**SIEM Setup and Live Attack Visualization with Azure Sentinel**

This project demonstrates the setup of a powerful Security Information and Event Management (SIEM) solution using Azure Sentinel, as well as the development of a live attack visualization using a heatmap. The following steps outline the technical process involved:

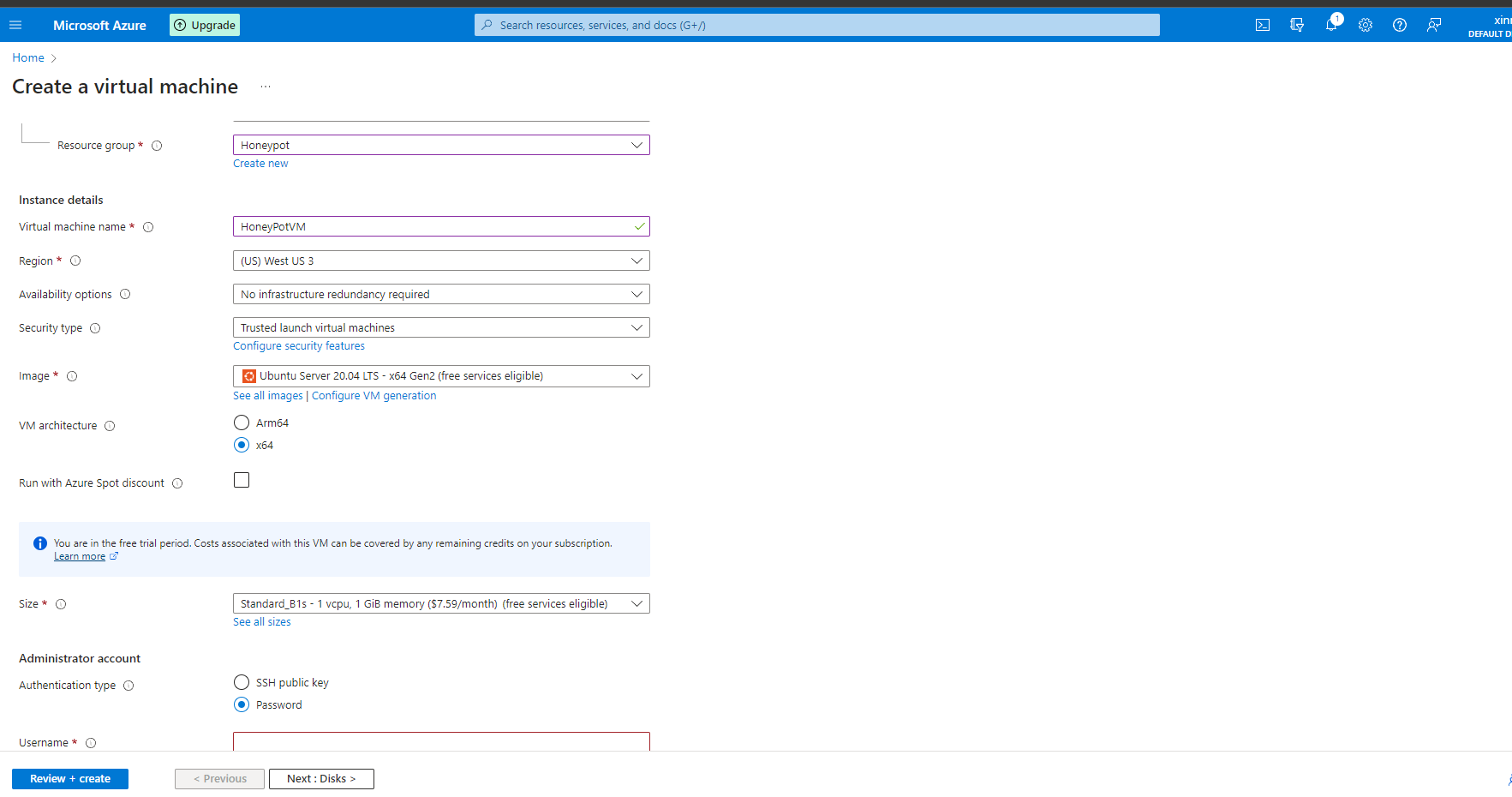
**Prerequisites**

Before starting the project, ensure that you have the following:

