**Module 20 –Contextual Security capabilities for AWS using Defender CSPM**

#### Level: 200 (Intermediate)

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

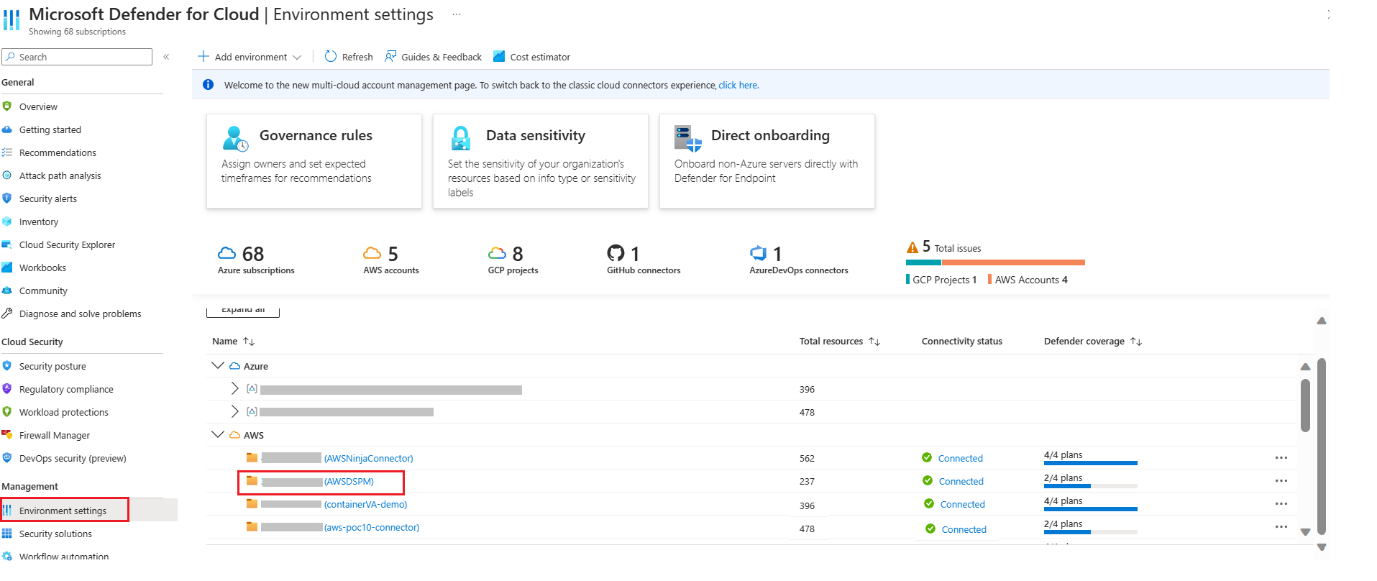
## **Objectives**

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

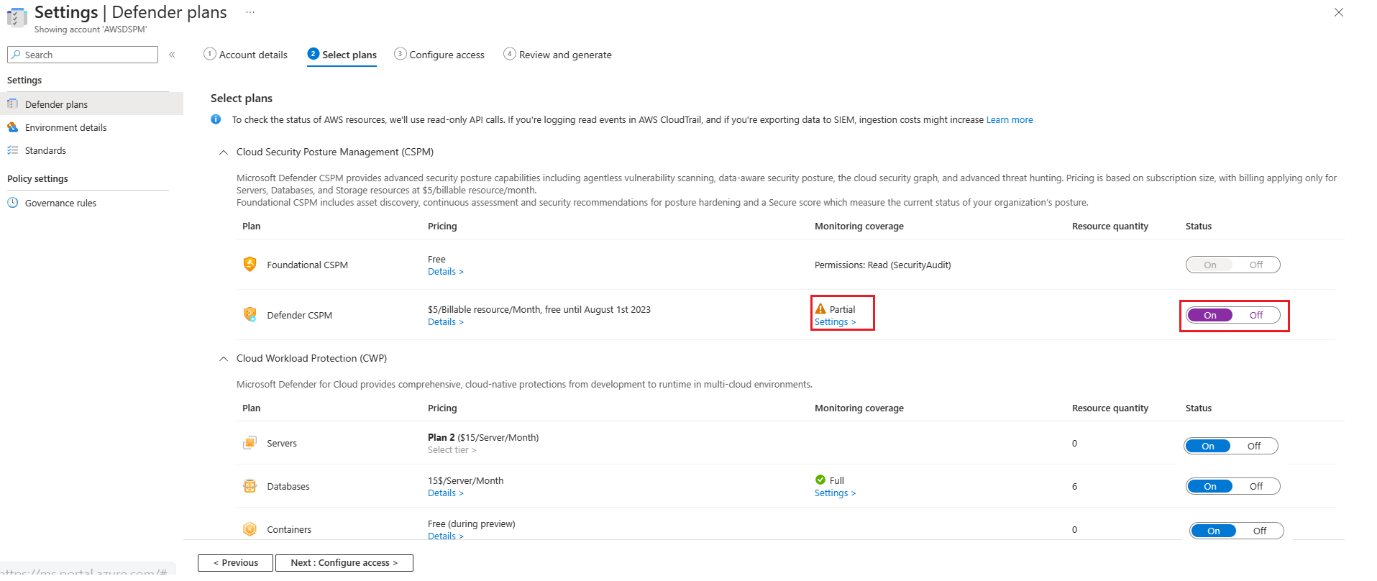
### **Exercise 1: Preparing the AWS Environment for Defender CSPM plan**

