LAB03: Securing Azure Arc-enabled servers with Microsoft Defender for Cloud

Student Lab Manual

Table of Contents

===

Exercise 1 - Detect threats on your servers using alerts

Objective

This exercise will walk you through simulating malicious activity on your machines and examine how Defender for Servers can alert you on those threats.

Estimated Time to Complete This Lab

45 minutes

Explanation

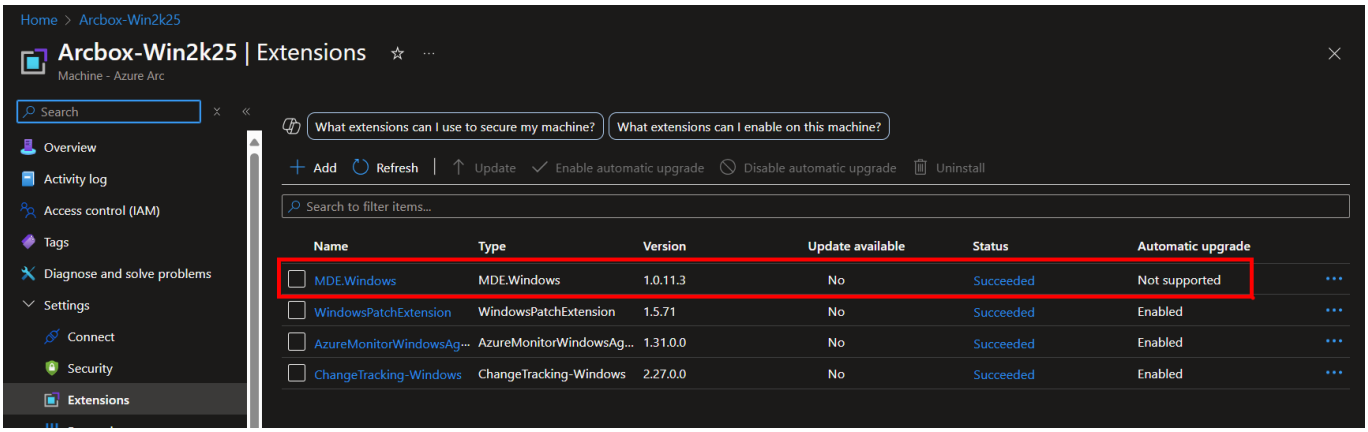
In this exercise, you will learn how to leverage Defender for Servers to detect threats and malicious activities.

===

Task 1: Simulate malicious activities

1. [] To simulate a malicious activity on the *ArcBox-Win2K25* servers, rdp into the *ArcBox-Client* VM.

> [!hint] **Before simulating the alert, make sure that the 'MDE.Windows' is installed on the Arc-enabled server.** You can do this by checking the Extensions installed on the Arc enabled server *ArcBox-Win2k25* from the Azure portal.



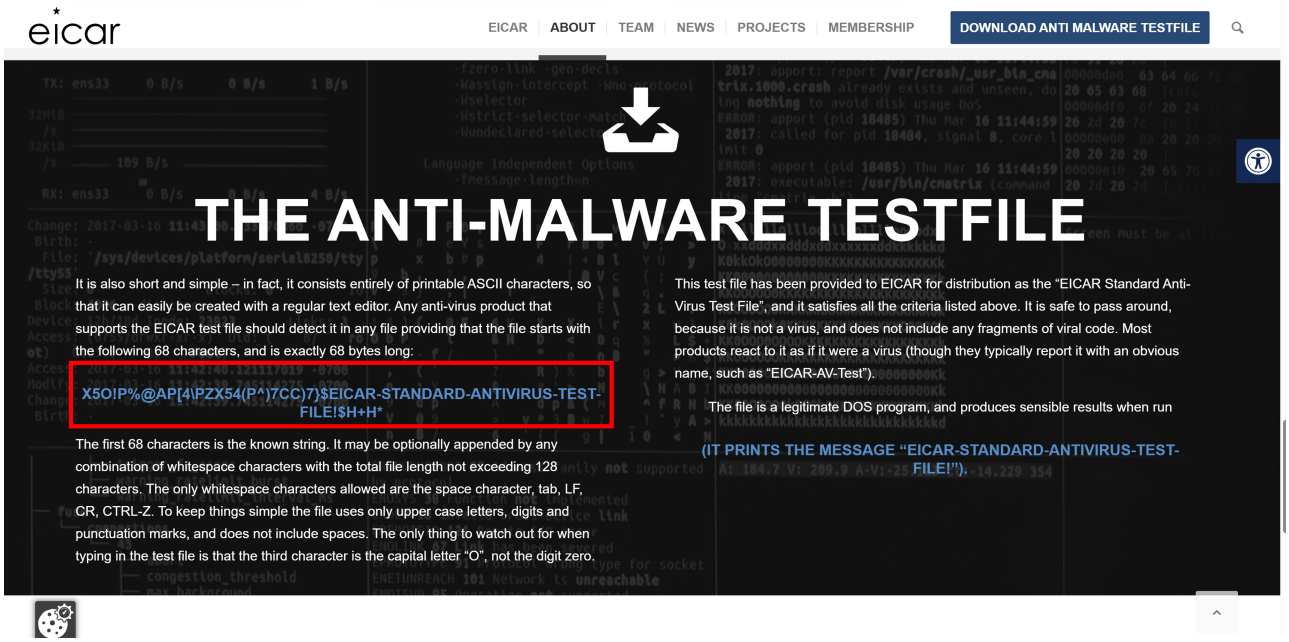
> [!hint] If the 'MDE.Windows' extension is missing then either the *Microsoft Defender for Cloud* configuration has not been set correctly as explained in Lab01 **OR** the configuration of the *Microsoft Defender for Cloud* has not taken effect yet. Go back to Lab01 and check that you have set the Defender for Cloud correctly in the step *Enable the Defender for Servers plan* and have saved the configuration.