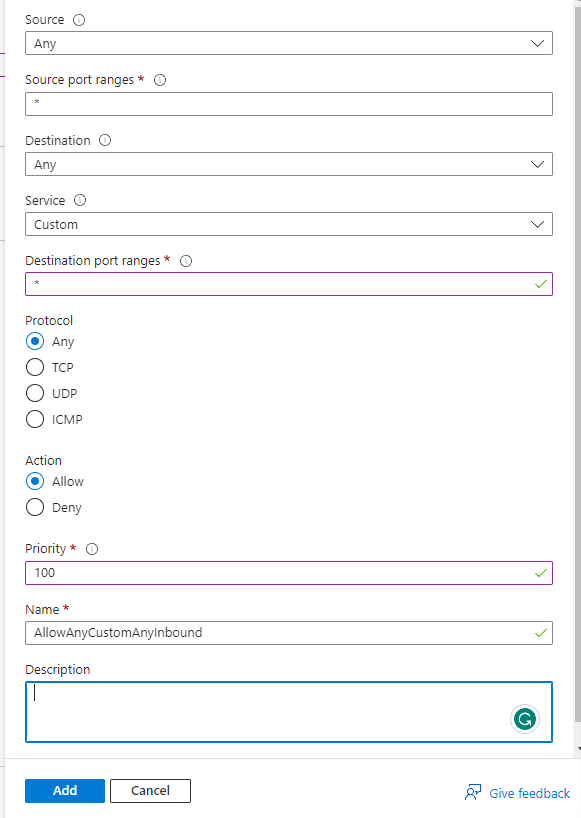
* An active Azure subscription. Free 12 months and 200-dollar credits can be found here (https://azure.microsoft.com/en-us/free/)

**Steps**

1. **Create Azure Subscription**
2. **2. Create Virtual Machine**
   * In the Azure portal, search for "Virtual Machine" in the search bar and click on "Create" to start the VM creation process.
   * Configure the VM settings based on your requirements and preferences.
   * Set up a private username and password for secure access to the VM.
   * Refer to the provided picture for a visual representation of the settings used in this project.
   * Adjust the disk settings according to your requirements or leave them as they are if they align with your needs and preferences.