# If you already finished [Module 11](https://github.com/Azure/Microsoft-Defender-for-Cloud/blob/main/Labs/Modules/Module-11-AWS.md)of this lab, (Module 11 – Connecting an AWS Account, Preparing the Environment), you will deploy an extended environment for Defender CSPM plan.

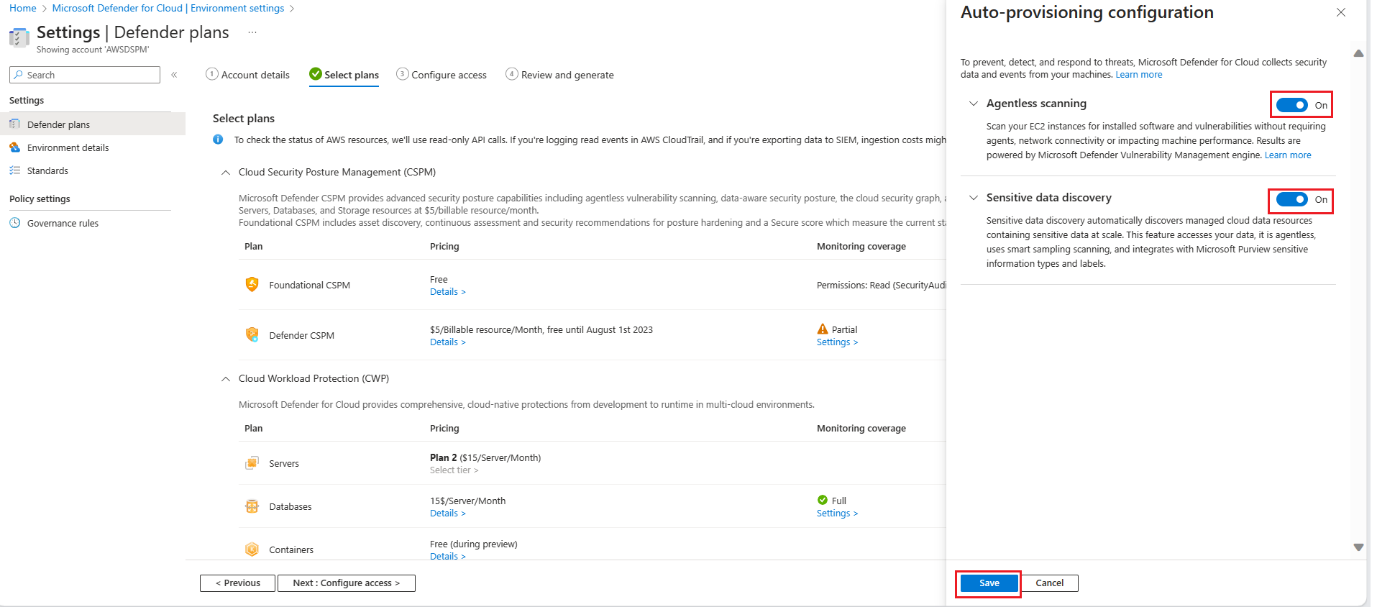
1. Sign in to the Azure portal.
2. Navigate to **Defender for Cloud**, then go to **Environment settings**.
3. Select an onboarded AWS Connector