2. [] **If the 'MDE.Windows' extension is missing and not in the process of being created as seen in the Azure Portal** then you can manually install it on the *ArcBox-Win2k25* by running the following Powershell script either in the *ArcBox-Client* machine or in Powershell from the Azure Portal cloud shell, **making sure that the Resource Group name is correct**. Otherwise if the extension is installed then move to the next step.

> [!hint] If you decide to run the manual installation of the *MDE.Windows* extension from the *ArcBox-Client* machine, then you will need to login from PowerShell using the *Connect-AzAccount* command and choosing the *Work or School* option. Additionally you will need to run the command *Install-Module Az.ConnectedMachine -Force* before continuing.

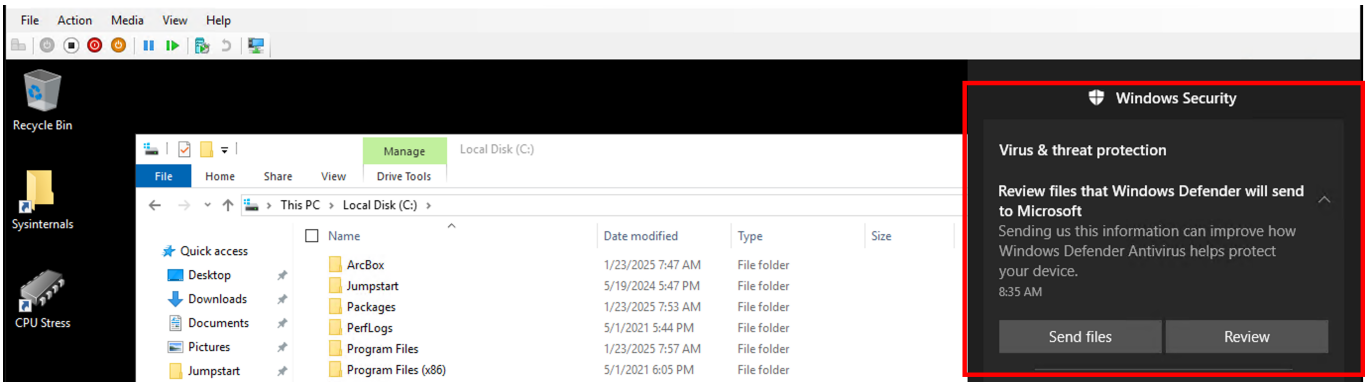
```
$vm = Get-AzConnectedMachine -ResourceGroupName "<Insert Resource Group Name>" -
Name "ArcBox-Win2k25"
$mdePackage = Invoke-AzRestMethod -Uri
https://management.azure.com/subscriptions/$($vm.id.split('/')
[2])/providers/Microsoft.Security/mdeOnboardings/?api-version=2021-10-01-preview

$protectedSetting = @{
    "defenderForEndpointOnboardingScript" = ($mdePackage.content | ConvertFrom-
Json).value.properties.onboardingPackageWindows
}

$Setting = @{
    "azureResourceId" = $vm.Id
    "vNextEnabled" = $true
}
New-AzConnectedMachineExtension -Name 'MDE.Windows' -ExtensionType 'MDE.Windows' -
ResourceGroupName $vm.ResourceGroupName -MachineName $vm.Name -Location
$vm.Location -Publisher 'Microsoft.Azure.AzureDefenderForServers' -Settings
$Setting -ProtectedSetting $protectedSetting -AutoUpgradeMinorVersion -
TypeHandlerVersion '1.0'
```