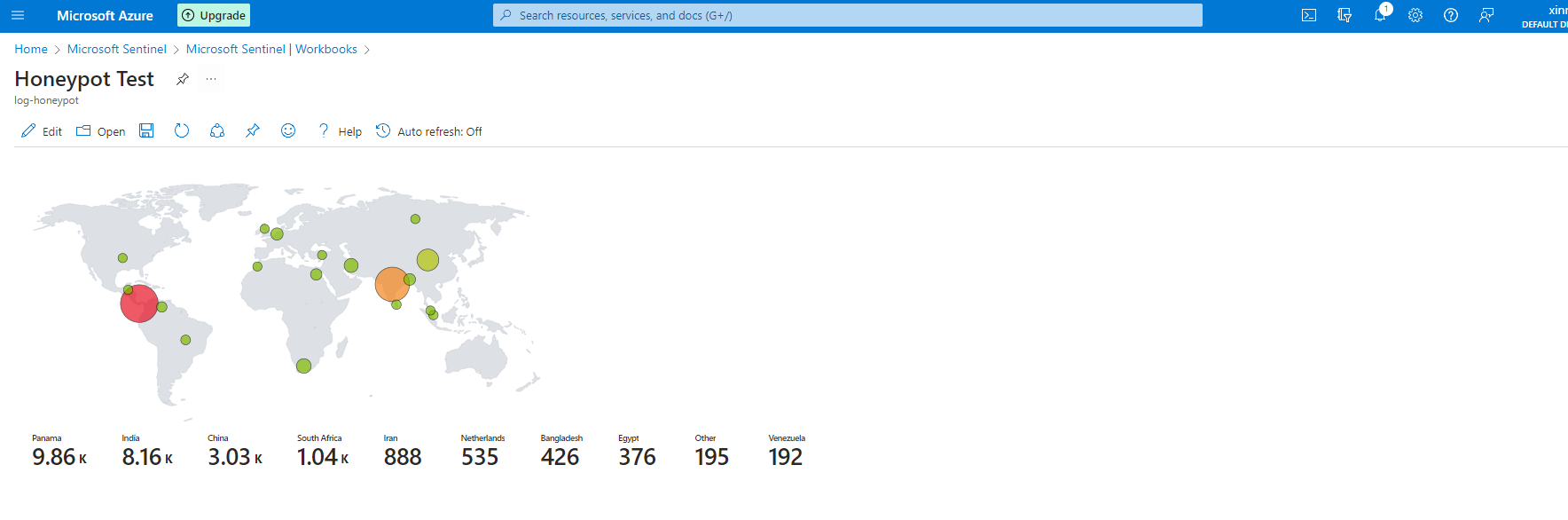


1. **Allow All in Firewall**
   * In the Azure portal, navigate to the "Networking" tab of your Virtual Machine settings.
   * Click on "NIC Network security group" and select "Advanced".
   * Delete the current firewall rule and add a new inbound rule to allow desired incoming traffic.
   * Refer to the provided picture for the specific settings used in this project.
   * Customize the remaining settings based on your specific needs and preferences.
   * Click on "Review + Create" to proceed with the creation of the virtual machine, verifying that all the settings are accurately configured.