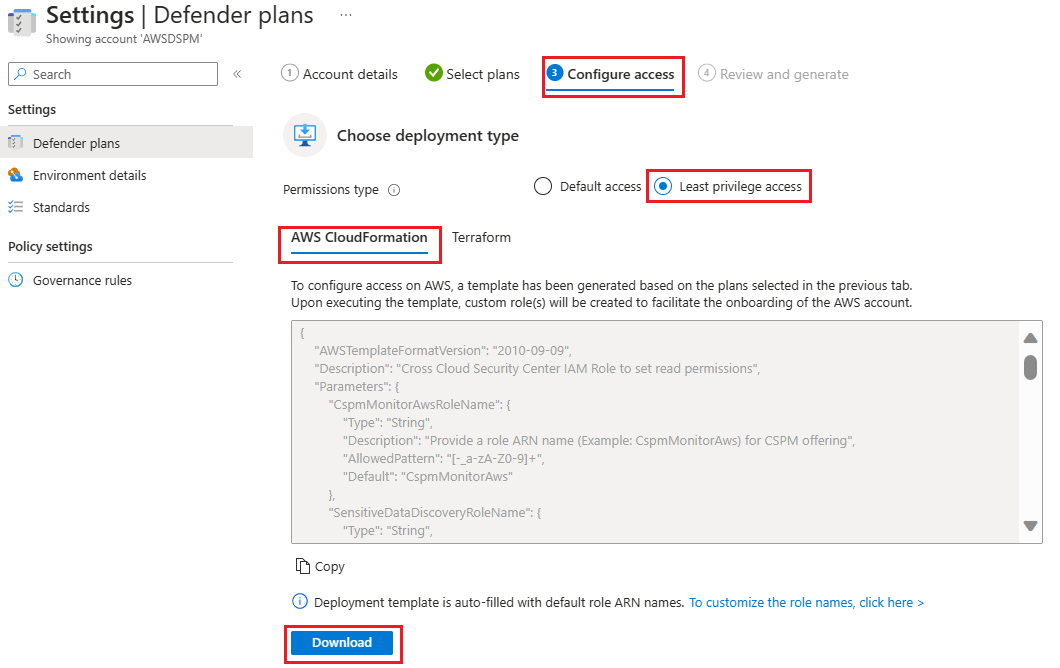
1. Under **Select Plans** -> Turn **Defender CSPM** to **ON** and click on **settings**



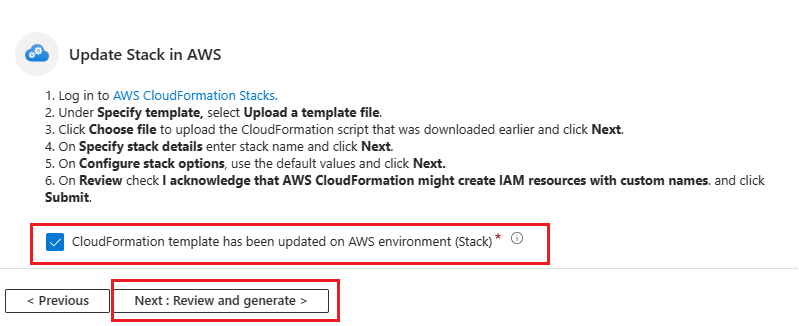
1. Under **Auto-provisioning configuration**, Turn On **Agentless Scanning** and **Sensitive Data Discovery** capabilities and click **Save**.