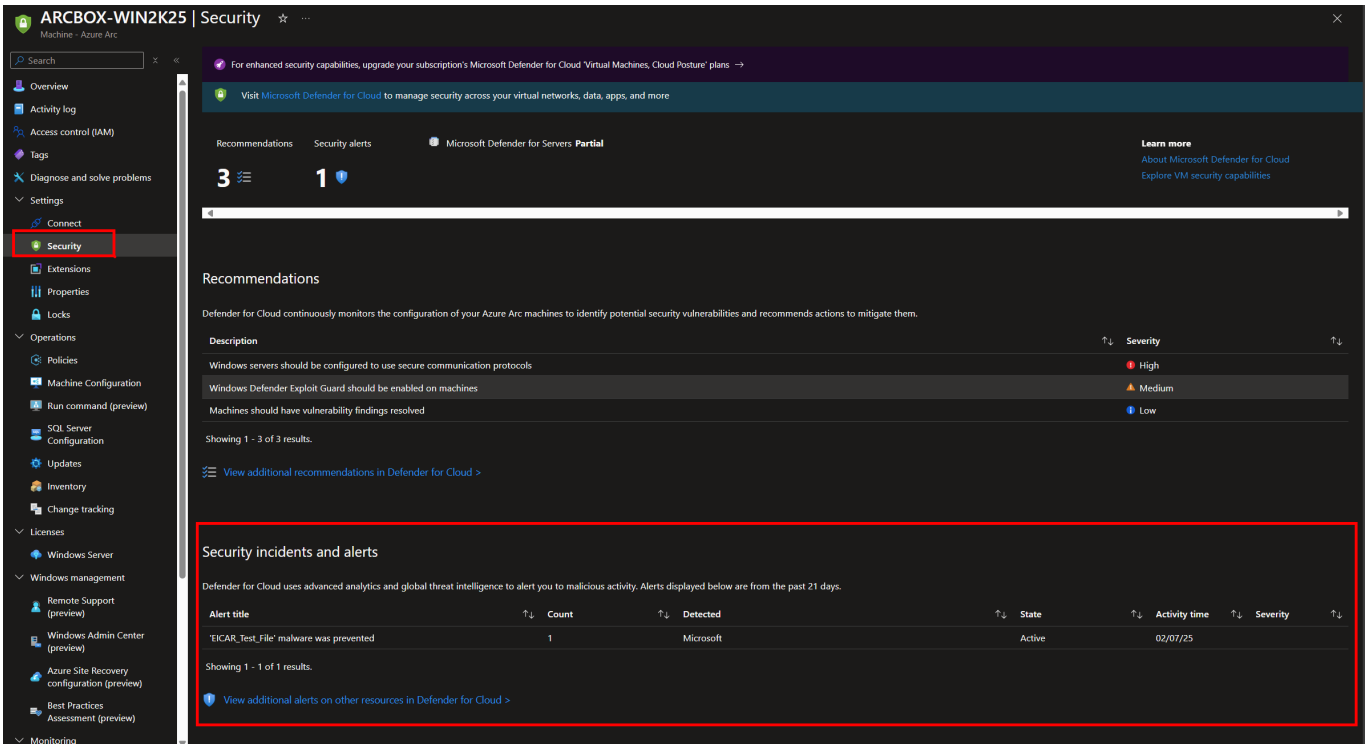
3. [] Wait for the installation of the MDE.Windows extension to be successful, then on the *ArcBox-Client* VM, go to Hyper-V manager and logon to the *ArcBox-Win2k25* VM using *JS123!!* as the Administrator password. Create an empty text file in the C: drive. Use the browser to open this site and find the malware test string. Copy the test string to the empty text file you created and save it as test.txt on the C: drive.



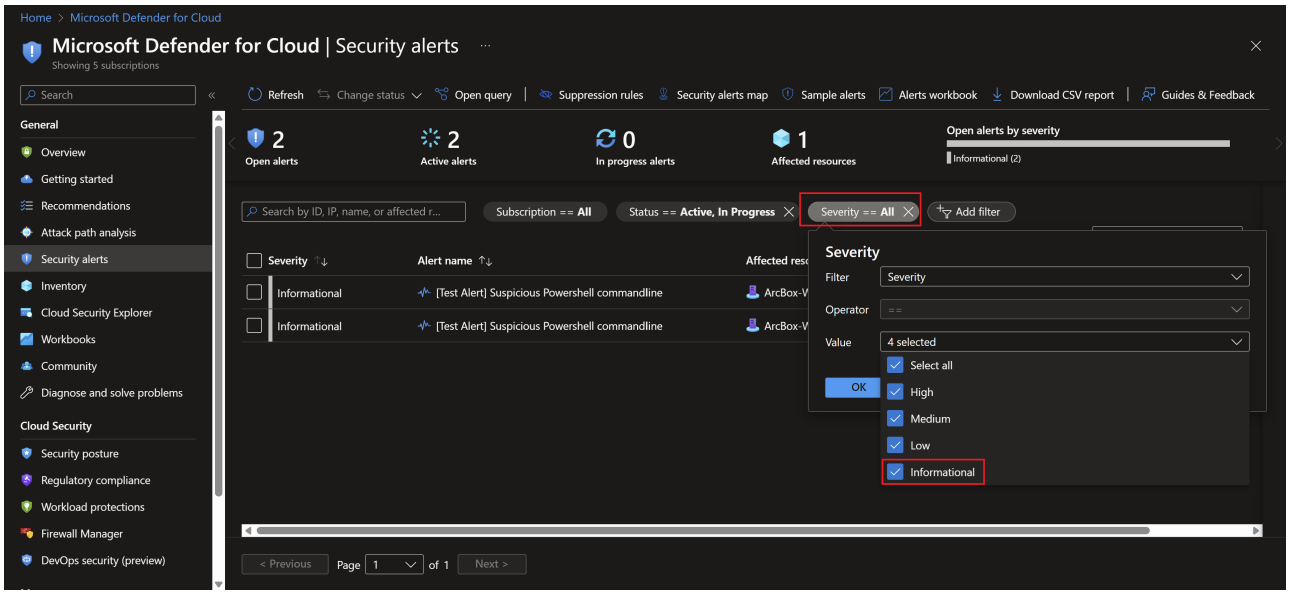
4. [] The local Anti-Malware software should detect this simulated threat on the ArcBox-Win2k25 VM. Navigate to the Security tab of the *ArcBox-Win2k25* Arc-enabled server in the portal

