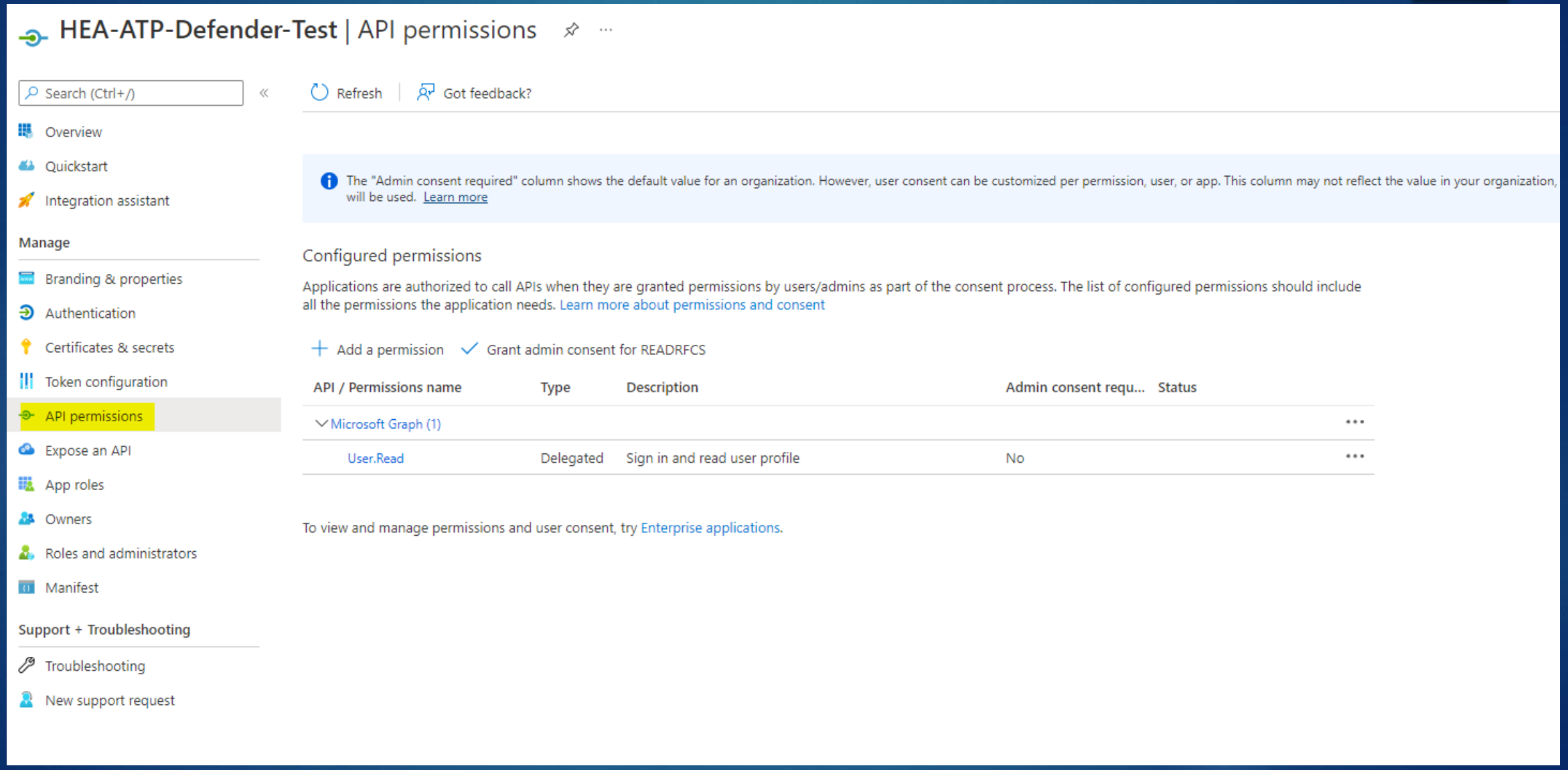


Create a Client Secret…

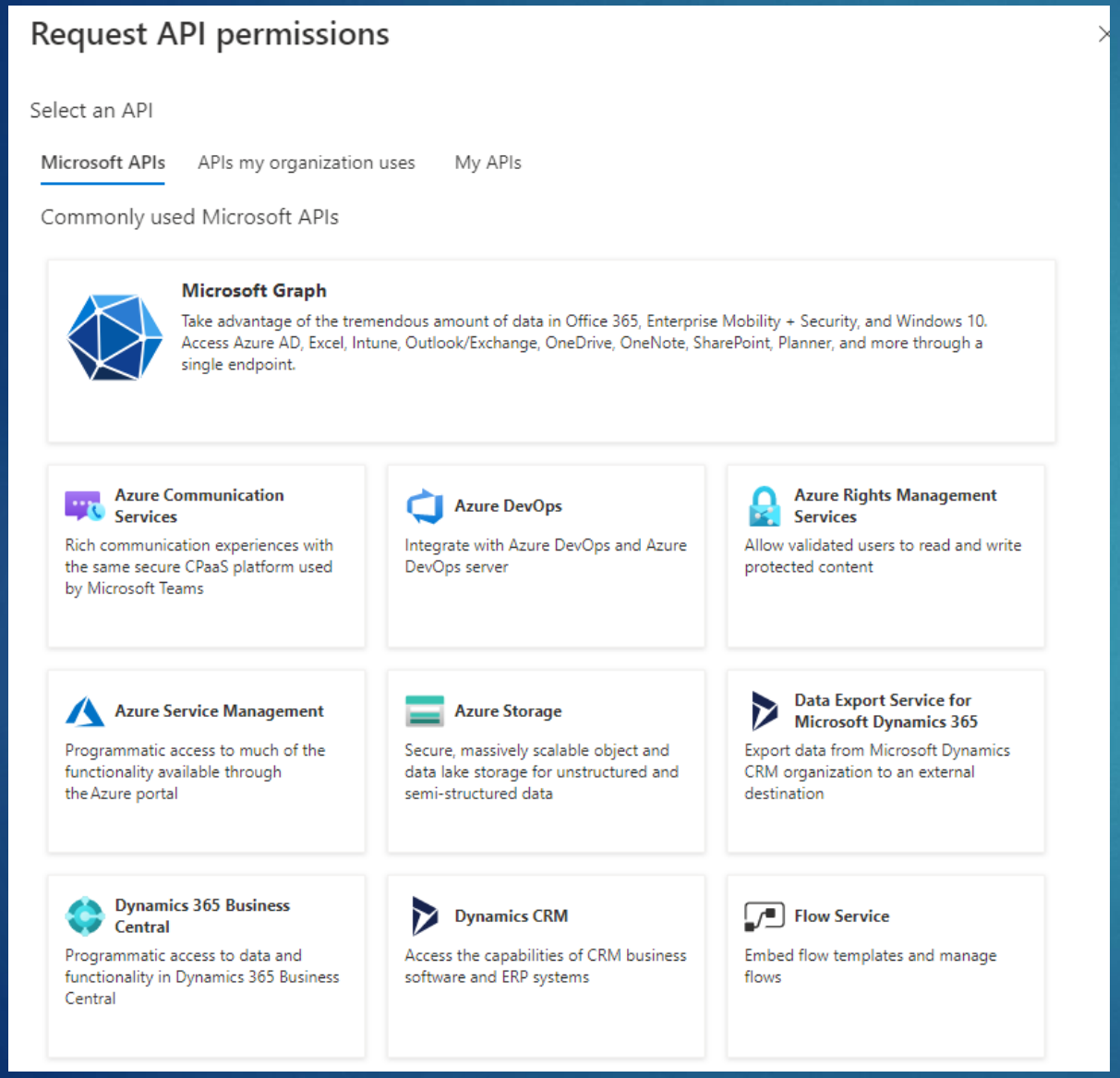




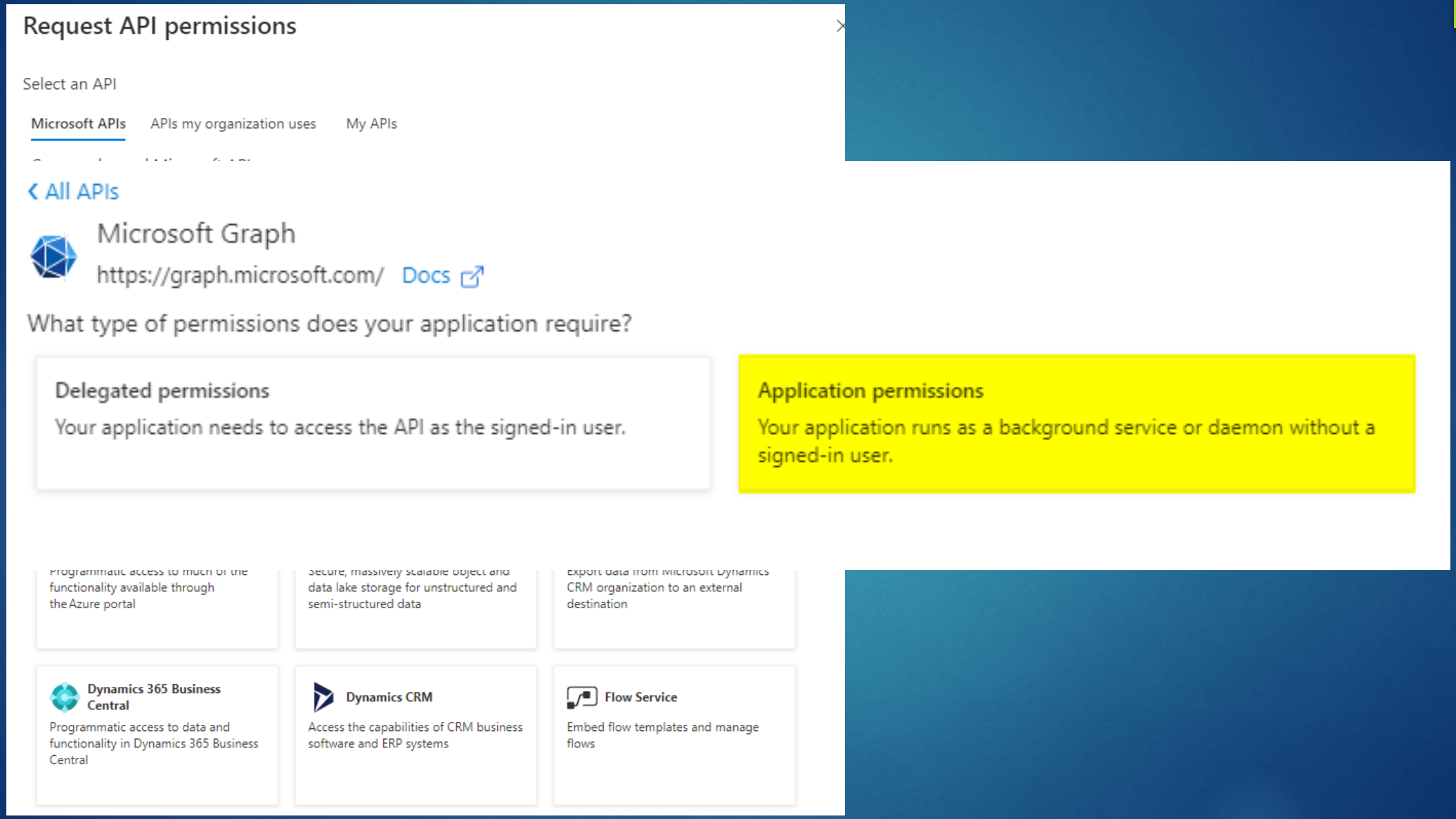
Set the API Permissions…



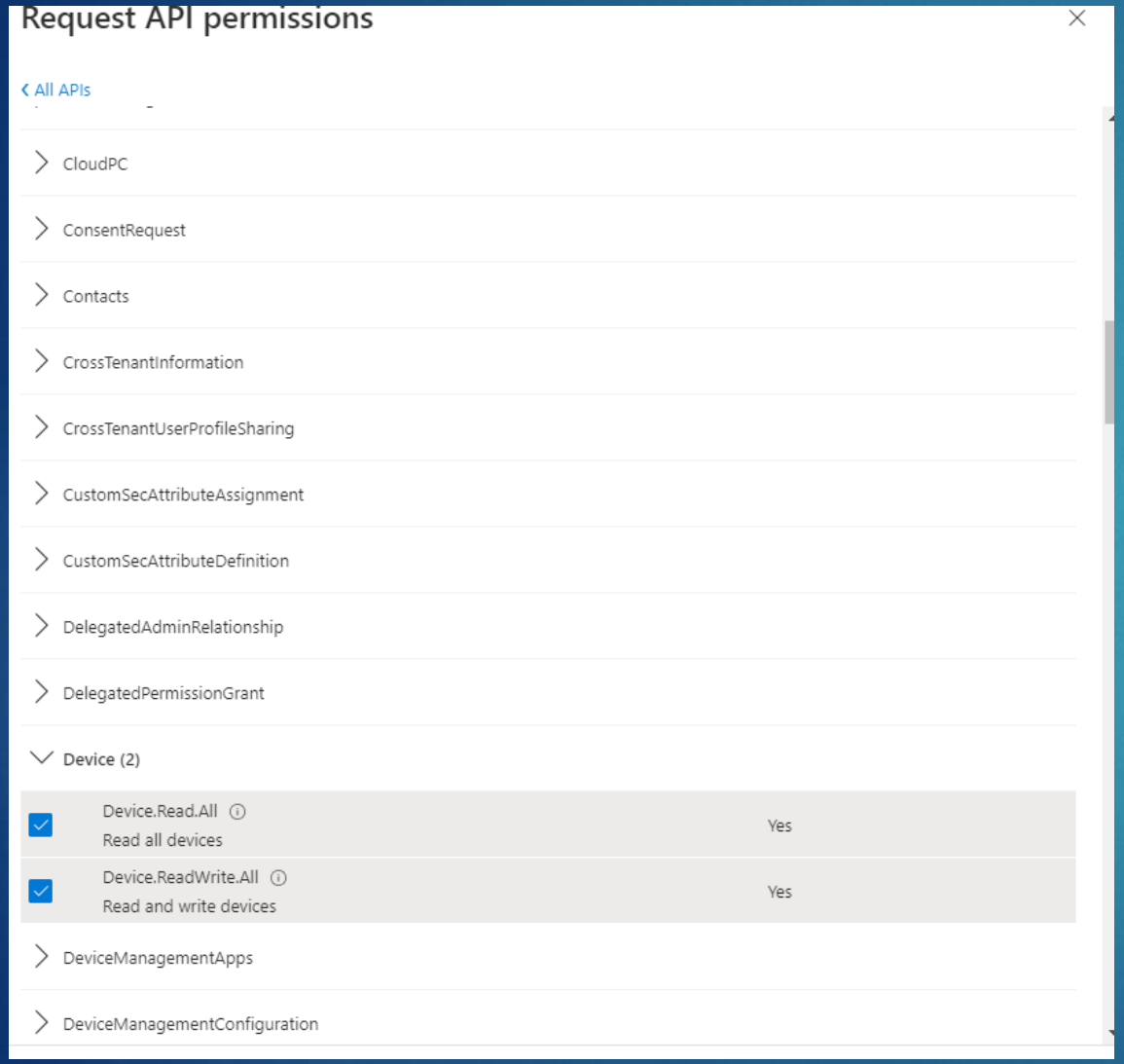
Set the API Permissions…

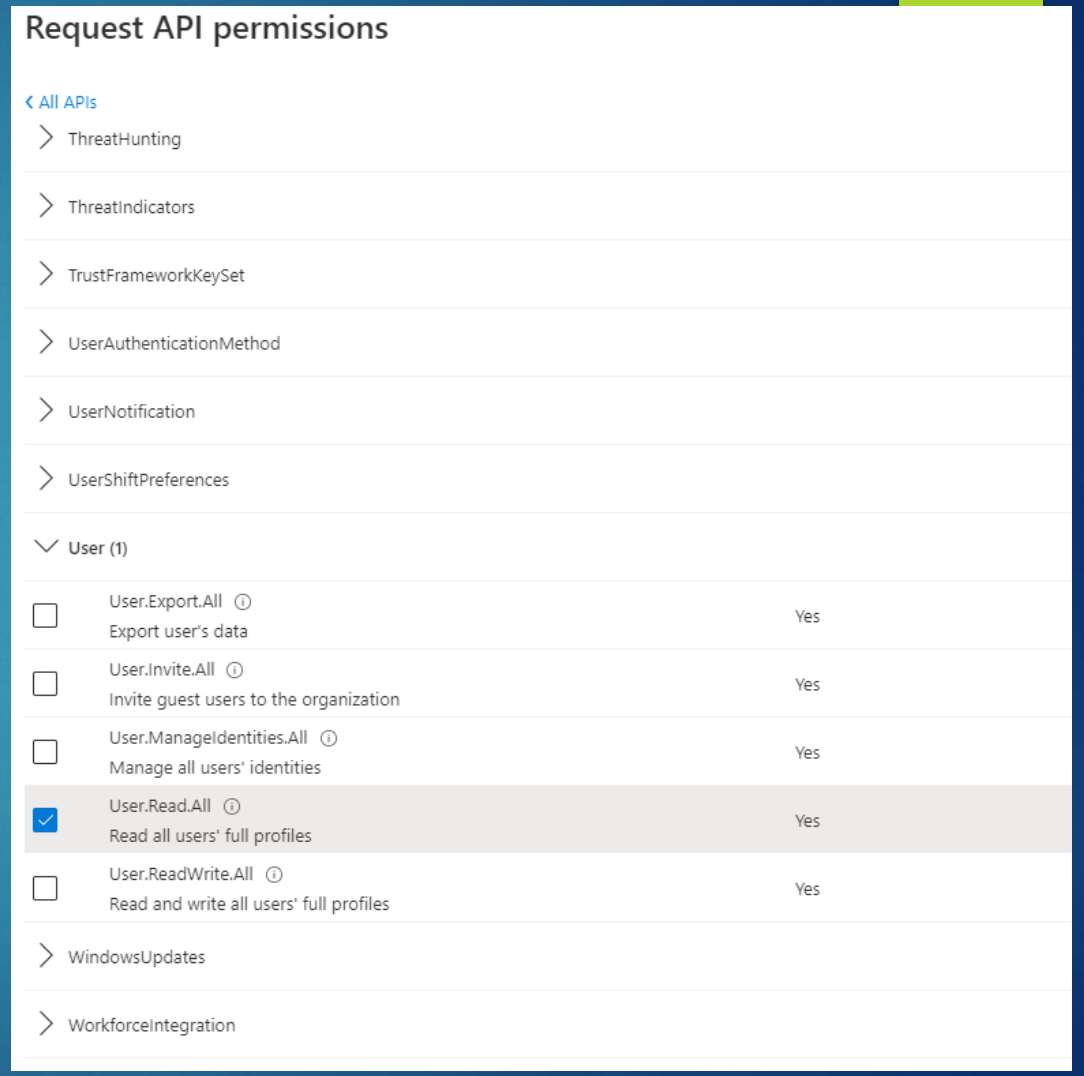


Set the API Permissions…

