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

**Author: Ragul B  
Contact Email: bragul7064gmail.onmicrosoft.com  
Published on: October 1, 2024  
Focus: Deploying Microsoft Sentinel and setting up a Security Operations Center (SOC) in Microsoft Azure.**

**Table of Contents**

1. [**Introduction**](#introduction)
2. [**Step 1: Create an Azure Account**](#step-1-create-an-azure-account)
3. [**Step 2: Set Up a Virtual Machine (VM)**](#step-2-set-up-a-virtual-machine-vm)
4. [**Step 3: Deploy Microsoft Sentinel**](#step-3-deploy-microsoft-sentinel)
5. [**Step 4: Configure Data Collection for Security Events**](#step-4-configure-data-collection-for-se)
6. [**Step 5: Set Up Alert Rules for RDP Login Attempts**](#step-5-set-up-alert-rules-for-rdp-login)
7. [**Step 6: Test Your Setup by Simulating an RDP Attack**](#step-6-test-your-setup-by-simulating-an)
8. [**Step 7: Expand Your SOC with Threat Intelligence**](#step-7-expand-your-soc-with-threat-inte)
9. [**Conclusion**](#conclusion)

**Introduction**

**In this project, we will be creating a Security Operations Center (SOC) using Microsoft Azure and Microsoft Sentinel. This involves setting up a virtual machine (VM), deploying a Security Information and Event Management (SIEM) tool, monitoring security events, and generating real-time alerts for suspicious activities. Completing this project will enhance your cybersecurity skills and make your resume more attractive to employers.**

**Objectives**

* **Understand how to create and configure resources in Azure.**
* **Learn to deploy and configure Microsoft Sentinel.**
* **Monitor security events and respond to incidents effectively.**
* **Gain hands-on experience with threat intelligence integration.**

**Step 1: Create an Azure Account**

**To begin with, you'll need a Microsoft Azure account. Follow these steps to create your account:**

1. **Go to the** [**Azure Portal**](https://azure.microsoft.com/en-us/free)**.**
2. **Click on "Start free" and follow the steps to create your account.**
3. **Provide your personal information and complete the sign-up process.**
4. **After signing up, you'll receive $200 in free credits to use on Azure services.**

**Importance of Azure Account**

**Creating an Azure account is the first step towards accessing a wide range of cloud services that are essential for building a Security Operations Center. The free credits allow you to explore these services without incurring costs.**

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

**Once you’ve set up your Azure account, the next step is to create a Virtual Machine (VM). Here’s how:**

1. **Open the Azure portal.**
2. **Click on Create a resource.**
3. **In the search bar, type Virtual Machine and click Create.**
4. **Configure the following settings:**
   * **Resource Group: Create a new resource group (e.g., *MadHatGroup*).**
   * **VM Name: Choose a name for the VM, like *MadHatVM*.**
   * **Region: Select the region closest to your location.**
   * **Image: Choose Windows Server 2019 Datacenter.**
   * **Size: Select the recommended size (e.g., *Standard B2s*).**
   * **Administrator Account: Set a username and password.**
   * **Public Inbound Ports: Enable RDP (Remote Desktop Protocol) on port 3389.**
5. **Click Review + Create, then click Create to start the deployment.**

**Why a Virtual Machine?**

**A VM serves as the foundational infrastructure for hosting applications and tools, including Microsoft Sentinel. It allows you to simulate a production environment for monitoring and security management.**

**Step 3: Deploy Microsoft Sentinel**

**Now, it's time to deploy Microsoft Sentinel, a SIEM tool for monitoring your VM:**

1. **Open the Azure portal.**
2. **Search for Microsoft Sentinel and click Create.**
3. **Before deploying Sentinel, you need to create a Log Analytics Workspace:**
   * **Assign it to the same Resource Group (e.g., *MadHatGroup*).**
   * **Choose the same Region as your virtual machine to minimize latency.**
4. **After creating the workspace, click Add to deploy Microsoft Sentinel.**

**Benefits of Microsoft Sentinel**

**Microsoft Sentinel provides real-time analytics, automated responses, and a unified view of security across your resources, allowing you to identify and respond to threats effectively.**

**Step 4: Configure Data Collection for Security Events**

**Once Sentinel is deployed, you need to configure it to collect security events from your virtual machine:**

1. **Go to the Log Analytics Workspace that you created earlier.**
2. **Under the Agents Management tab, click Add and install the Azure Monitor Agent on your virtual machine.**
3. **After installing the agent, create a Data Collection Rule:**
   * **Name the rule something like *Windows Events to Sentinel*.**
   * **Select your virtual machine (*MadHatVM*) as the data source.**
   * **Choose All Security Events for comprehensive logging.**
4. **Click Create to finalize the data collection rule.**

**Data Collection Importance**

**Configuring data collection is crucial for monitoring and analyzing security events effectively. By collecting all security events, you ensure that no critical information is missed during monitoring.**

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

**To get real-time notifications for successful RDP login attempts:**

1. **In Microsoft Sentinel, go to the Analytics section.**
2. **Click Create New Rule and configure it as follows:**
   * **Query: SigninLogs | where ResultType == 0 and Protocol == "RDP"**
   * **Severity: Set to High.**
   * **Set the rule to run every 5 minutes for near real-time detection.**
3. **Save and enable the rule.**

**Importance of Alert Rules**

**Setting up alert rules ensures that you are immediately notified of any suspicious activities, allowing for timely investigation and response.**

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

**To ensure that your setup works, simulate an RDP login attempt:**

1. **Open Remote Desktop on your local machine.**
2. **Enter the Public IP address of your virtual machine and log in using the credentials you created earlier.**
3. **Check Microsoft Sentinel to see if an alert is generated in the Incidents dashboard.**

**Testing Significance**

**Testing your setup is critical to confirm that your monitoring and alerting systems are functioning correctly. It ensures that any potential security breaches can be detected in real-time.**

**Step 7: Expand Your SOC with Threat Intelligence**

**For more advanced monitoring, integrate external threat intelligence feeds into Sentinel:**

1. **In Microsoft Sentinel, go to Threat Intelligence.**
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).**

**Threat Intelligence Benefits**

**Integrating threat intelligence enhances your SOC by providing context for alerts, helping you identify threats more accurately and efficiently.**

**Conclusion**

**Congratulations! You’ve successfully built a Security Operations Center (SOC) using Microsoft Azure and Microsoft Sentinel. This project provides valuable hands-on experience with SIEM tools, virtual machines, and security monitoring—highly sought-after skills in cybersecurity.**

**Next Steps**

**You can expand this project by exploring automation and API-based threat intelligence, as well as adding other security measures for a more advanced SOC. Continuous learning and adaptation are essential in the ever-evolving field of cybersecurity.**

**Additional URLs**

* **Virtual Machine (Kali) Overview**: [Virtual Machine URL](https://portal.azure.com/#@bragul7064gmail.onmicrosoft.com/resource/subscriptions/b012e352-59b4-4acf-9d71-af76e0fa2683/resourceGroups/ragul/providers/Microsoft.Compute/virtualMachines/kali/overview)
* **Log Analytics Workspace (ragulkali) Overview**: [Log Analytics Workspace URL](https://portal.azure.com/#@bragul7064gmail.onmicrosoft.com/resource/subscriptions/b012e352-59b4-4acf-9d71-af76e0fa2683/resourceGroups/ragul/providers/Microsoft.OperationalInsights/workspaces/ragulkali/Overview)
* **Azure Monitoring Overview**: [Azure Monitoring URL](https://portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/overview)