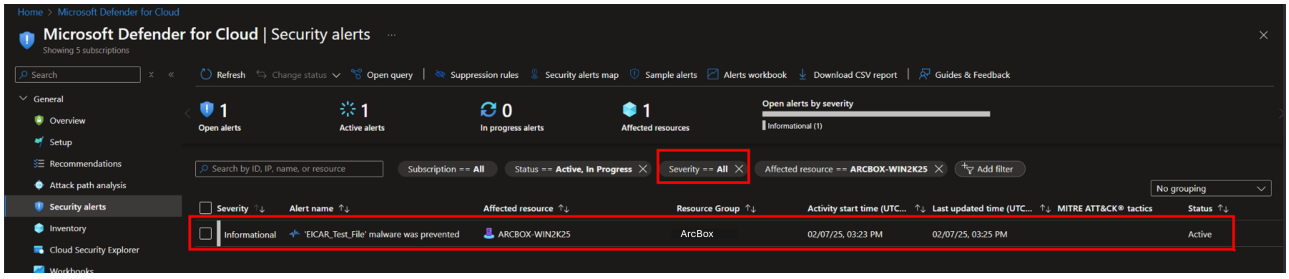
> [!hint] **It might take up to 20 minutes or more for the alert to show up in the portal, you can move to the next exercise or lab and come back later to see the results if you prefer. This way, you can make better use of your time in this workshop**.





5. [] You can also see the alerts from the *Defender for Cloud* portal, in the *Security alerts* pane. **If you don't see the alerts, make sure to select the Information severity in the filters.**.





Task 1 has been completed

===

Exercise 2 - Configure vulnerability assessment on your machines

Objective

This exercise will walk you through enabling a vulnerability assessment solution on your machines.

Estimated Time to Complete This Lab

20 minutes

Explanation

In this exercise, you will learn how to configure a vulnerability assessment on your machines and view detected vulnerabilities.