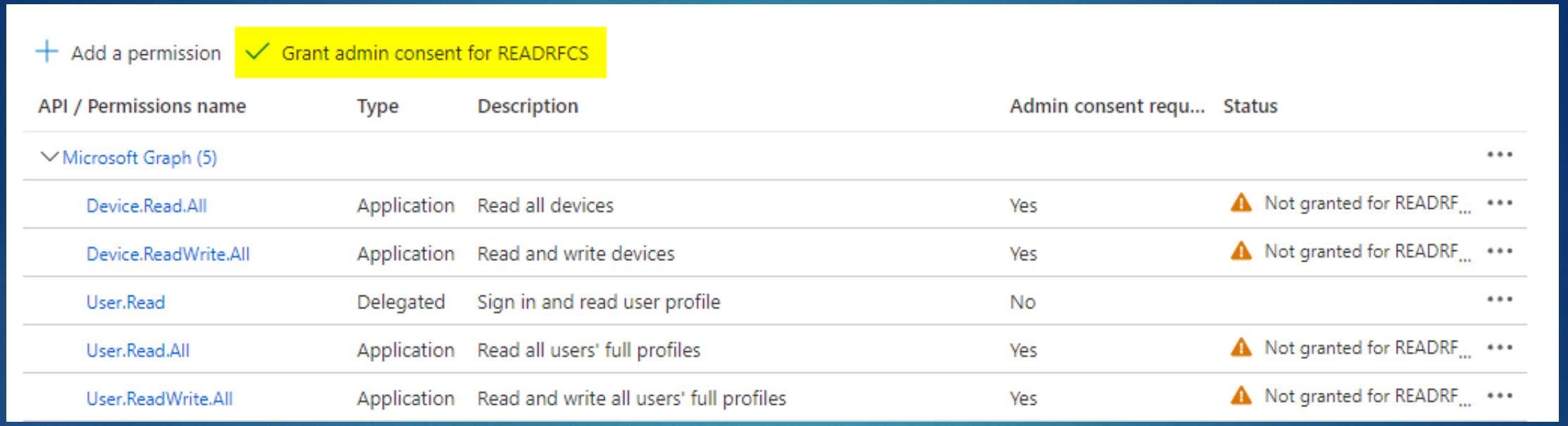


Set the API Permissions…





Set the API Permissions…

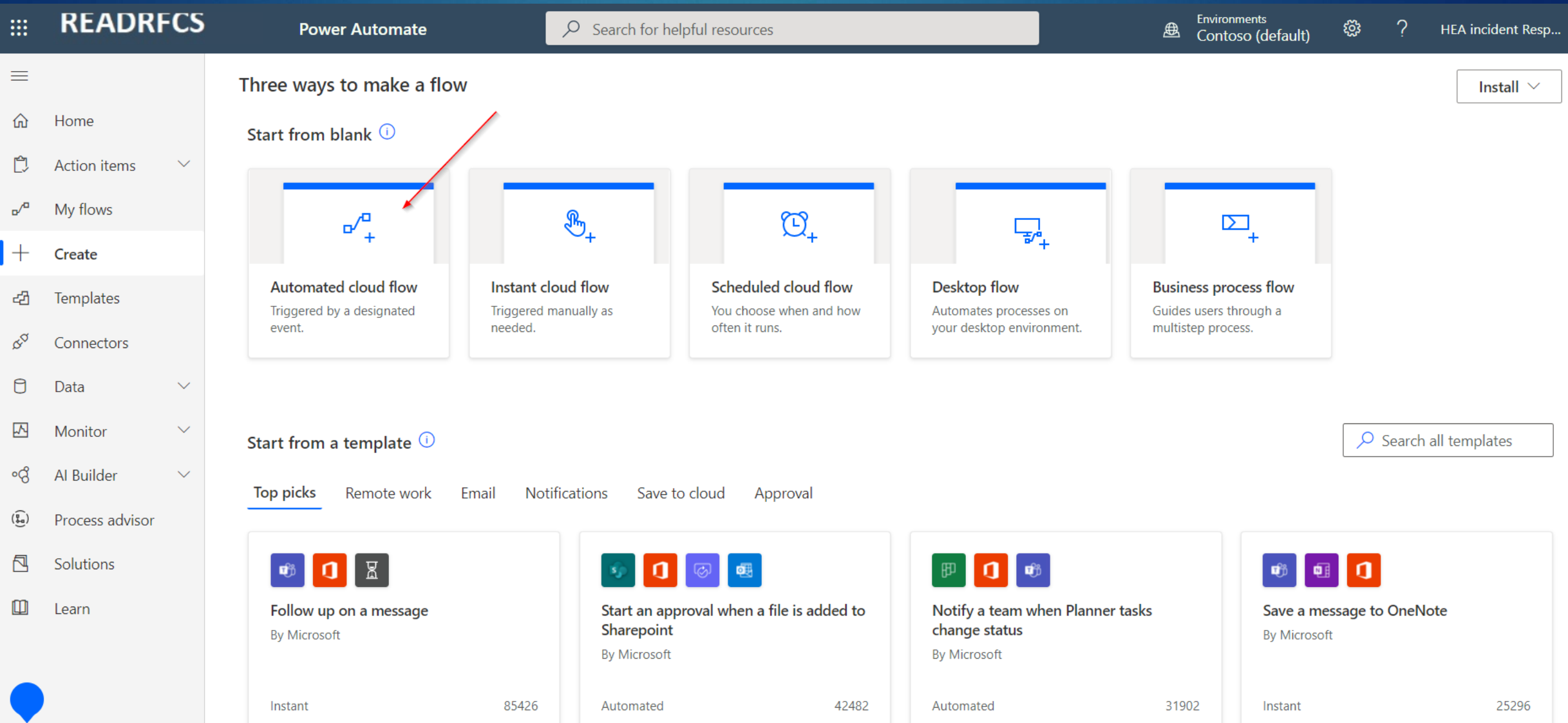


Set the API Permissions…

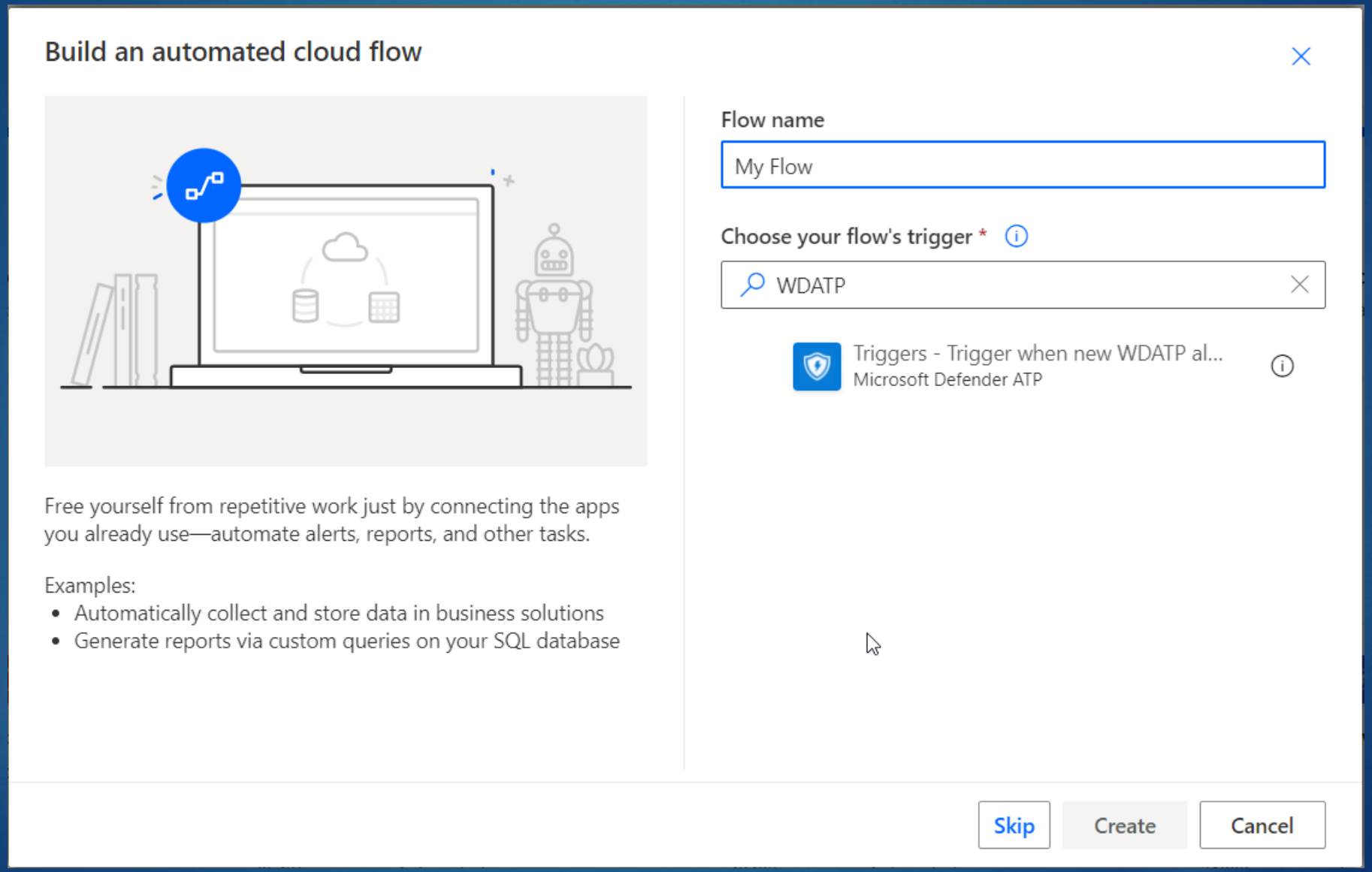
+ Add a permission ✓ Grant admin consent for READRFCS

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
Device.Read.All	Application	Read all devices	Yes	Granted for READRFCS
Device.ReadWrite.All	Application	Read and write devices	Yes	Granted for READRFCS
User.Read	Delegated	Sign in and read user profile	No	Granted for READRFCS
User.Read.All	Application	Read all users' full profiles	Yes	Granted for READRFCS
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	Granted for READRFCS