1. Click Next: Configure Access

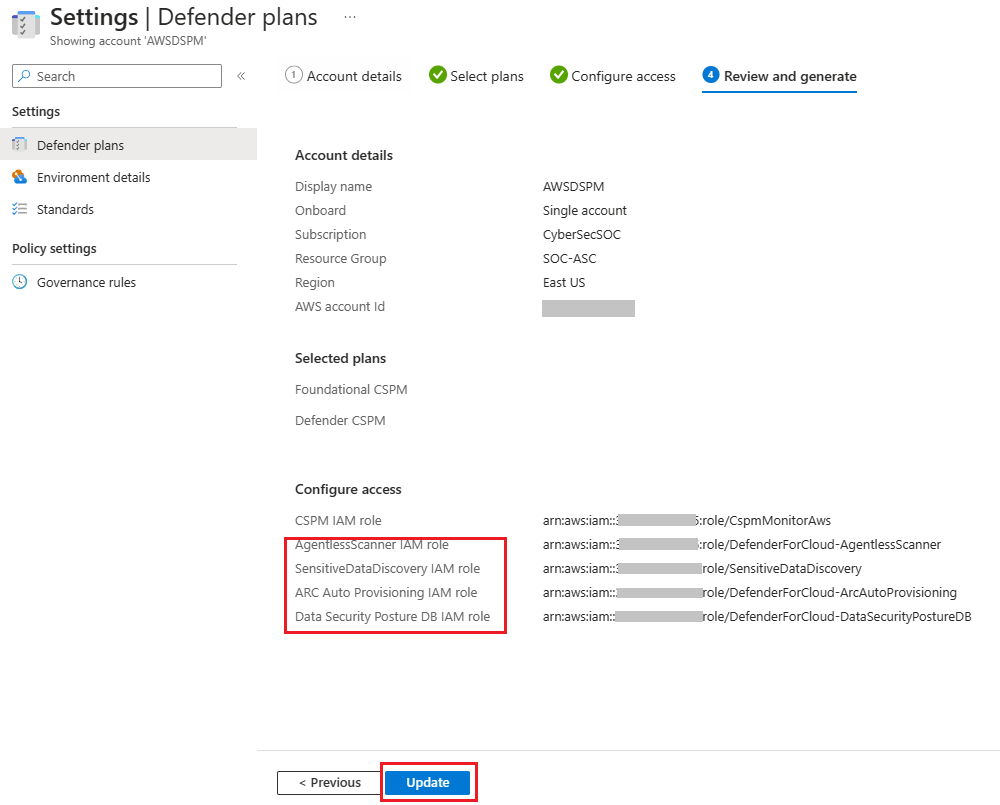


1. Choose a deployment method: **AWS CloudFormation** or **Terraform** and **Download** the Template
2. Under update stack in AWS, select the checkbox **CloudFormation template has been updated on AWS environment** and click **Review and Generate**

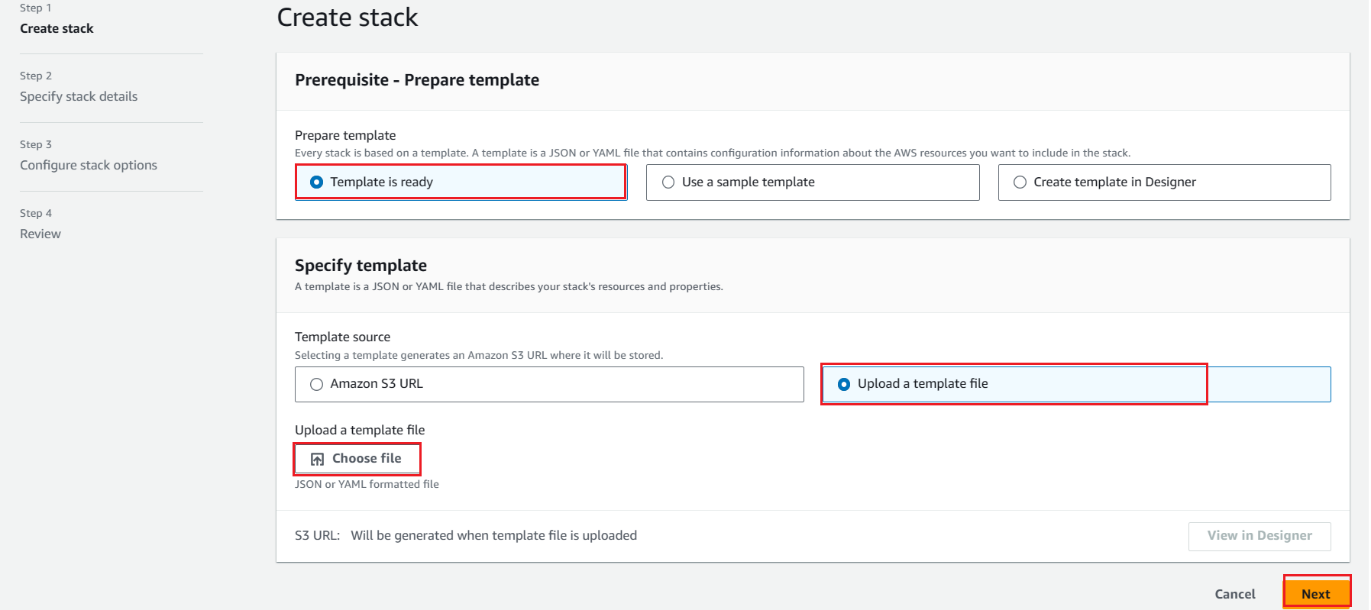


1. Observe the new IAM roles are created for Defender CSPM plan. Click on Update

*Note: Updating plan selection requires an update of the CloudFormation template to add or remove access roles. Without performing this action, Defender will only have partial access to your environment.*