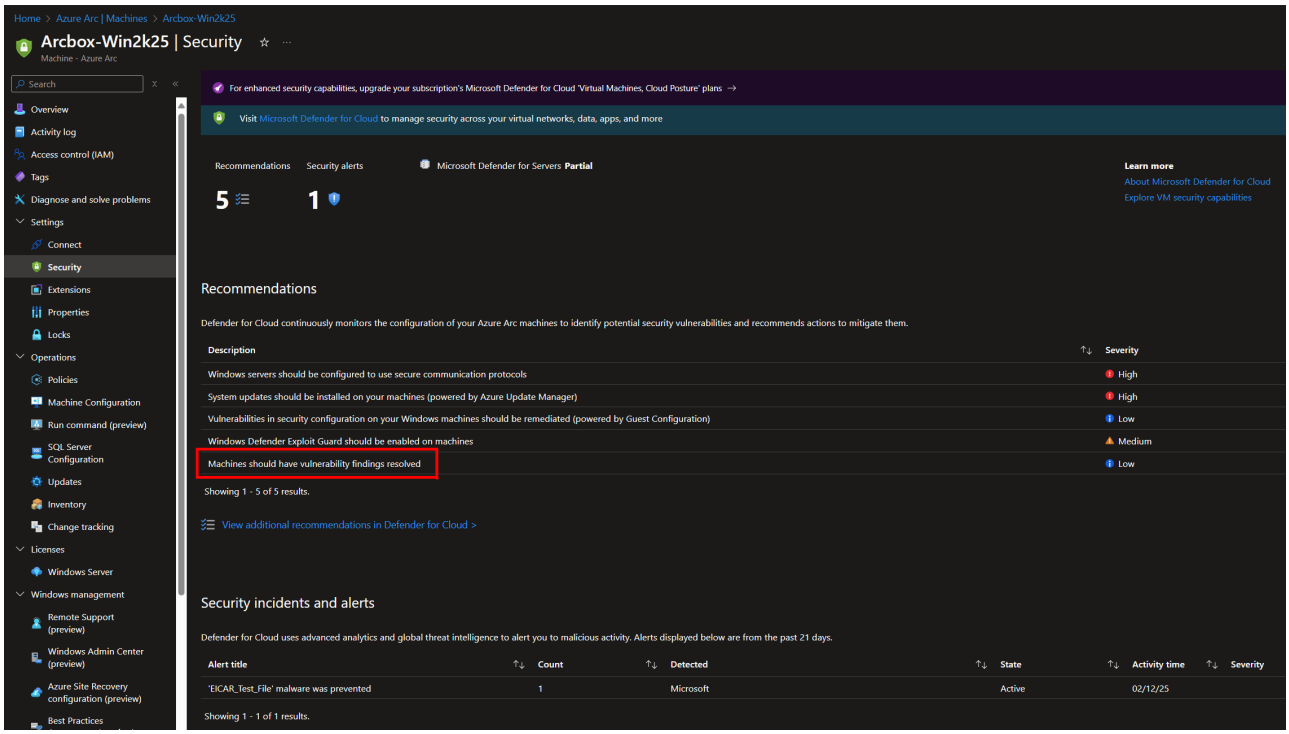
===

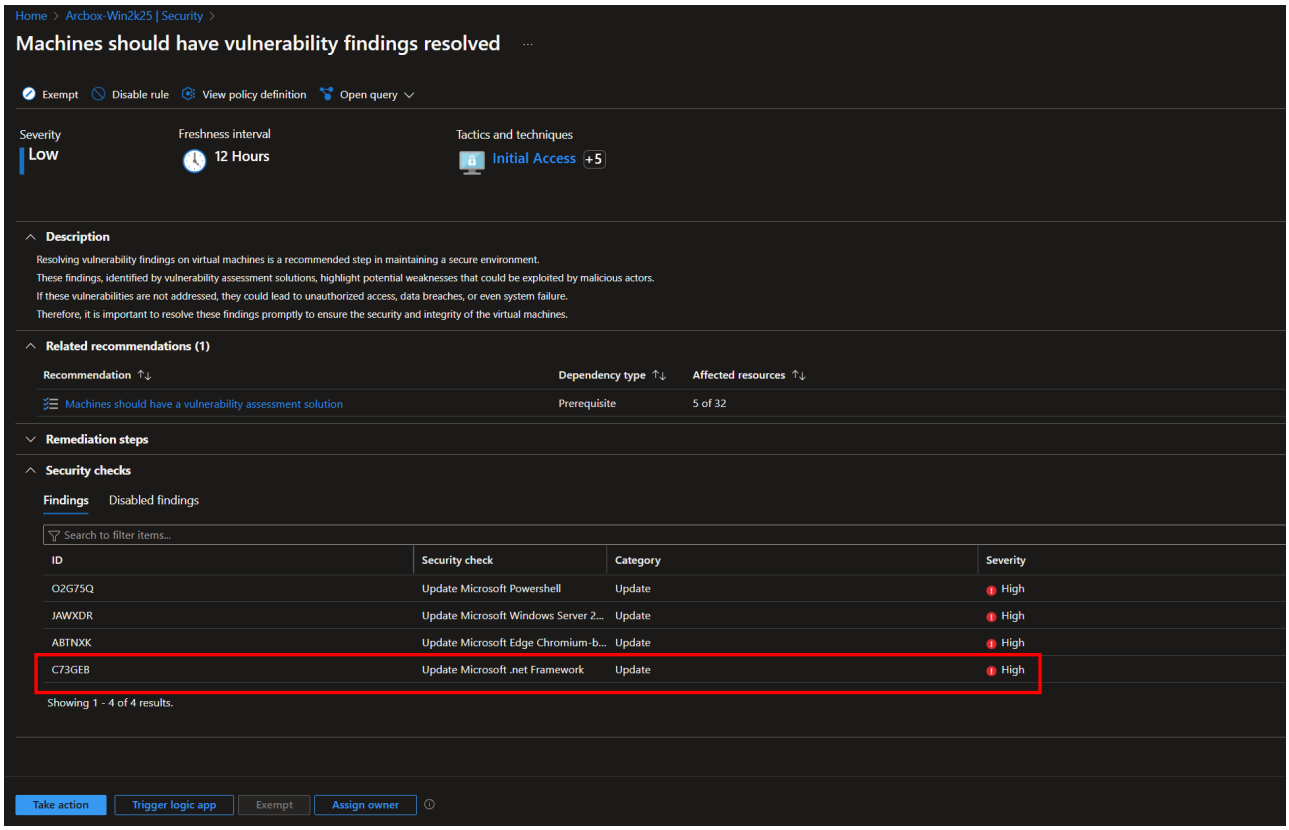
Task 1: Configure vulnerability assessment on your machines

1. [] After about 20-30 minutes from setting up Defender plans for servers (done in Lab01), you should start seeing recommendations for the Arc-enabled machines in the "Security" blade.

> [!NOTE]: **On rare occasions, it might take much longer before the recommendations start to appear**

2. [] You should find the recommendation *Machines should have vulnerability findings resolved* if the vulnerability assessment has been enabled automatically on the subscription. Click on the recommendation.