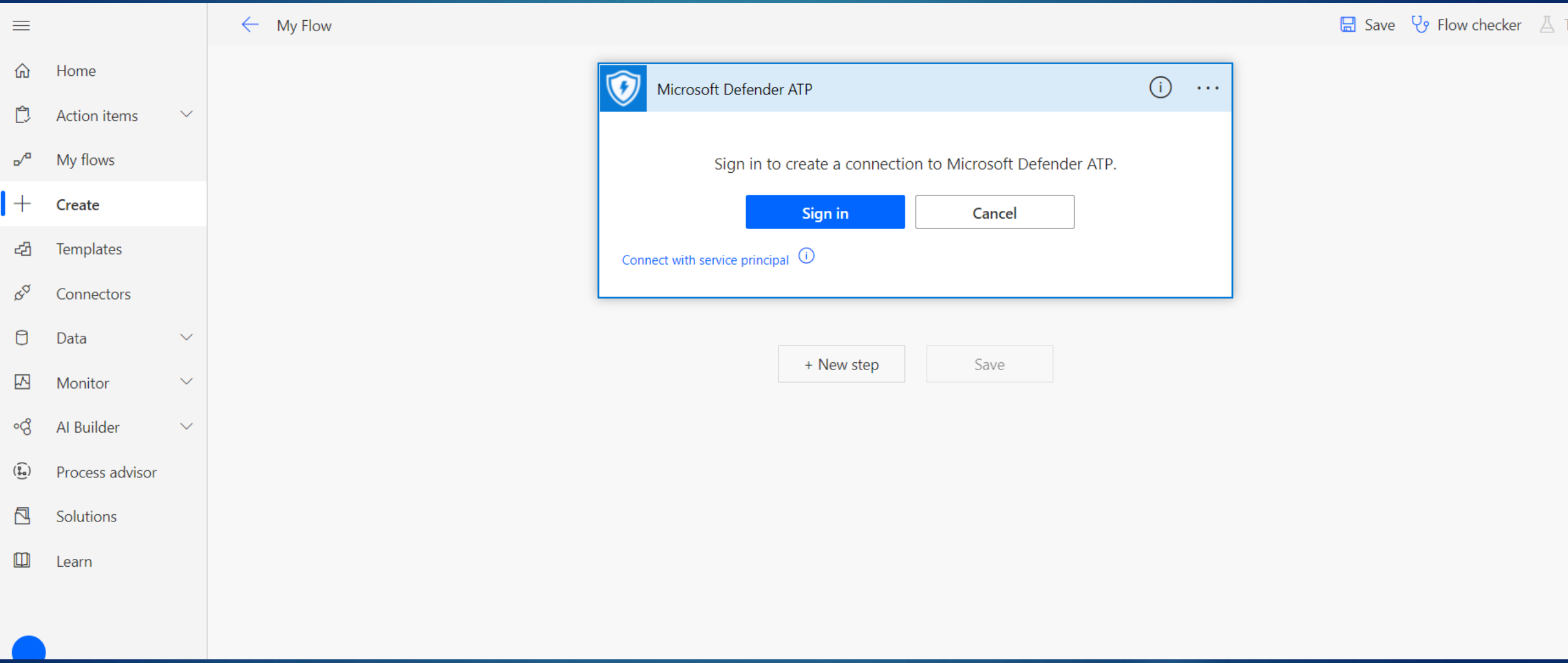
Creating the Powerautomate app



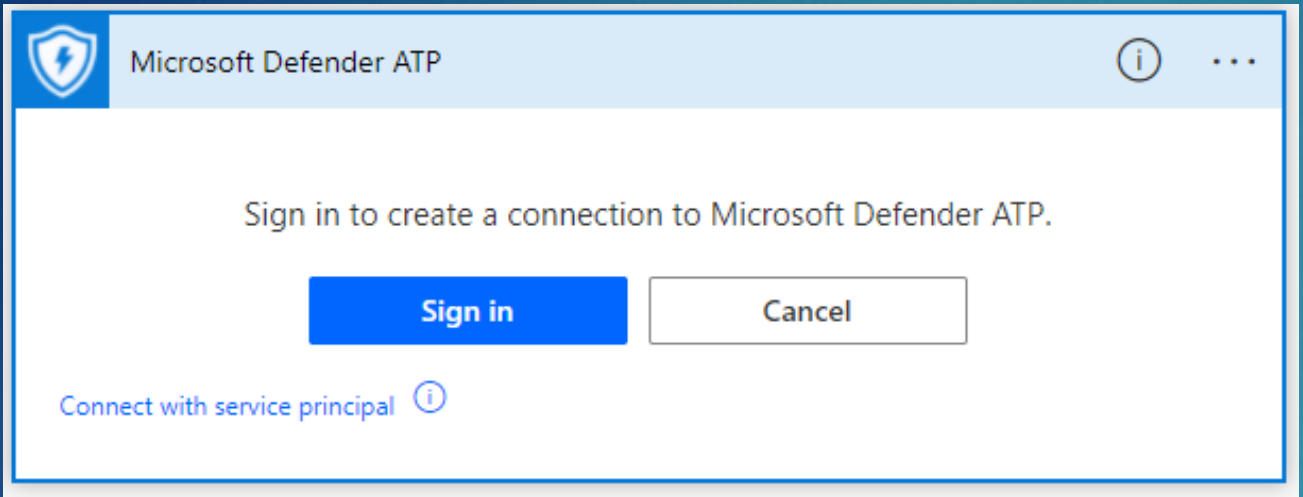
Creating the Powerautomate app



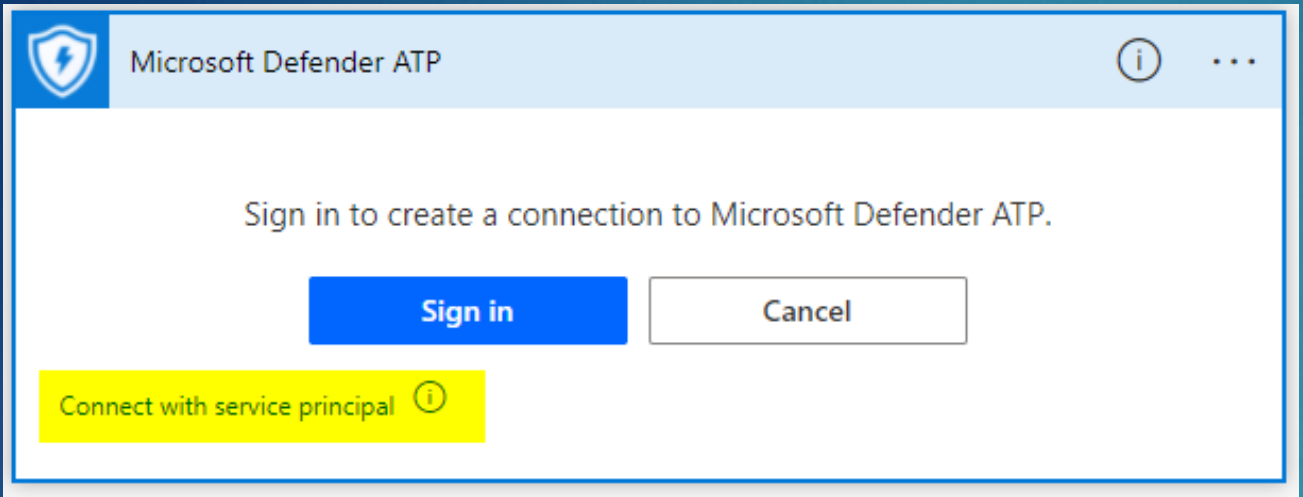
Creating the Powerautomate app

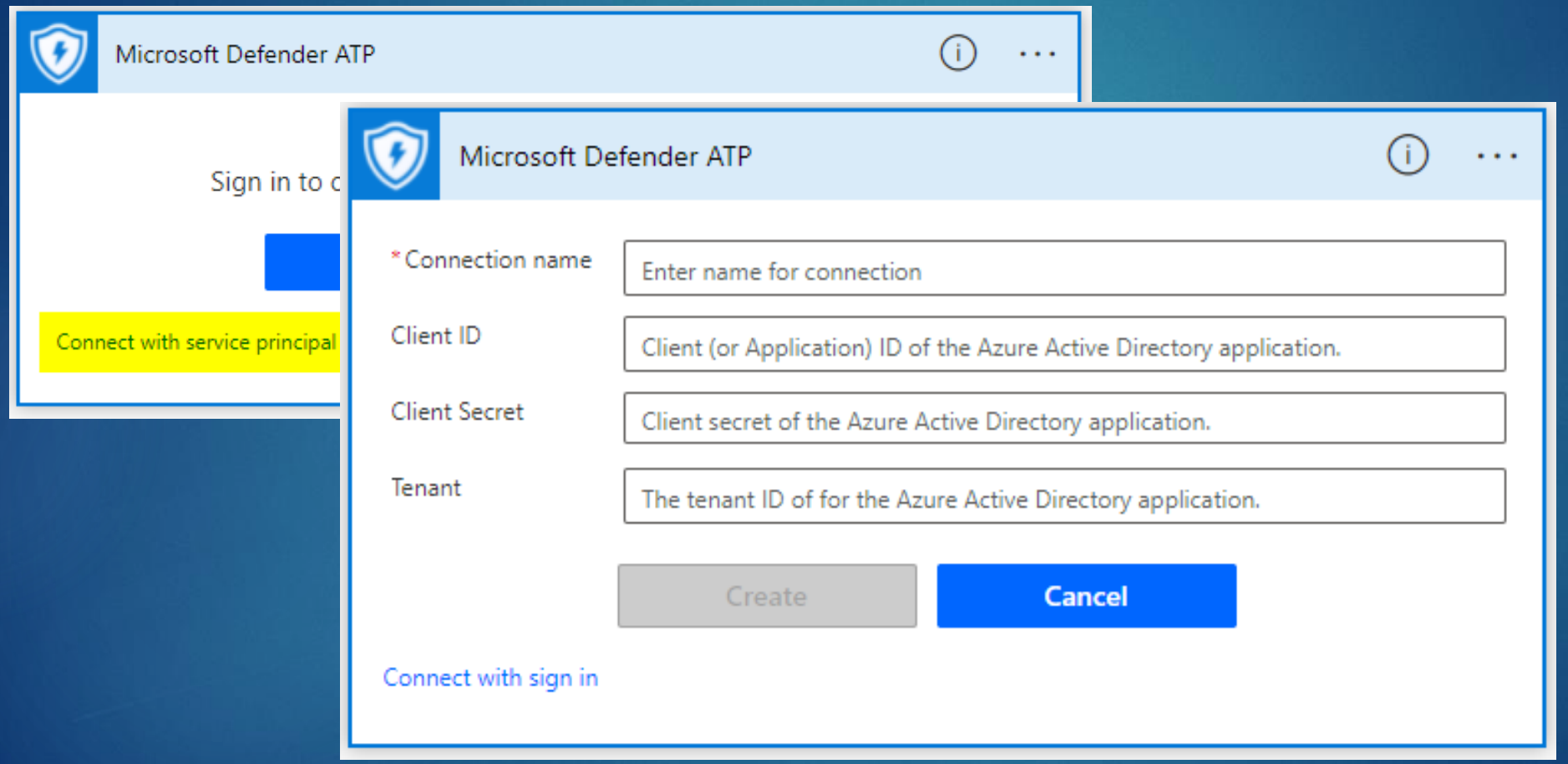


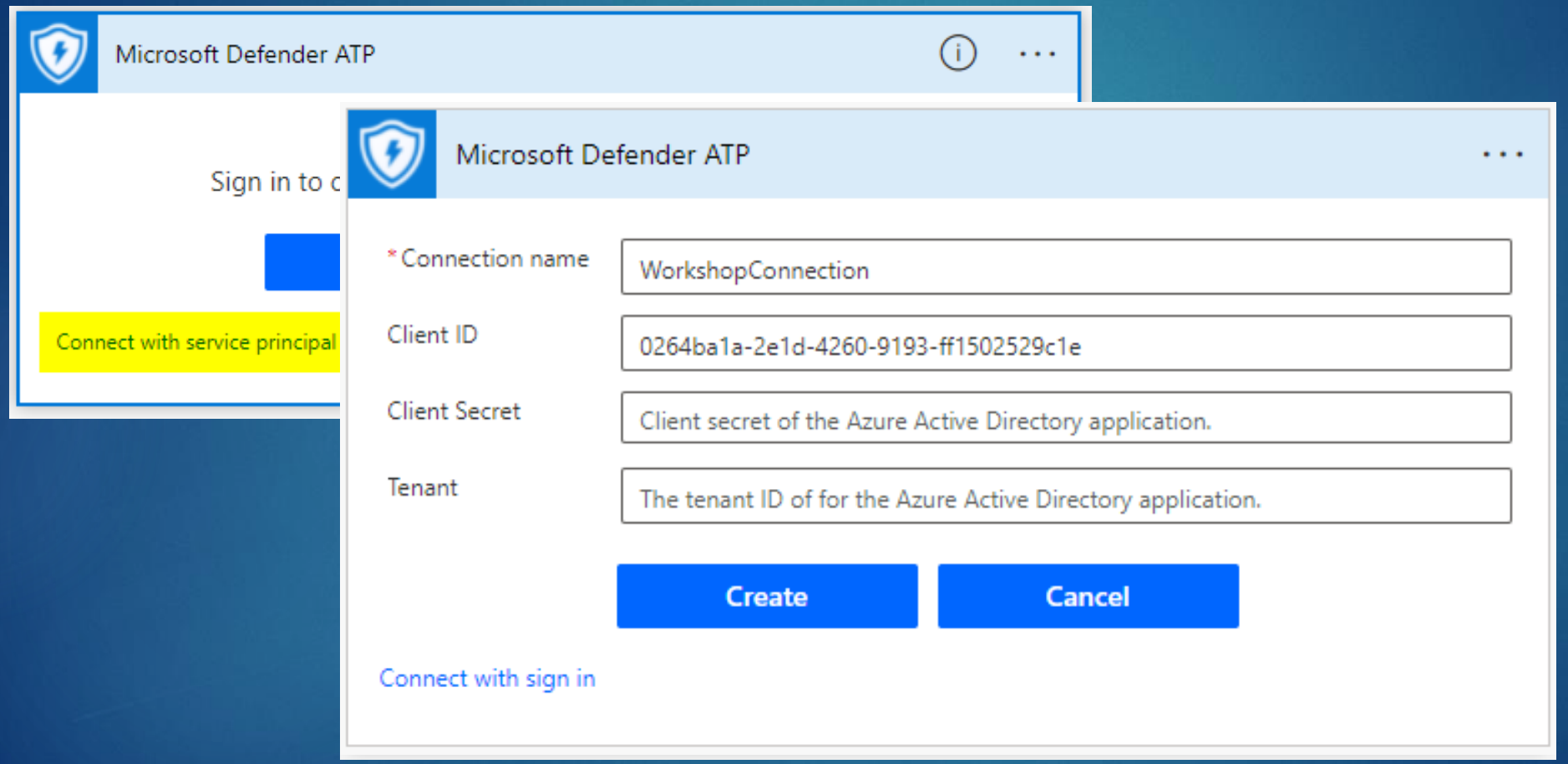
Creating the Powerautomate app

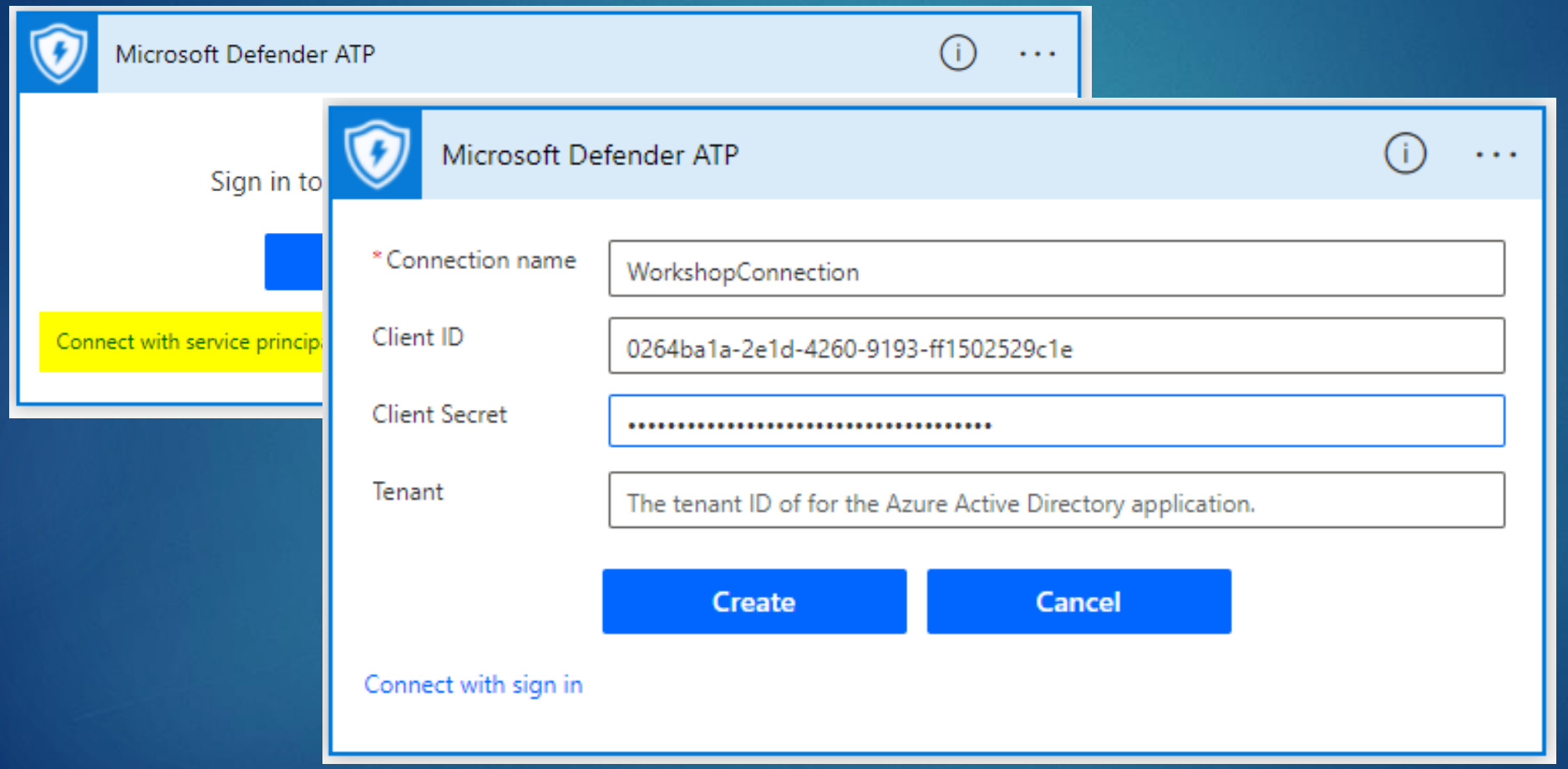


