

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

Task 1 - Simulate malicious activities

Exercise 2 - Enable vulnerability assessment

Task 1 - Configure vulnerability assessment on your machines

====

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.

The screenshot shows the 'Extensions' blade for a machine named 'Arcbox-Win2k25'. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Connect, Security), and Extensions. The main area displays a list of extensions with columns for Name, Type, Version, Update available, Status, and Automatic upgrade. The 'MDE.Windows' extension is highlighted with a red box.

Name	Type	Version	Update available	Status	Automatic upgrade
MDE.Windows	MDE.Windows	1.0.11.3	No	Succeeded	Not supported
WindowsPatchExtension	WindowsPatchExtension	1.5.71	No	Succeeded	Enabled
AzureMonitorWindowsAg...	AzureMonitorWindowsAg...	1.31.0.0	No	Succeeded	Enabled
ChangeTracking-Windows	ChangeTracking-Windows	2.27.0.0	No	Succeeded	Enabled

[!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.

The screenshot shows the EICAR website with the title "THE ANTI-MALWARE TESTFILE". A red box highlights the test string: "X5O!P%@AP[4!PZX54(P^)7CC]7\$EICAR-STANDARD-ANTIVIRUS-TESTFILE!\$H+H*". Below this, a note states: "The first 68 characters is the known string. It may be optionally appended by any combination of whitespace characters with the total file length not exceeding 128 characters. The only whitespace characters allowed are the space character, tab, LF, CR, CTRL-Z. To keep things simple the file uses only upper case letters, digits and punctuation marks, and does not include spaces. The only thing to watch out for when typing in the test file is that the third character is the capital letter 'O', not the digit zero."

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.

The screenshot shows the Windows File Explorer interface with a list of files in the Local Disk (C:) folder. A red box highlights the Windows Security window, which displays a "Virus & threat protection" alert. The alert message says: "Review files that Windows Defender will send to Microsoft. Sending us this information can improve how Windows Defender Antivirus helps protect your device. 8:35 AM". There are "Send files" and "Review" buttons at the bottom.

The screenshot shows the Azure ArcBox-WIN2K25 Security blade. On the left, a navigation menu includes 'Security' (which is highlighted with a red box). The main area displays 'Recommendations' (3) and 'Security alerts' (1). A section titled 'Recommendations' lists three items: 'Windows servers should be configured to use secure communication protocols' (High severity), 'Windows Defender Exploit Guard should be enabled on machines' (Medium severity), and 'Machines should have vulnerability findings resolved' (Low severity). Below this is a 'Security incidents and alerts' section, also highlighted with a red box. It shows one alert: "'EICAR_Test_File' malware was prevented' (Detected by Microsoft, Active status, 02/07/25). A link to 'View additional alerts on other resources in Defender for Cloud' is present.

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..**

The screenshot shows the Microsoft Defender for Cloud Security alerts page. The left sidebar has 'Security alerts' selected. The main area shows 2 open alerts, 2 active alerts, 0 in-progress alerts, and 1 affected resource. A modal window is open over the alerts table, focusing on the 'Severity' filter. The 'Severity' dropdown is set to 'All'. A sub-menu is open with options: 'OK' (selected), 'Select all', 'High', 'Medium', 'Low', and 'Informational' (which is checked and highlighted with a red box). The main table below shows two alerts: '[Test Alert] Suspicious Powershell commandline' (Informational severity) and another '[Test Alert] Suspicious Powershell commandline' (Informational severity).

The screenshot shows the Microsoft Defender for Cloud Security alerts page. The left sidebar has 'Security alerts' selected. The main area shows 1 open alert, 1 active alert, 0 in-progress alerts, and 1 affected resource. A modal window is open over the alerts table, focusing on the 'Affected resource' filter. The 'Affected resource' dropdown is set to 'ARCBOX-WIN2K25' (highlighted with a red box). The main table shows one alert: "'EICAR_Test_File' malware was prevented' (Informational severity, Affected resource: ARCBOX-WIN2K25, Resource Group: ArcBox, Activity start time: 02/07/25, 03:23 PM, Last updated time: 02/07/25, 03:25 PM, Status: Active).

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.

Recommendations

- Windows servers should be configured to use secure communication protocols
- System updates should be installed on your machines (powered by Azure Update Manager)
- Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration)
- Windows Defender Exploit Guard should be enabled on machines
- Machines should have vulnerability findings resolved

Security incidents and alerts

Alert title	Count	Detected	State	Activity time	Severity
'ICAR.Test.File' malware was prevented	1	Microsoft	Active	02/12/25	High

Description

Resolving vulnerability findings on virtual machines is a recommended step in maintaining a secure environment. These findings, identified by vulnerability assessment solutions, highlight potential weaknesses that could be exploited by malicious actors. If these vulnerabilities are not addressed, they could lead to unauthorized access, data breaches, or even system failure. Therefore, it is important to resolve these findings promptly to ensure the security and integrity of the virtual machines.