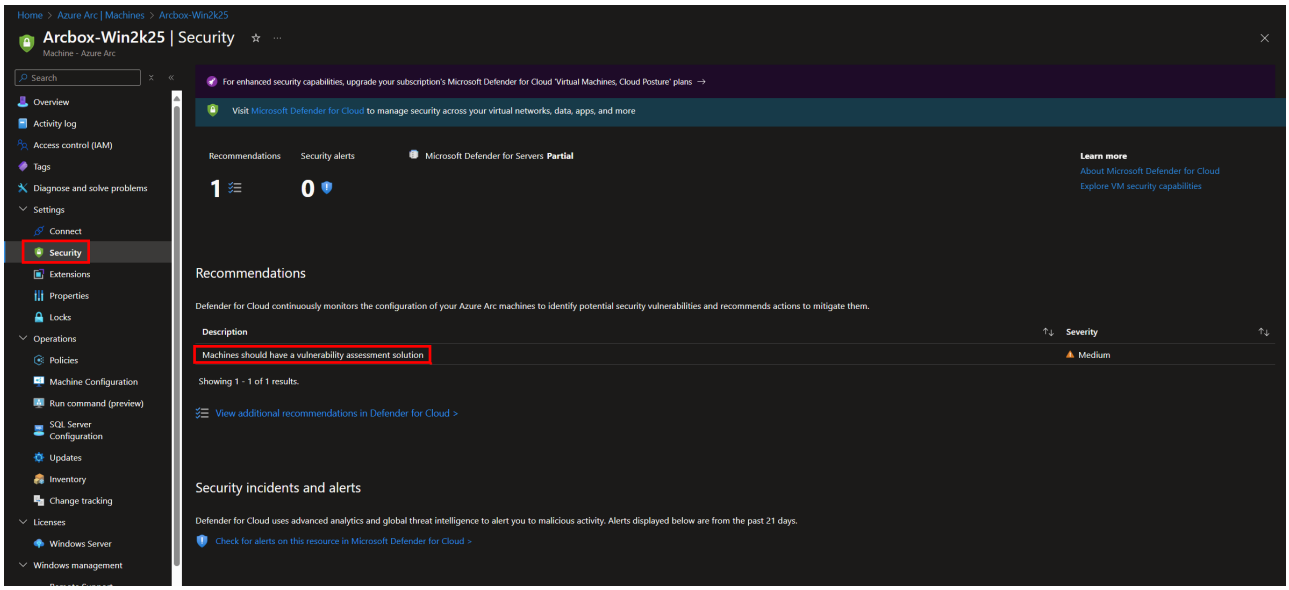




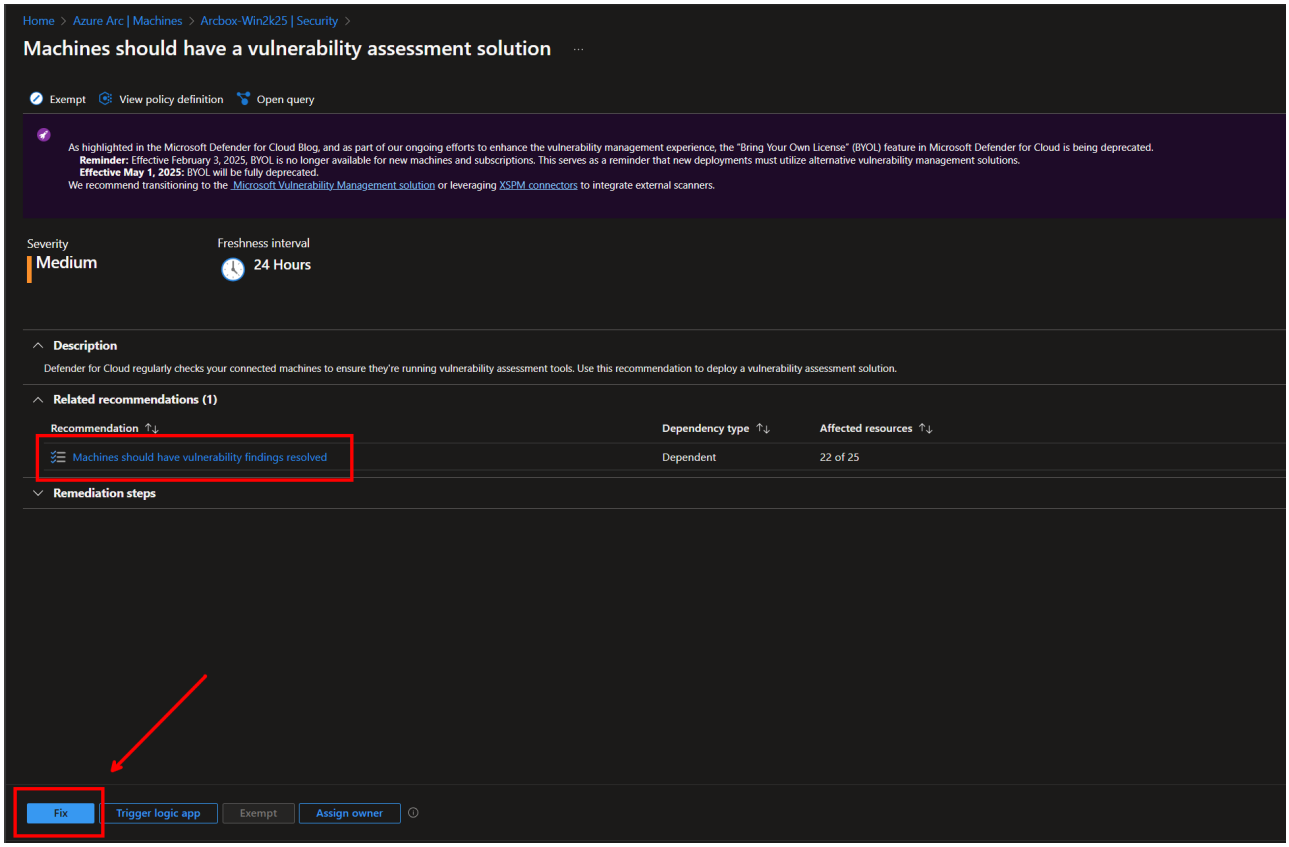
.