**

1. Deploy the CloudFormation template by using Stack

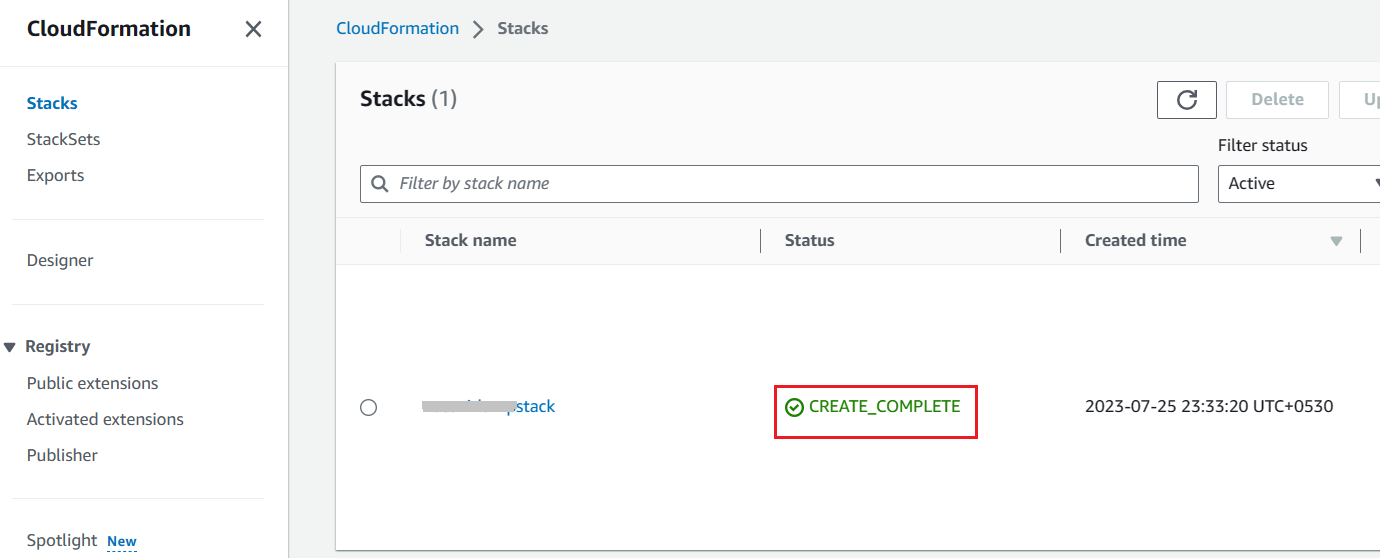
**

1. Upload the downloaded CloudFormation template and click Next
2. Specify a stack name and click Next and Submit.

A screenshot of a computer

Description automatically generated

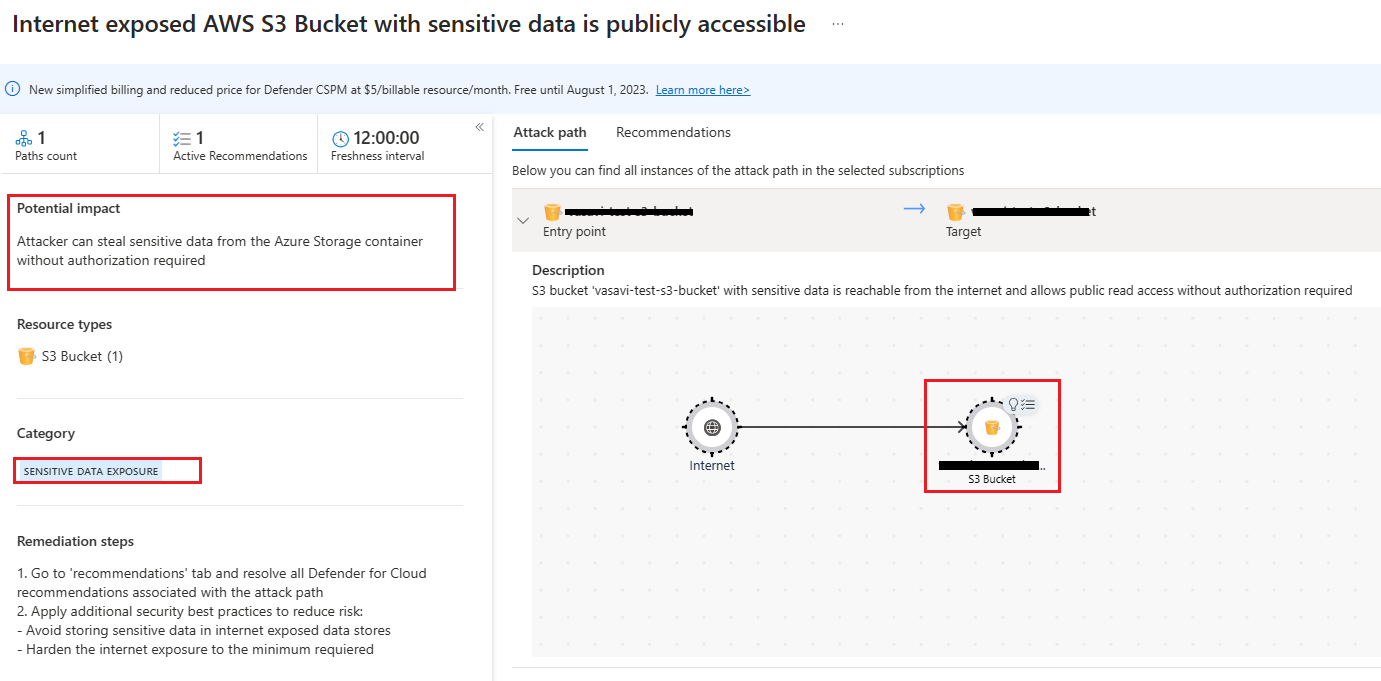
1. Wait till the Stack deployment is complete



