Step-by-Step Guide: Building a Security Operations Center (SOC) Using Azure and Microsoft Sentinel

Suraj M
Passionate about Data Science and Analytics
Freelance Software Developer
Full Stack Engineer
linkedin.com/in/suraj-m-jnnce

October 1, 2024

1 Introduction

In this project, we will be setting up a Security Operations Center (SOC) using Microsoft Azure and Microsoft Sentinel. You will learn how to create a virtual machine (VM), deploy a Security Information and Event Management (SIEM) tool, monitor security events, and generate real-time alerts for suspicious activities. This project will significantly enhance your resume and improve your cybersecurity skills.

2 Step 1: Create an Azure Account

Follow the steps below to create an Azure account and get started:

1. Go to the Azure portal: azure.microsoft.com/en-us/free.
2. Click on "Start free" and create a new account.
3. Complete the sign-up process by entering your personal details.
4. You will receive $200 in free credits to use within Azure.

3 Step 2: Set Up a Virtual Machine (VM)

Once you have your Azure account, follow these steps to create a virtual machine (VM):

1. In the Azure portal, click on **Create a resource**.

2. Search for **Virtual Machine** and click **Create**.
3. Configure the VM settings:
    - **Resource Group**: Create a new resource group (e.g., `MadHatGroup`).
    - **VM Name**: You can name the VM something like `MadHatVM`.
    - **Region**: Choose the region closest to your location.
    - **Image**: Select `Windows Server 2019 Datacenter`.
    - **Size**: Choose the recommended size (e.g., `Standard B2s`).
    - **Administrator Account**: Set a username and password.
    - **Public Inbound Ports**: Allow RDP (Remote Desktop Protocol) on port 3389.
4. Click **Review + create** and then **Create**.
5. Wait for the VM to be deployed (this may take a few minutes).

4 Step 3: Deploy Microsoft Sentinel

Microsoft Sentinel is the SIEM tool that will monitor your VM for security events. Follow these steps to set up Sentinel:

1. In the Azure portal, search for **Microsoft Sentinel**.
2. Click on **Create** to deploy Sentinel.
3. First, create a **Log Analytics Workspace**:
    - Assign the workspace to the same resource group (e.g., `MadHatGroup`).
    - Choose the same region as your VM to minimize latency.
4. After the workspace is created, click **Add** to deploy Microsoft Sentinel.

5 Step 4: Configure Data Collection for Security Events

Now, you need to configure data collection so that Sentinel can gather security events from your VM:

1. Go to the **Log Analytics Workspace** that you created in the previous step.
2. Under the **Agents Management** tab, click **Add** and install the **Azure Monitor Agent**.
3. Once the agent is installed, create a **Data Collection Rule**:

- Name the rule something like `Windows Events to Sentinel`.
- Select the virtual machine (`MadHatVM`) as the data source.
- Select **All Security Events** to ensure comprehensive logging.

4. Click **Create** to finalize the data collection rule.

6 Step 5: Set Up Alert Rules for RDP Login Attempts

Next, you'll set up alert rules to notify you of any successful Remote Desktop Protocol (RDP) login attempts. Follow these steps:

1. In Microsoft Sentinel, go to the **Analytics** section and click **Create New Rule**.
2. Configure the rule to monitor for successful RDP logins:
   - Set the query to: `SigninLogs | where ResultType == 0 and Protocol == "RDP"`.
   - Set the severity to **High**.
   - Set the rule to run every 5 minutes for near real-time detection.
3. Save the rule and enable it.

7 Step 6: Test Your Setup by Simulating an RDP Attack

To ensure that everything is working correctly, simulate an RDP login attempt:

1. Open Remote Desktop on your local machine.
2. Enter the public IP address of your VM and use the credentials you created.
3. Log in to the VM and monitor Sentinel for any alerts.
4. You should see an alert generated in the Sentinel dashboard under **Incidents**.

8 Step 7: Expand Your SOC with Threat Intelligence

For more advanced monitoring, you can integrate external Threat Intelligence feeds into your Sentinel instance:

1. Go to **Threat Intelligence** in Microsoft Sentinel.
2. Click **Add** and configure a Threat Intelligence feed.
3. You can use sources such as AlienVault OTX or VirusTotal to gather Indicators of Compromise (IOCs).

9 Conclusion

Congratulations! You have successfully built your own Security Operations Center (SOC) using Microsoft Azure and Sentinel. This project gives you hands-on experience with SIEM tools, virtual machines, and cybersecurity monitoring—key skills that are highly sought after by employers.

You can now add this project to your resume and continue to build upon it with more advanced features like automation and API-based threat intelligence.