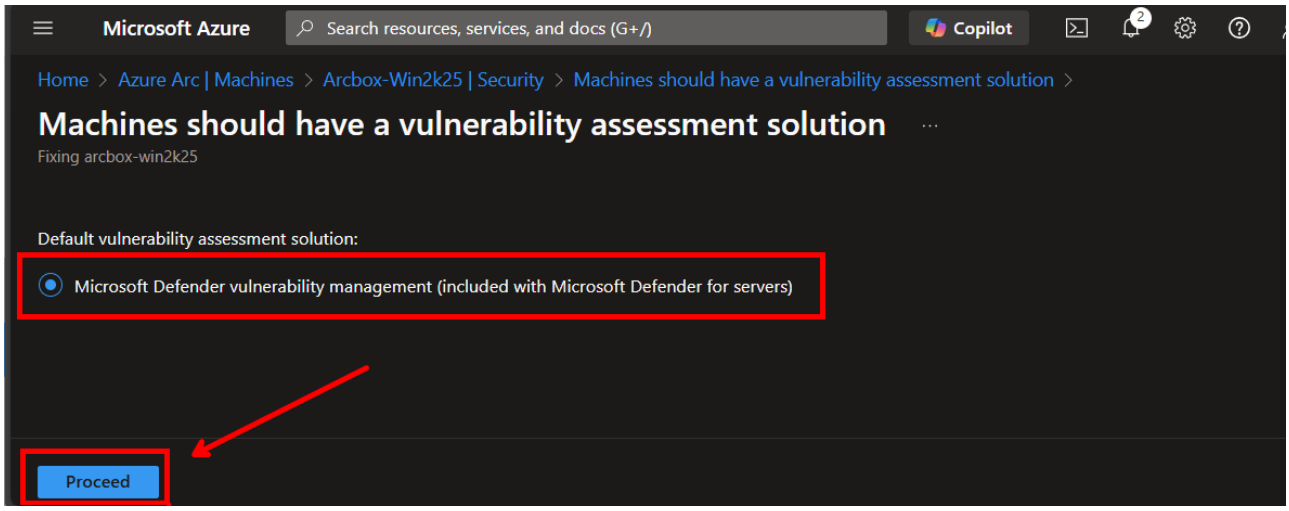
This means that Vulnerability Assessment is working on the server and you can end this lab at this point.

