Lab #6: Setup of Microsoft Defender for Cloud Logging

Purpose:

• We'll be enabling **Microsoft Defender for Cloud**, which gives us a high-level security view of an Azure environment. I'll also be configuring Defender logs to be forwarded to our Log Analytics workspace.

Tasks:

- 1. Enable Microsoft Defender for Cloud (Log Analytics)
- 2. Enable Microsoft Defender for Cloud (Subscription)
- 3. Enable Microsoft Defender for Cloud (Continuous Export)

Task 1: Enable Microsoft Defender for Cloud (Log Analytics)

<u>Note</u>: This will allow us to forward logs from our "tester" VMs to our Log Analytics workspace.

- 1. Azure account (portal.azure.com) > Microsoft Defender for Cloud > Environment Settings.
- Scroll down to the lower table > under Name, expand our subscription to view our workspace > select the "options" icon to the right, and then select Edit Settings.

Name ↑↓	Total resources \uparrow_\downarrow	Connectivity status	Defender coverage $\uparrow \downarrow$
V 🛆 Azure			
✓	6		0/12 plans ***
.	•		0/2 plans
		C	Edit settings

3. In the **Defender plans** tab, update the **Servers** and **SQL servers** plans to <u>ON</u> > **Save**.

Plan	Pricing	Resource quantity	Plan
Foundational CSPM	Free		On Off
Servers	\$15/Server/Month O	0 servers	On Off
SQL servers on machines	\$15/Server/Month \$0.015/Care/Hour	0 servers	On Off

<u>Note</u>: This allows us to collect logs from these plans.

4. In the Data collection tab, select All Events > Save.

<u>**Note</u>**: This allows us to collect all events from the Windows security logs and forward them to our Log Analytics workspace.</u>

Task 2: Enable Microsoft Defender for Cloud (Subscription)

- 1. Azure portal > Microsoft Defender for Cloud > select Environment Settings.
- Scroll down to the lower table > under Name, locate our subscription > select the "options" icon to the right, and then select Edit Settings.



- 3. Go to the **Defender plans** tab.
 - a. Switch these plans to $ON \rightarrow Servers$, Databases, Storage, Key Vault.
 - b. Under the "Servers" plan, select Settings > Under "Log Analytics agent, select Edit configuration > select Custome workspace radio button, and select the workspace > Apply.
 c. Select Continue (top left) > select Save (top left).

Note: This allows us to forward our "tester" VM logs to our Log Analytics workspace.

Task 3: Enable Microsoft Defender for Cloud (Continuous Export)

- 1. Azure portal > Microsoft Defender for Cloud > select Environment Settings.
- 2. Scroll down to the lower table > under **Name**, locate our subscription > select the "options" icon to the right, and then select **Edit Settings**.



- 3. At the **Continuous export** tab > select the **Log Analytics workspace** tab.
 - a. **Export** should be enabled (ON).

Event hub	Log Analytics workspace	
Export enabl	ed On	Off

<u>Note</u>: This will allow alerts to be exported into my Log Analytics workspace, allowing us to query these alerts later.

b. Update the **Exported data types** settings:

Security recommendations	All recommendations selected \checkmark
Recommendation severity \star	Low,Medium,High 🗸
Include security findings 🛈	Yes
Secure score ①	Overall score
Security alerts	Low,Medium,High,Informational
Regulatory compliance	All standards selected \checkmark

- c. **Export configuration > Resource group**: (the "Tester" resource group).
- d. Export target > Subscription, Target workspace > Select Save.

End:

• Defender logs will now be forwarded to our Log Analytics workspace. Soon, we'll manually install agents to assist with automatically forward logs to our Log Analytics workspace.