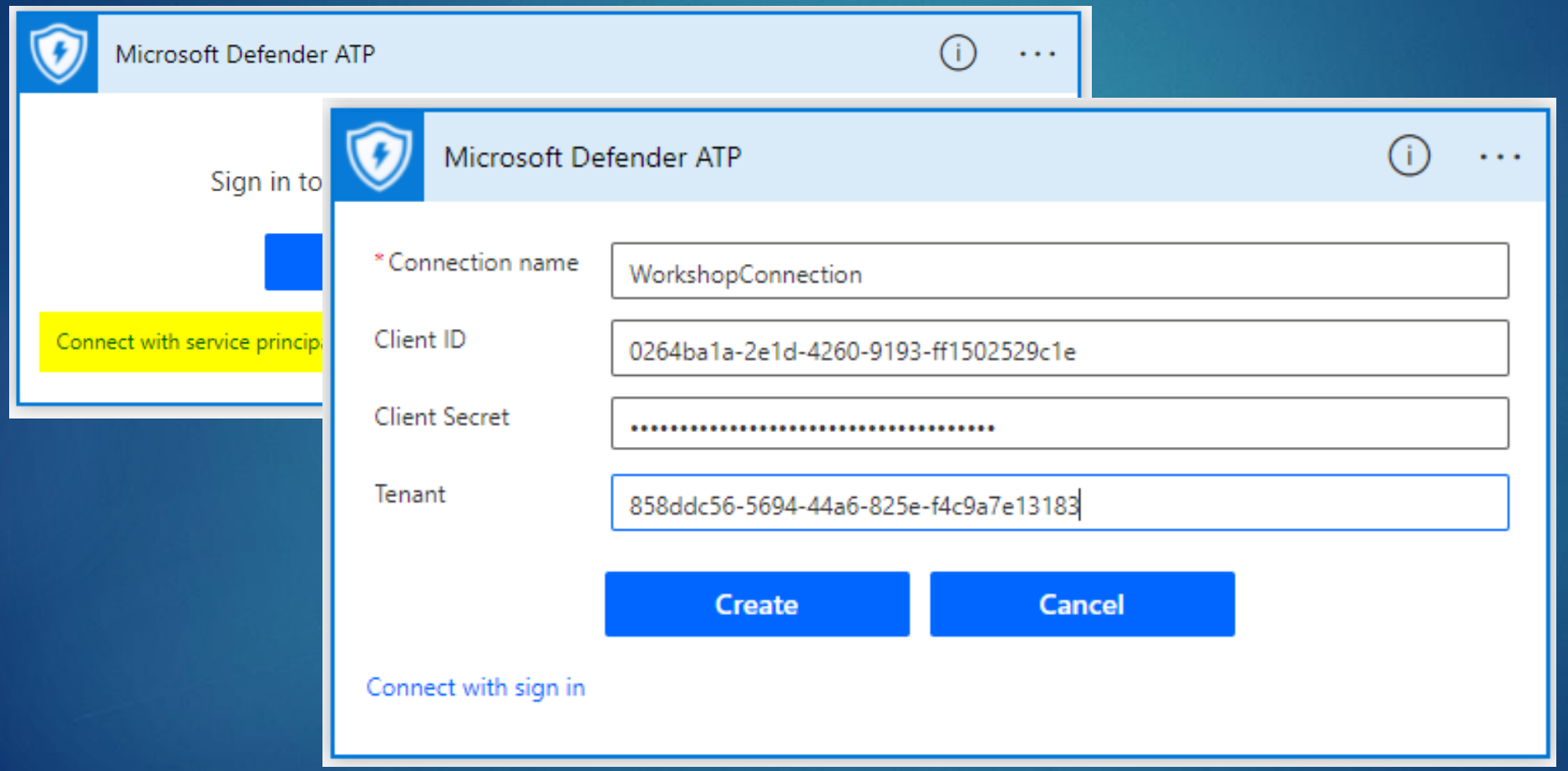
Creating the Powerautomate app

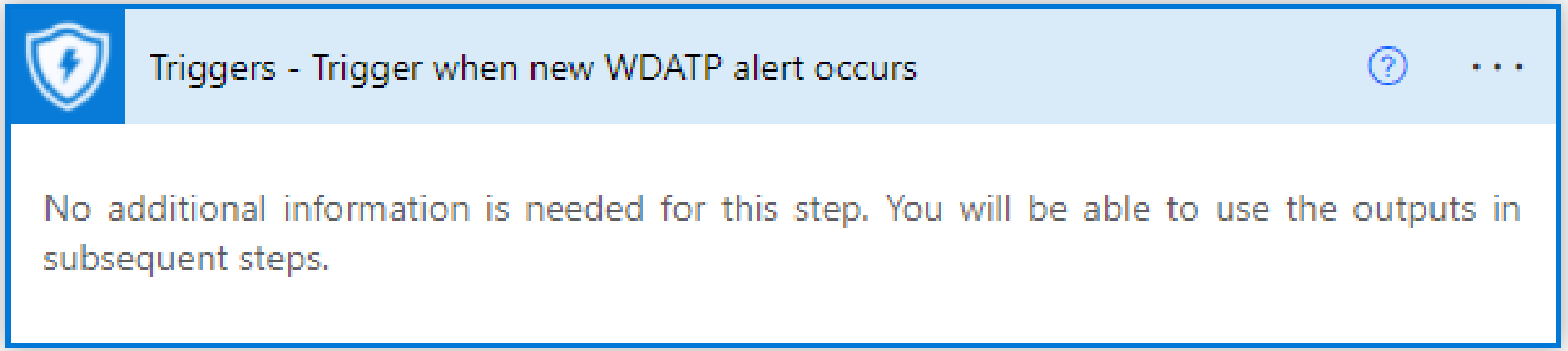












Jump over to….

Powerautomate flow in our Incident response account

5. Things to be aware of

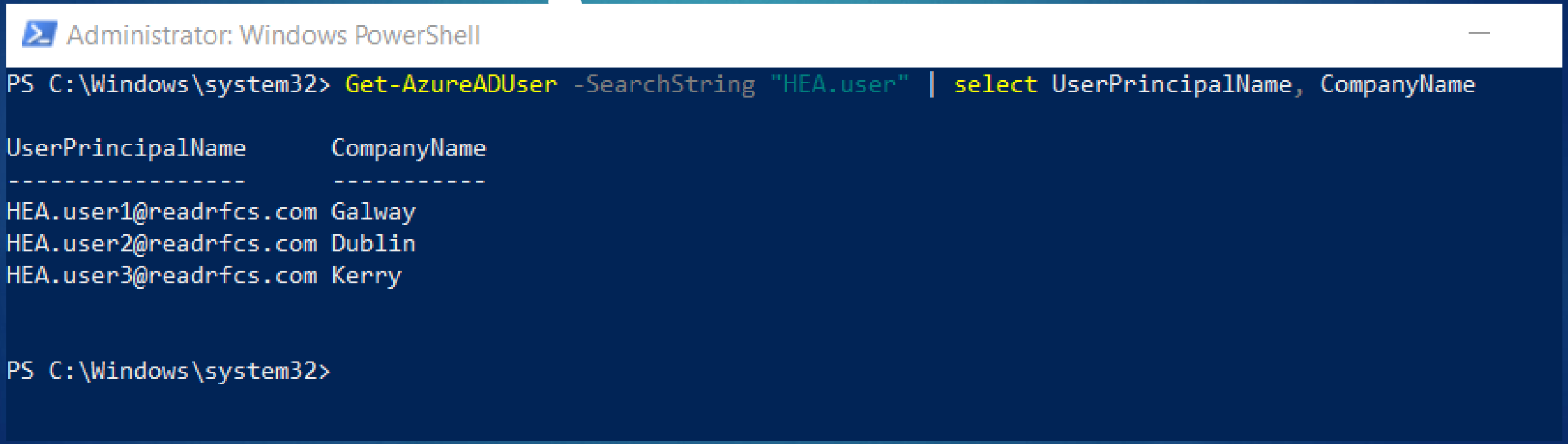
Things to be aware of….

- Isolation is only supported on versions of win 10 1709 or higher
- Doesn't occur on MacOS devices (but it will send an alert that should be investigated)
- Powerautomate script needs to live in a user account. Ensure you protect this account with CA policies, MFA, block sign in from outside of your org IP range etc.
- If sending emails from this account, give it a name that is relevant, such as incident.response@domainname.com
- Use Service principals where possible with the appropriate API permissions

