**Module 17 –Defender CSPM**

#### Level: 200 (Intermediate)

#### ⌛ Estimated time to complete this lab: 30 minutes

## **Objectives**

In this exercise, you will learn how to enable Defender for CSPM, and leverage Defender for CSPM Capabilities

### **Exercise 1: Preparing the Environment for DCSPM plan**

# If you already finished [Module 1](https://github.com/Azure/Microsoft-Defender-for-Cloud/blob/main/Labs/Modules/Module-1-Preparing-the-Environment.md) of this lab, (Module 1 – Preparing the Environment), you will deploy an extended environment for Defender CSPM plan.

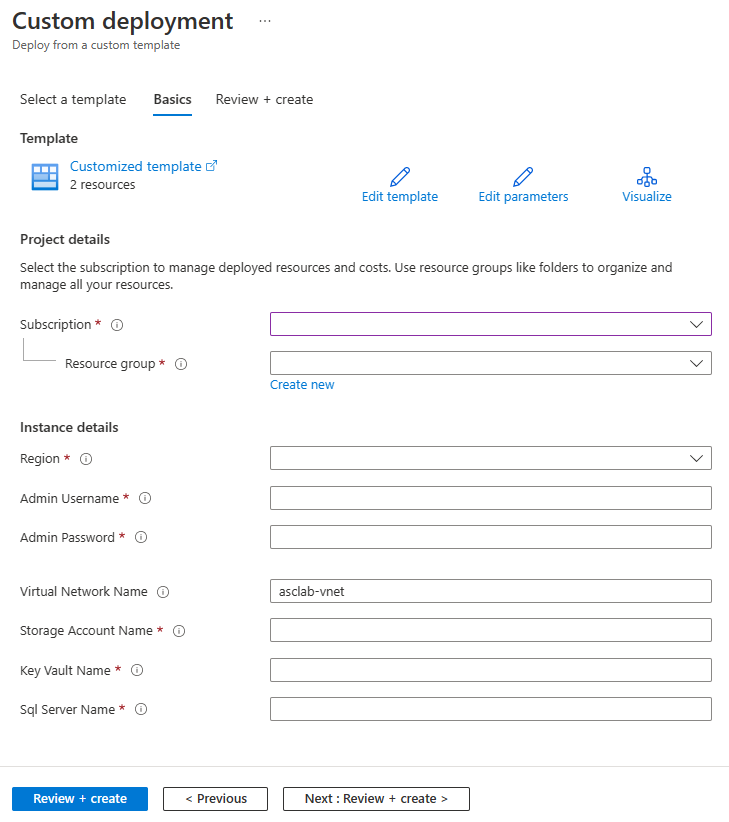
As part of this exercise, you will create an environment using an automated deployment based on ARM template. An ARM template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project. The template uses declarative syntax, which lets you state what you intend to deploy without having to write the sequence of programming commands to create it. The following list of resources will be deployed during the provisioning process (including dependencies like disks, network interfaces, public IP addresses, etc.):

| **Name** | **Resource Type** | **Purpose** |
| --- | --- | --- |
| dcspmlab-winsrv | Virtual machine | Windows Server |
| dcspmlab-nix | Virtual machine | Linux Server |

1. Prepare your lab environment by clicking on the blue **Deploy to Azure** button below:

[](https://raw.githubusercontent.com/Azure/Microsoft-Defender-for-Cloud/main/Labs/Files/dcspmlabdeploy.json)

1. You will be redirected to Azure Portal > custom deployment page where you should specify mandatory fields for deployment.



1. On the subscription field, select **Azure subscription 1**.
2. On the resource group field, click on **select existing** and select **asclab** (you can pick any name you want or keep the default).
3. On the parameters section, select the data center **region** you deployed the ARM Template in Module 1 (all downstream resources will be created in the same region as the resource group).
4. Select **Admin Username** and **Admin password** that will be used for Windows Virtual Machine and Linux Virtual Machine you are deploying.

Notice that password must be between 12 and 72 characters and have 3 of the following: 1 lower case, 1 upper case, 1 number and 1 special character.

1. Select **Storage Account Name** (asclabsa[uniqestring]), **Key Vault Name** (asclab-kv-[uniqestring]), and **Sql Server Name** (asclab-sql-[uniqestring]) you already deployed in Module 1.
2. Click **Review + create** to start the validation process. Once validation passed, click on **Create** to start the ARM deployment on your subscription.
3. The deployment takes about **10 minutes** to complete.

The *deployment is in progress* page continues to update and show the resources being uploaded to the environment assuming the deployment is successful.

You can also check the progress of your deployment if you click on your created resource group details, then click on **Deployments** (*1 deploying*).