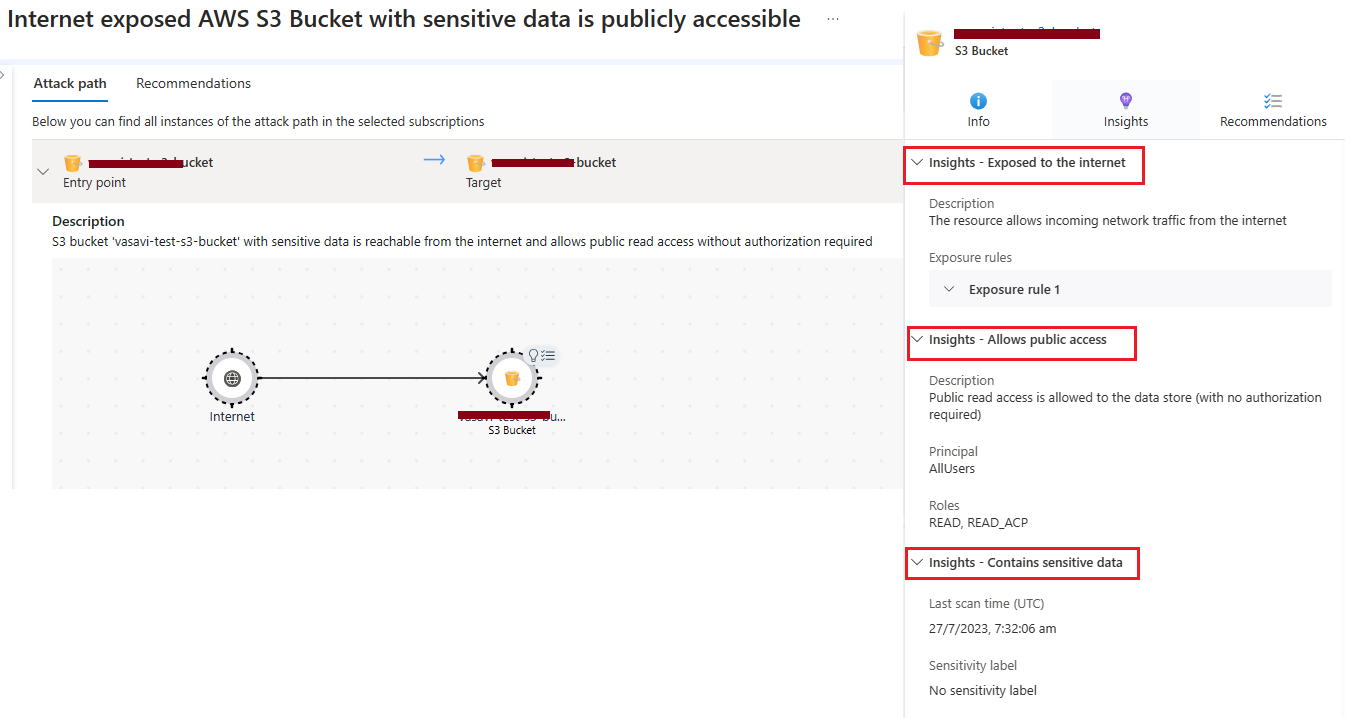
1. In the AWS Console deploy the AWS Resources required for the Lab Scenario using the [Cloud Formation Template](https://github.com/Azure/Microsoft-Defender-for-Cloud/blob/main/Labs/Files/AWS-Cloudformation-Template.json). Repeat Steps 10 to 13. Once the stack is deployed, wait for 2-4 hours and come back to the setup