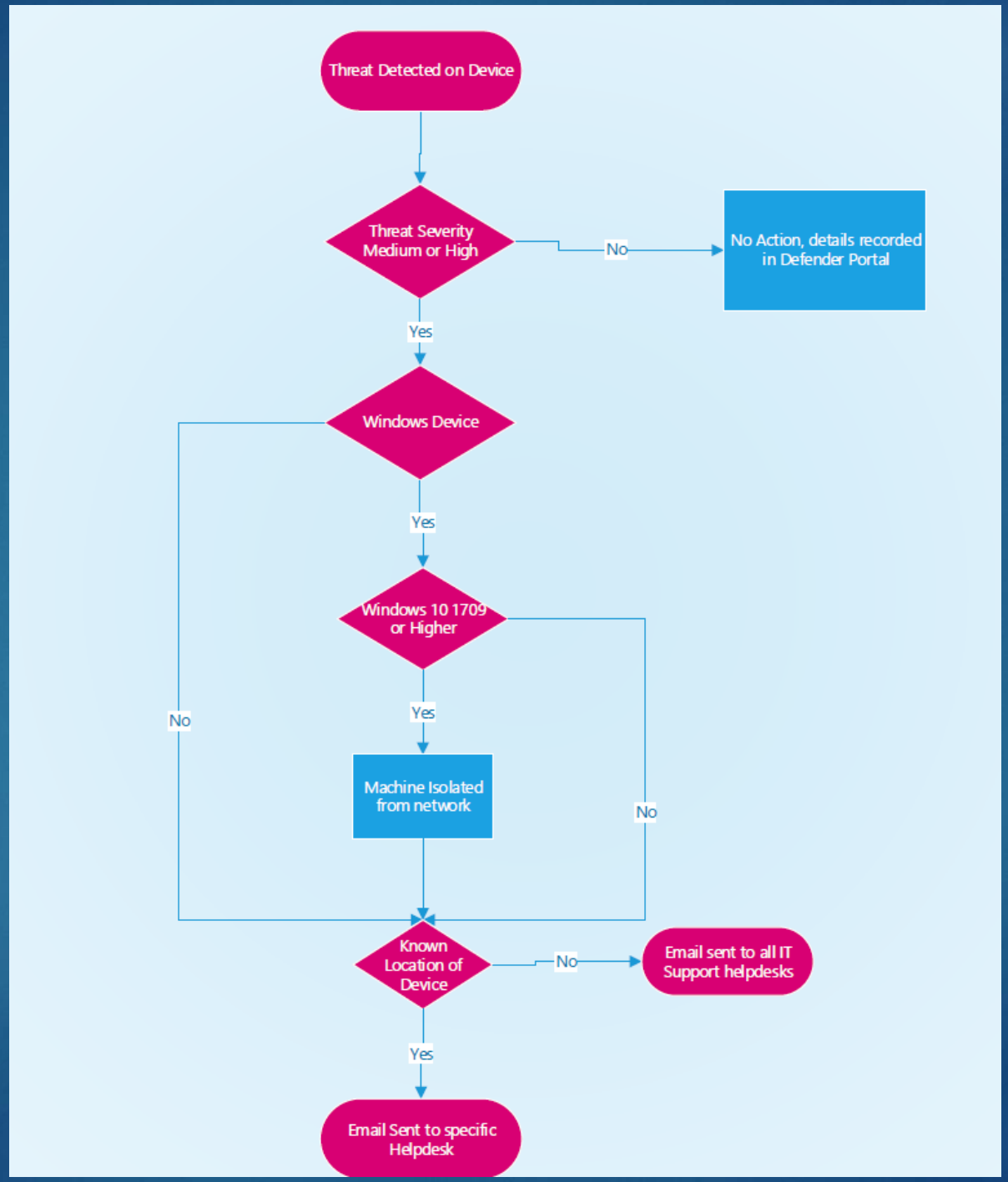
Live Demo

Before we show the Demo

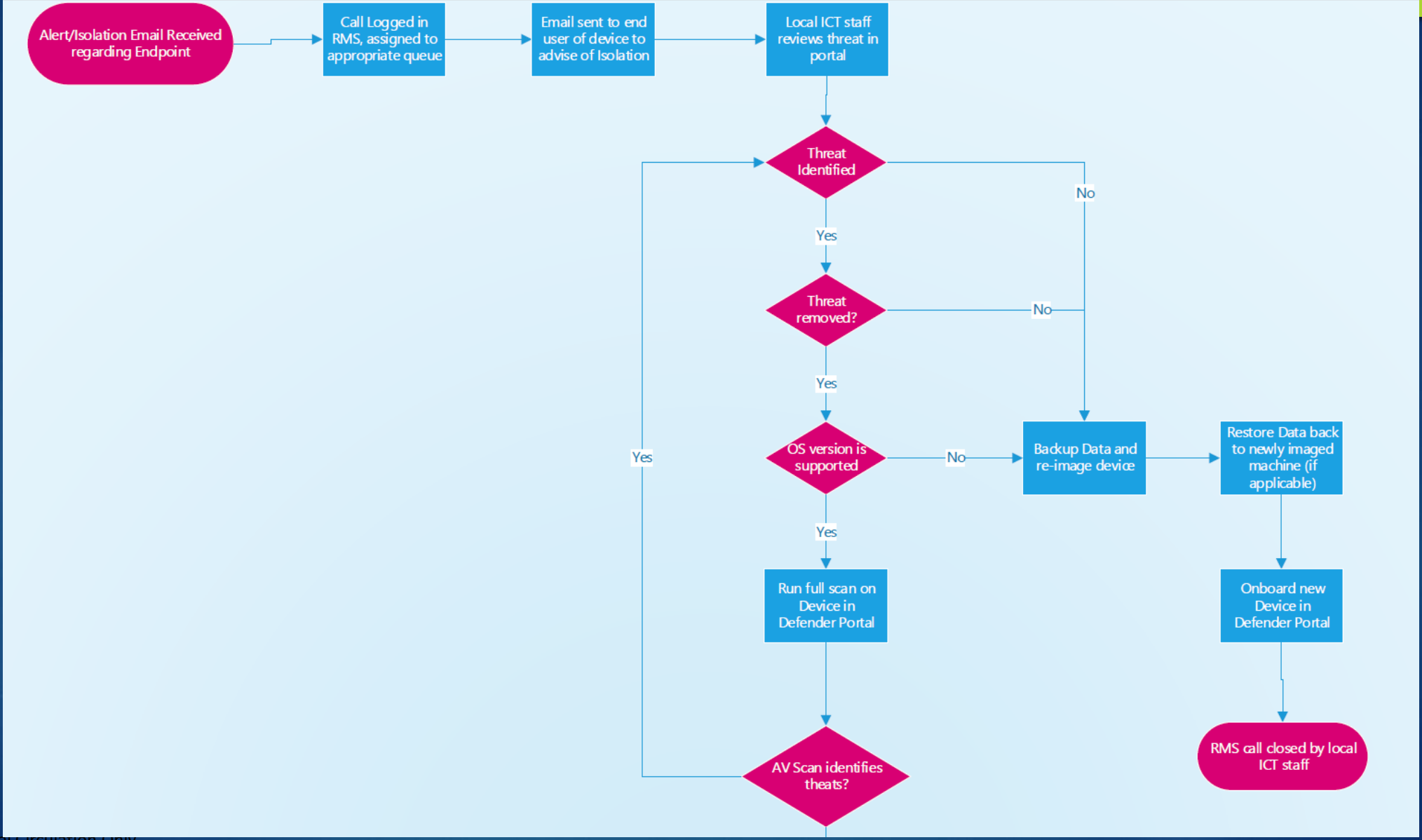
3 Users with CompanyName Attribute set as different values….



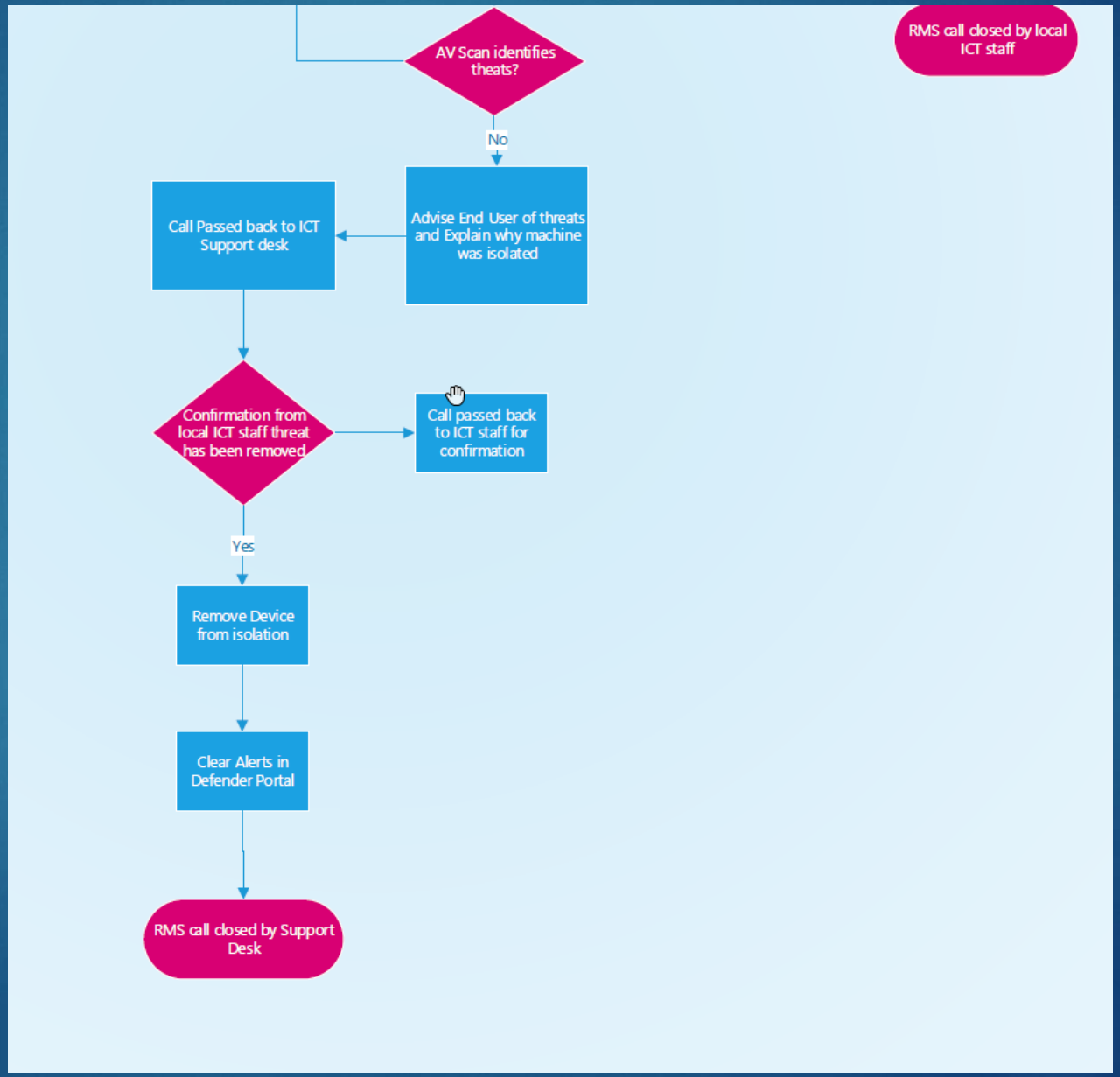
Process



Helpdesk Flow



Helpdesk Flow



In case the demo doesn't work….

Settings > Endpoints > workshop-l-pc02

workshop-l-pc02

No known risks • Active

Manage tags | Go hunt | Release from isolation | Restrict app execution | ...

Device summary

Security Info

Open incidents
0

Active alerts
0

Exposure level
High

Risk level
None

Device details

Domain
AAD joined

OS
Windows 10 64-bit
Version 21H1
Build 19043.1052

Device group
WorkshopDevices

Overview | Alerts | Timeline | Security recommendations | Software inventory | Discovered vulnerabilities | Missing KBs

Page 1 | Choose columns | 30 items per page | Filters

Title	Tags	Severity	Stat...	Linked by	Category	Impacted Entities	Service sour...
Bloodhound post-exploitation to...		Medium	Resolved		Suspicious activi...	workshop-l-pc...	Endpoint
'Vigorf' malware was prevented		Informational...	Resolved		Malware	workshop-l-pc...	Endpoint
Mimikatz credential theft tool		High	Resolved		Credential access	workshop-l-pc...	Endpoint
'Pynamer' malware was prevented		Informational...	Resolved		Malware	workshop-l-pc...	Endpoint

Settings > Endpoints > workshop-l-pc02 > Mimikatz credential theft tool

In January, we announced that the MDE SIEM API is being deprecated on March 1st in a post in Message center (MC311064). For customers who are still using this API, we have automatically extended the support until April 1st. Please refer to Deprecating the legacy SIEM API - Microsoft Tech Community for guidance on moving to alternative APIs and SIEM connectors. If you need assistance in the migration, please contact support.