When the deployment is complete, you should see the following:

| **Name** | **Resource Type** | **Purpose** |
| --- | --- | --- |
| dcspmlab-winsrv | Virtual machine | Windows Server |
| dcspmlab-nix | Virtual machine | Linux Server |

### **Exercise 2: Enabling Defender CSPM plan**

To gain access to the capabilities provided by Defender CSPM, you'll need to [enable the Defender Cloud Security Posture Management (CSPM) plan](https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security) on your subscription

1. Open **Azure Portal** and navigate to **Microsoft Defender for Cloud** blade.
2. From Defender for Cloud's menu, open the **Environment Settings** page and select the relevant subscription.
3. In the [Defender plans page](https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/pricingTier), select **Defender CSPM turn the status to ON** and select **Settings under Monitoring Coverage**.
4. Turn **ON** the **Agentless scanning for machines (preview)** and click **continue**
5. Click on **Save** to save the changes

Agentless scanning for VMs provides vulnerability assessment and software inventory in 24 hours. Leave the setup and comeback after 24 hours.

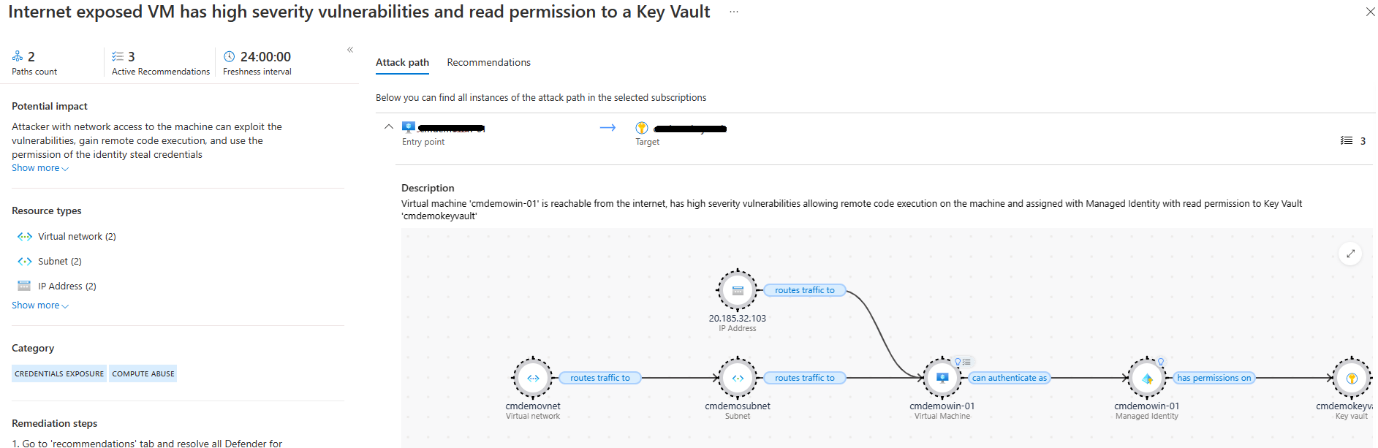
### **Exercise 3: Explore Attack Paths in your Environment**

1. Open **Azure Portal** and navigate to **Microsoft Defender for Cloud** blade.
2. From Defender for Cloud's menu, open the **Recommendations** page
3. You will find Attack path tab as below:

Graphical user interface, text, application, email

Description automatically generated

1. Click on Attack path. You will find the Attack Paths in your Environment.
2. Click on “Internet exposed VM has High severity vulnerabilities and read permission to key vault”



1. You can observe the Attack path and the resources involved in the attack path.
2. Remediate the recommendations to resolve the attack path
3. Explore the rest of the Attack paths found in your Environment and remidiate

### **Exercise 4: Build query with Cloud Security Explorer**

1. Open **Azure Portal** and navigate to **Microsoft Defender for Cloud** blade.
2. From Defender for Cloud's menu, open the **Cloud Security Explorer(preview)** page

Graphical user interface, application

Description automatically generated

1. Select a predefined query Template “**Internet exposed VMs with high severity vulnerabilities**” and click on Search
2. You will find the list of VMs with high severity Vulnerabilities.
3. Select a predefined query Template “**Internet exposed SQL servers with managed identity**” and click on Search
4. You will find the list of SQL servers with managed identity.
5. You can also explore and build your own queries using query builder as shown below: In the dropdown select ->Virtual machines ->Insight ->Title -> vulnerable to remote code execution.



1. Explore your Environment for Virtual Machines with a specific vulnerability

Graphical user interface, application

Description automatically generated

1. Explore your Environment for Storage Accounts exposed to the Internet

Graphical user interface, application

Description automatically generated

1. Explore your Environment for Virtual machines with a managed identity

Table

Description automatically generated with medium confidence

### **Exercise 5: Assign Governance Rule**

1. Open **Azure Portal** and navigate to **Microsoft Defender for Cloud** blade.
2. From Defender for Cloud's menu, open the **Environment Settings** page and select the relevant subscription.
3. Under **settings** Select **Governance Rules(Preview)**
4. Click on **+Create governance rule**
5. Give a **rule name,** select **scope** at subscription level, priority 100
6. Under **conditions**, select **By severity** -> **High**, **Owner** -> **By email address**, specify the email address of the workload owner to receive notification email, **Remediation timeframe** -> **90 days**
7. **Notify Owners weekly about open and overdue tasks** and click **Save**.

Graphical user interface, text, application, email

Description automatically generated

1. Click on Governance report to view the status of tasks Complete, Overdue, Ontime, Unassign