## **Exercise 2: Explore Attack Paths in your AWS Environment**

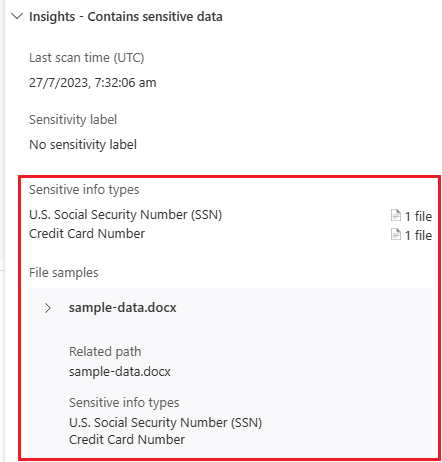
1. Open **Azure Portal** and navigate to **Microsoft Defender for Cloud** blade.
2. From Defender for Cloud's menu, open the **Attack Path Analysis** page
3. You will find the Attack Paths in your AWS Environment. Click on **“Internet exposed AWS S3 Bucket with sensitive data is publicly accessible”**



1. You can observe the risk involved is Sensitive Data Exposure and Potential Impact. Click on the S3 bucket to drill down the sensitive data stored in the S3 bucket



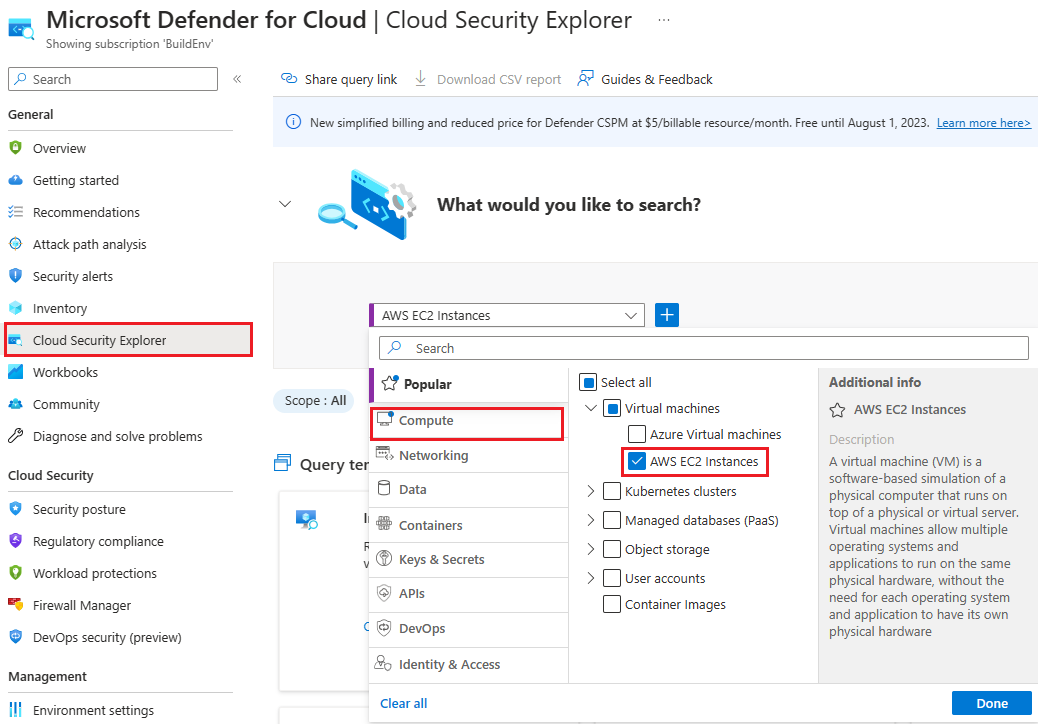
1. The Insights tab provides the detailed insights of the Attack path. You can observe the Insights Exposed to the Internet, Allows Public access, Contains Sensitive Data. You can drill down further on Contains Sensitive Data, to check what files contains sensitive data and Sensitive Info Types.