1. **Create Log Analytics Workspace**
   * Search Log Analytics Workspace within Azure click create type in a name click review and create.
2. **Enable Gathering VM Logs in Microsoft Defender for the Cloud**
   * In the video, the security center is referred to as Microsoft Defender for the Cloud, which is the updated name.
   * Instead of "Pricing and settings," it is now called "Environment Settings."
   * Select the newly created workspace, and under "Environment Settings," click on "Enable all plans" and disable SQL servers as instructed.
   * On the left-hand side, locate and click on "Data collection."
   * Select all events for data collection and click "Save" to apply the changes.
3. **Setup Azure Sentinel**
   * Search for "Azure Sentinel" in the Azure portal and click on "Create."
   * Select the previously created Log Analytics workspace for Azure Sentinel integration.
4. **Log into VM with Remote Desktop**
   * Access the VM through Remote Desktop on Windows.
   * Use the IP address associated with your VM to establish the connection.
   * Enter the username and password that you previously created for the VM to log in.
5. **Observe Event Viewer Logs in VM**
   * Explore the Event Viewer logs within the VM to identify security-related events.
   * The necessary information will be automatically collected through the script that will be executed later.
6. **Turn Off Windows Firewall on VM**
   * Disable the Windows Firewall temporarily to allow the download and execution of PowerShell scripts.
   * Search for "wf.msc" in the Windows search bar and open "Windows Defender Firewall with Advanced Security."
   * Navigate to the first three tabs and disable the firewall settings by selecting the "Off" option.
7. **Download PowerShell Script**
   * Obtain the necessary PowerShell script for extracting geolocation data from the attackers.
   * You can refer to the PowerShell script provided by Josh ([Link Here](https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1)) but please note that there might be potential errors if the attacks occur too rapidly.
   * To address this issue, I have rewritten the script, incorporating a small delay to ensure smooth execution. You can access my modified script as an alternative ([Link Here](https://github.com/Abdi-Ahmed1/SIEM-Project/blob/main/PowerShell%20Script%20Extracting%20Data)) Both scripts will work effectively for extracting geolocation data.
8. **Get Geolocation.io API Key**
   * Create an account on Geolocation.io to obtain the API key required for collecting geolocation data.
   * Acquire an API key from Geolocation.io to enable geolocation data retrieval.
9. **Run Script to Get Geo Data from Attackers**
   * Execute the PowerShell ISE script to retrieve geolocation data for the attackers.
   * Copy the script from either of the provided links and paste it into the PowerShell Integrated Scripting Environment (ISE).
   * Locate the line in the script that specifies the API key and replace it with your own Geolocation.io API key.
   * Save the modified script and execute it to initiate the extraction of geolocation data.
10. **Create Custom Log in Log Analytics Workspace**
    * In Log Analytics, navigate to the "Tables" tab (formerly known as "Custom Logs").
    * Inside your VM, locate the log file that was generated when you executed the script. Look for a file named "logfile" or "failed\_RDP."
    * Open the log file, copy its contents, and create a new Notepad document on your personal PC.
    * Paste the copied information into the new Notepad document and save it with the same name as the log file.
    * Use this saved file to create a new Table in the Log Analytics workspace.
11. **Create Custom Fields/Extract Fields from Raw Custom Log Data**
    * Please note that the method shown in the video for extracting raw data using an old Azure feature is no longer available.
    * To extract the raw data required for the heatmap, I have prepared a custom query ([Link Here](https://github.com/Abdi-Ahmed1/SIEM-Project/blob/main/Extraction%20Query)) that you can copy and paste into the Logs table.
    * Execute this query in the Logs tab of Log Analytics to retrieve the necessary raw data for generating the heatmap.
12. **Setup Map the Heatmap in Azure** 
    * Search for "Azure Sentinel" in the Azure portal and create a workspace, selecting the appropriate resource group you previously created.
    * After creating the workspace, navigate to the "Workbooks" tab on the left-hand side and create a new workbook.
    * Click on "Edit" and remove the existing tables in the workbook.
    * Then, click on "Add new" and insert the query I provided to sort the raw data for your heatmap. ([Link Here](https://github.com/Abdi-Ahmed1/SIEM-Project/blob/main/Azure%20Sentinel%20workbook%20query))
    * This query will help organize the data in a suitable format for generating the heatmap visualization.
13. **Monitor and Analyze Live Attacks**
    * Let the script and VM run for a few hours to collect live attack data.
    * Refresh the workbook to observe and analyze the map visualization, tracking the origins and patterns of the attacks.
    * Analyze the live attacks on the map to gain insights into their sources and patterns.
14. **Final Thoughts and Takeaways**
    * Completing this project has provided valuable opportunities for me to enhance my proficiency in Azure settings, tabs, and stay updated on the latest platform updates. Through this hands-on experience, I have gained the following key takeaways that will be of interest to potential employers:
    * In-depth Azure Knowledge: This project allowed me to deepen my understanding of Azure services, particularly in the context of cybersecurity and SIEM implementation using Azure Sentinel.
    * Adaptability and Learning Agility: By navigating the changes in Azure's interface and incorporating updated steps, I demonstrated my ability to quickly adapt to evolving technologies and stay current with the latest industry trends.
    * Problem-solving Skills: Overcoming challenges, such as modifying the PowerShell script to address potential errors and finding alternative methods to extract and analyze raw data, showcased my strong problem-solving skills and resourcefulness.
    * Attention to Detail: Through careful configuration and analysis, I ensured accurate data collection and visualization, highlighting my meticulous approach to tasks and a keen eye for detail.
    * Collaboration and Self-Motivation: Completing this project required self-directed learning, resourcefulness, and effective collaboration with various resources and documentation to achieve the desired outcomes.
    * I am confident that the knowledge and skills gained from this project position me as a capable and adaptable professional, ready to contribute effectively to cybersecurity initiatives.

**FINAL HEAT MAP**

****