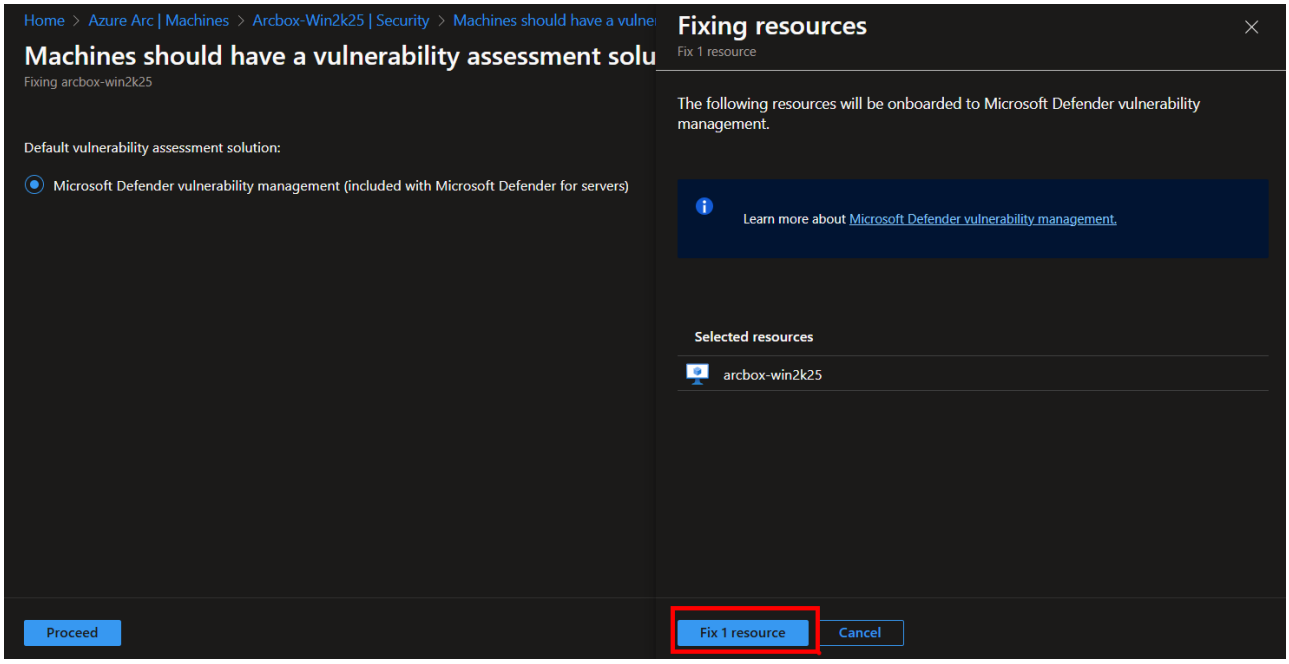
3. [] If you do not see this recommendation, click on the *Machines should have a vulnerability assessment solution*

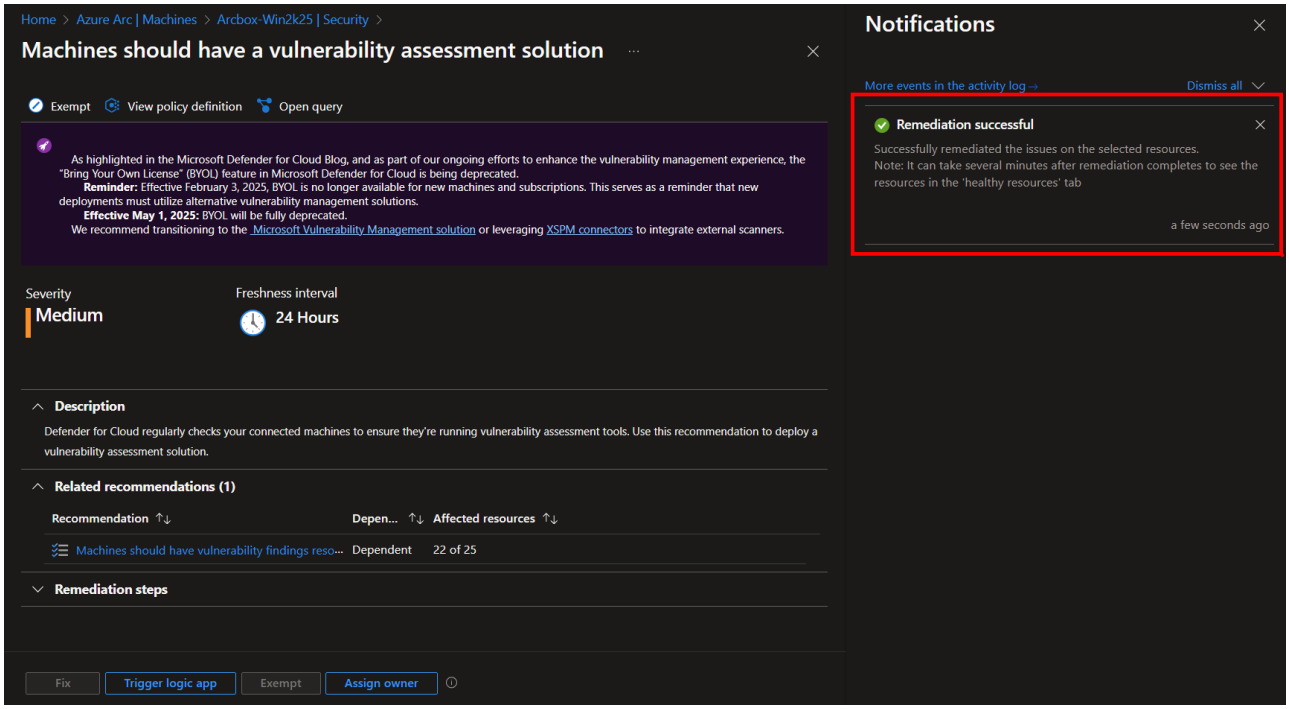


4. [] Click on the "Machines should have a vulnerability assessment solution" recommendation and click "Fix"









> [!hint]: **The same steps can be applied to the Linux Arc-enabled machines**

Task 1 has been completed

===

Congratulations, you have completed all tasks in this lab

Click **Next** for the next lab or **Go back to the main table of content**