Related recommendations (1)

Recommendation	Dependency type	Affected resources
Machines should have a vulnerability assessment solution	Prerequisite	5 of 32

Remediation steps

Security checks

Findings **Disabled findings**

ID	Security check	Category	Severity
OZG75Q	Update Microsoft Powershell	Update	High
JAWXDR	Update Microsoft Windows Server 2...	Update	High
ABTNXK	Update Microsoft Edge Chromium b...	Update	High
C73GEB	Update Microsoft .net Framework	Update	High

Showing 1 - 4 of 4 results.

Actions

- Take action
- Trigger logic app
- Exempt
- Assign owner

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

- If you do not see this recommendation, click on the *Machines should have a vulnerability assessment solution*

Home > Azure Arc | Machines > Arbox-Win2k25 | Security

Arbox-Win2k25 | Security

Machine - Azure Arc

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Connect
- Security** (highlighted)
- Extensions
- Properties
- Locks
- Operations
- Policies
- Machine Configuration
- Run command (preview)
- SQL Server Configuration
- Updates
- Inventory
- Change tracking
- Licenses
- Windows Server
- Windows management

For enhanced security capabilities, upgrade your subscription's Microsoft Defender for Cloud 'Virtual Machines, Cloud Posture' plans →

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Recommendations Security alerts Microsoft Defender for Servers Partial

Learn more About Microsoft Defender for Cloud Explore VM security capabilities

1 0

Recommendations

Defender for Cloud continuously monitors the configuration of your Azure Arc machines to identify potential security vulnerabilities and recommends actions to mitigate them.

Description	Severity
Machines should have a vulnerability assessment solution	Medium

Showing 1 - 1 of 1 results.

[View additional recommendations in Defender for Cloud >](#)

Security incidents and alerts

Defender for Cloud uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.

[Check for alerts on this resource in Microsoft Defender for Cloud >](#)

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

Home > Azure Arc | Machines > Arbox-Win2k25 | Security >

Machines should have a vulnerability assessment solution

Exempt View policy definition Open query

As highlighted in the Microsoft Defender for Cloud Blog, and as part of our ongoing efforts to enhance the vulnerability management experience, the "Bring Your Own License" (BYOL) feature in Microsoft Defender for Cloud is being deprecated. **Reminder:** Effective February 3, 2025, BYOL is no longer available for new machines and subscriptions. This serves as a reminder that new deployments must utilize alternative vulnerability management solutions. **Effective May 1, 2025:** BYOL will be fully deprecated. We recommend transitioning to the [Microsoft Vulnerability Management solution](#) or leveraging [XSPM connectors](#) to integrate external scanners.

Severity: Medium Freshness interval: 24 Hours

Description
Defender for Cloud regularly checks your connected machines to ensure they're running vulnerability assessment tools. Use this recommendation to deploy a vulnerability assessment solution.

Related recommendations (1)

Recommendation	Dependency type	Affected resources
Machines should have vulnerability findings resolved	Dependent	22 of 25

Remediation steps

Fix Trigger logic app Exempt Assign owner

Default vulnerability assessment solution:

- Microsoft Defender vulnerability management (included with Microsoft Defender for servers)

Proceed

Fixing resources

Fix 1 resource

The following resources will be onboarded to Microsoft Defender vulnerability management.

Selected resources

arcbox-win2k25

Fix 1 resource **Cancel**

Home > Azure Arc | Machines > Arcbox-Win2k25 | Security >

Machines should have a vulnerability assessment solution

Exempt View policy definition Open query

As highlighted in the Microsoft Defender for Cloud Blog, and as part of our ongoing efforts to enhance the vulnerability management experience, the "Bring Your Own License" (BYOL) feature in Microsoft Defender for Cloud is being deprecated.

Reminder: Effective February 3, 2025, BYOL is no longer available for new machines and subscriptions. This serves as a reminder that new deployments must utilize alternative vulnerability management solutions.

Effective May 1, 2025: BYOL will be fully deprecated.

We recommend transitioning to the [Microsoft Vulnerability Management solution](#) or leveraging [XPM connectors](#) to integrate external scanners.

Severity	Freshness interval
Medium	24 Hours

Description
Defender for Cloud regularly checks your connected machines to ensure they're running vulnerability assessment tools. Use this recommendation to deploy a vulnerability assessment solution.

Related recommendations (1)

Recommendation	Depen...	Affected resources
Machines should have vulnerability findings reso...	Dependent	22 of 25

Remediation steps

Fix **Trigger logic app** **Exempt** **Assign owner**

More events in the activity log → Dismiss all

Remediation successful ×
Successfully remediated the issues on the selected resources.
Note: It can take several minutes after remediation completes to see the resources in the 'healthy resources' tab

a few seconds ago

[!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**