Part of incident: Multiple threat families detected on one endpoint View incident page

workshop-l-pc02
Windows10 +1

AzureAD\HEAUser3

ALERT STORY

Expand all

3/1/2022 9:10:54 PM [5716] **explorer.exe**

9:10:54 PM File Interaction **mimikatz.exe**
Mimikatz credential theft tool High Prevented Resolved

9:10:54 PM File Interaction **mimikatz.exe**
Mimikatz credential theft tool High Prevented Resolved

9:10:54 PM File Interaction **mimilove.exe**
'Pynamer' malware was prevented Informational Prevented Resolved

9:10:54 PM File Interaction **Brain.A.zip**
'Vigorf' malware was prevented Informational Prevented Resolved

9:11:08 PM [9096] **OneDrive.exe** /background

Mimikatz credential theft tool

High Prevented Resolved

Manage alert See in timeline

Details Recommendations

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification: Not Set
Set Classification

Assigned to: Alan.pike.ca@readrfcs.com

Alert details

Category

MITRE ATT&CK Techniques

9:10:54 PM

File Interaction **mimikatz.exe**

SHA1	d1f7832035c3e8a73cc78afd28cfd7f4cece6d20
Path	D:\mimikatz-master\x64\mimikatz.exe
Signer	Unknown
VirusTotal detection ratio	57/69
Prevention details	**Defender detected and quarantined 'HackTool:Win32/Mimikatz.D' in file 'mi...**

Mimikatz credential theft tool High Prevented Resolved

9:10:54 PM

File Interaction **mimikatz.exe**

SHA1	040fbf1325d51358606b710bc3bd774c04bdb308
Path	D:\mimikatz-master\Win32\mimikatz.exe
Signer	Unknown
VirusTotal detection ratio	58/69
Prevention details	**Defender detected and quarantined 'HackTool:Win32/Mimikatz.D' in file 'mi...**

Multiple threat families detected on one endpoint

Manage incident | Consult a threat expert | Comments and history

Summary | Alerts (3) | Devices (1) | Users (0) | Mailboxes (0) | Apps (0) | Investigations (1) | Evidence and Response (16) | Graph

Alerts and categories

0/3 active alerts
1 MITRE ATT&CK tactics
1 other alert categories

Mar 5, 2022, 5:39:23 PM | **Resolved**
Mimikatz credential theft tool on workshop-l-pc02

Mar 5, 2022, 5:39:30 PM | **Resolved**
'Pynamer' malware was prevented on workshop-l-pc02

Mar 5, 2022, 5:49:59 PM | **Resolved**

Scope

1 impacted device

Top impacted entities

Entity type	Risk level/investigation priority	Tags
workshop-l-pc02	No known risks	

View devices

Evidence

16 entities found

View all entities

Incident Information

Tags summary

Incident tags

Incident details

Status
Resolved

Severity
High

Incident ID
88

First activity
First - Mar 5, 2022, 5:39:23 PM

Last activity
Last - Mar 5, 2022, 5:49:59 PM

Classification
Not set

Determination
Not set

Multiple threat families detected on one endpoint

Manage incident | Consult a threat expert | Comments and history

Summary | Alerts (3) | Devices (1) | Users (0) | Mailboxes (0) | Apps (0) | Investigations (1) | Evidence and Response (16) | Graph

Incident's alerts [0/3 active alerts]

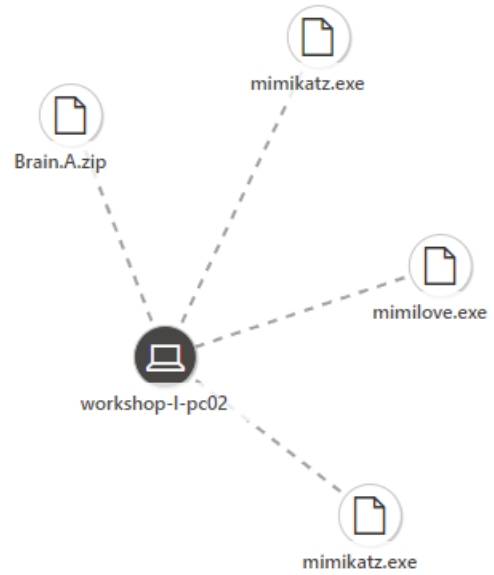
Play attack story | Unpin all | ...

Mar 5, 2022 5:39 PM ● Resolved
Mimikatz credential theft tool
workshop-l-pc02

Mar 5, 2022 5:39 PM ● Resolved
'Pynamer' malware was prevented
workshop-l-pc02

Mar 5, 2022 5:49 PM ● Resolved
'Vigorf' malware was prevented
workshop-l-pc02

Layout | Group similar nodes



Multiple threat families detected on one endpoint

Manage incident | Consult a threat expert | Comments and history

Summary | Alerts (3) | Devices (1) | Users (0) | Mailboxes (0) | Apps (0) | Investigations (1) | Evidence and Response (16) | Graph

All evidence (16)

Files (15)

Processes (1)

1-16 of 16 | Choose columns | 30 items per page | Filters

First seen	Entity	Verdict	Remediation status	Impacted assets	Detection origin
3/7/2022, 10:59 AM	helper.exe (9928)	Unknown	Remediated	WORKSHOP-L-PC02	Get related entities Completed
3/7/2022, 10:53 AM	f_0001ed	Malicious	Remediated	WORKSHOP-L-PC02	Find recently created or modified executable files Complet...
3/7/2022, 10:53 AM	sharphound.exe	Malicious	Remediated	WORKSHOP-L-PC02	Find recently created or modified executable files Complet...
3/7/2022, 10:53 AM	sharphound.exe	Malicious	Prevented	WORKSHOP-L-PC02	Get downloaded executable files Completed
3/7/2022, 10:53 AM	sharphound.exe	Malicious	Remediated	WORKSHOP-L-PC02	Find recently run files Completed
3/7/2022, 10:53 AM	btweb_installer.exe	Malicious	Remediated	WORKSHOP-L-PC02	Find recently run files Completed
3/7/2022, 10:53 AM	carrier.exe	Malicious	Remediated	WORKSHOP-L-PC02	Find recently run files Completed
3/7/2022, 10:53 AM	helper.exe	Malicious	Remediated	WORKSHOP-L-PC02	Find recently run files Completed
3/5/2022, 5:53 PM	Brain.A.zip	Suspicious	Prevented	workshop-l-pc02	'Vigorf' malware was prevented Informational
3/5/2022, 5:49 PM	brain.a.zip	Malicious	Prevented	WORKSHOP-L-PC02	'Vigorf' malware was prevented
3/5/2022, 5:39 PM	mimikatz.exe	Suspicious	Prevented	workshop-l-pc02	Mimikatz credential theft tool High
3/5/2022, 5:39 PM	mimilove.exe	Suspicious	Prevented	workshop-l-pc02	'Pynamer' malware was prevented Informational

All evidence (16)

Files (15)

Processes (1)

1 Selected

First seen	Entity	Verdict	Remediation status	Impacte
3/7/2022, 10:59 AM	helper.exe (9928)	Unknown	Remediated	W
3/7/2022, 10:53 AM	f_0001ed	Malicious	Remediated	W
3/7/2022, 10:53 AM	sharphound.exe	Malicious	Remediated	W
3/7/2022, 10:53 AM	sharphound.exe	Malicious	Prevented	W
3/7/2022, 10:53 AM	sharphound.exe	Malicious	Remediated	W
3/7/2022, 10:53 AM	btweb_installer.exe	Malicious	Remediated	W
3/7/2022, 10:53 AM	carrier.exe	Malicious	Remediated	W
3/7/2022, 10:53 AM	helper.exe	Malicious	Remediated	W
3/5/2022, 5:53 PM	Brain.A.zip	Suspicious	Prevented	w
3/5/2022, 5:49 PM	brain.a.zip	Malicious	Prevented	W
3/5/2022, 5:39 PM	mimikatz.exe	Suspicious	Prevented	w
3/5/2022, 5:39 PM	mimilove.exe	Suspicious	Prevented	w
3/5/2022, 5:39 PM	mimikatz.exe	Suspicious	Prevented	w
3/5/2022, 5:39 PM	mimikatz.exe	Malicious	Prevented	W
3/5/2022, 5:39 PM	mimilove.exe	Malicious	Prevented	W
3/5/2022, 5:39 PM	mimikatz.exe	Malicious	Prevented	W

mimikatz.exe

File

Go hunt

File details

Verdict

File Name mimikatz.exe

Go hunt

HEA incident Response <HEA-IncidentResponse@readrfcs.com>
to Alan, me, HEA

Mon, 7 Mar, 11:03 (1 day ago)

This is to notify that the machine (workshop-l-pc02) has been isolated by WDATP due to a Medium severity alert. This device is tagged as "Kerry" within the defender portal

Device information
OS Platform: Windows10
OS Version:
Machine Last IP Address: 192.168.0.68
Last external IP: 37.228.248.241
Machine Risk score: None
Machine Health status: Active

Alert information:
Alert Status: New
Alert Title: Bloodhound post-exploitation tool
Alert Classification:
Alert Description: Bloodhound, a post-exploitation open-source reconnaissance tool, has been detected on this device. Bloodhound has been used in a wide range of documented attacks, including attacks involving state-sponsored groups and groups associated with ransomware campaigns. An attacker might be attempting to collect information about users, user sessions, groups, accounts, domain controller properties and permissions. Detections of Bloodhound tools and activity should be thoroughly investigated.
Alert Threat Family: SharpHound
Alert Detection Source: WindowsDefenderAv

Alert URL:
https://security.microsoft.com/alerts/da637822477635918028_-1337180965

Machine URL:
https://security.microsoft.com/machines/f051075f76ef17f906a454cacdd84e4e727df871

Note: this is an automated email sent by the incident response O365 account. Please investigate the root cause and notify the user as soon as possible

Any suggestions or Questions or Anything you wish to discuss

alan.pike@tudublin.ie