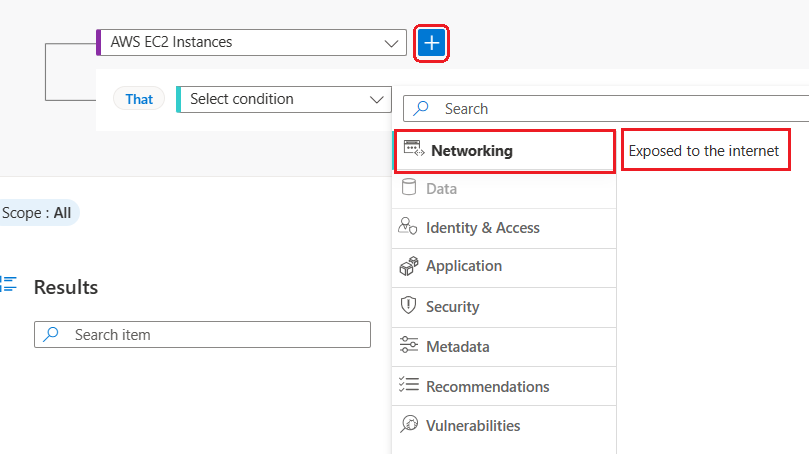


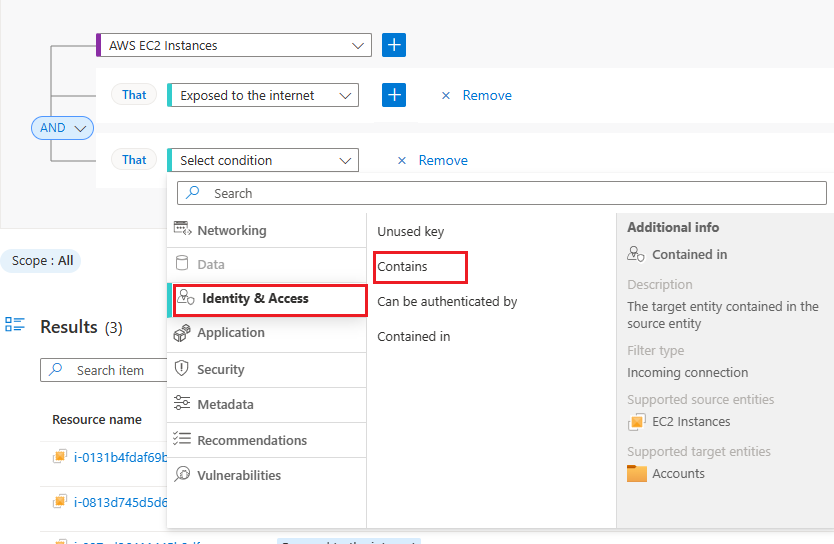
1. Remediate the recommendations to resolve the attack path
2. Explore the rest of the Attack paths found in your Environment and remidiate

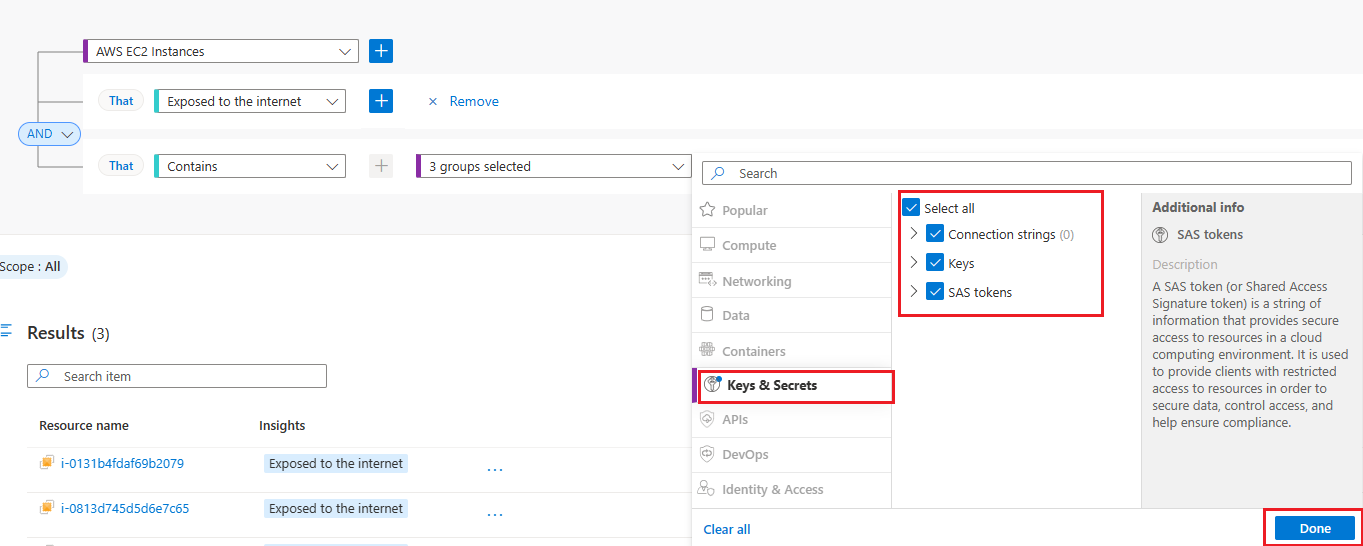
## **Exercise 3: Build query with Cloud Security Explorer**

1. Open **Azure Portal** and navigate to **Microsoft Defender for Cloud** blade.
2. From Defender for Cloud's menu, open the **Cloud Security Explorer** page, build the query as shown below and click done and search.









1. You can drill down further to observe the Insights and secrets file stored on the EC2 Instance

