**Create Virtual Machine**

1. Launch Resource Creation:

* Begin by selecting **Create a resource**.

2. Initiate Virtual Machine Setup:

* Navigate to **Virtual machine** and click **Create**.

3. Define Essential Information:

* Provide a suitable name for both the Resource group and the Virtual machine itself.
* Choose the **Region** that aligns with your location.
* For **Availability zone**, select **No infrastructure redundancy required**.
* Opt for **Standard** security type.
* Select the **image**; for this tutorial, we'll use Windows 10 Pro.

4. Establish User Credentials:

* Create a robust username and password combination.

5. Configure Inbound Ports:

* For **public inbound ports,** select **allow selected ports**.
* Under **Select inbound ports**, specifically choose **RDP (3389)**.
* Select **Next:disk** to Proceed to the Next step for Disk configuration (optionally review settings).
* Subsequently, advance to the Networking step by selecting **Next:networking**.

6. Manage Network Security Group:

* Within the NIC network security group section, select **Advanced**.
* Under **configure network security group**, opt to **Create new**.

7. Customize Inbound Rules:

* Under **inbound rules** remove any existing rules present.
* Initiate the creation of a new inbound rule by clicking **+Add**.
* Within the new rule configuration, specify the following:
  + Source: Any
  + Source port ranges: \* (all)
  + Destination: Any
  + Service: Custom
  + Destination port ranges: \* (all)
  + Protocol: Any
  + Action: Allow
  + Priority: 100 (adjust as needed, avoiding overly high or low values)
  + Name: Assign a descriptive name for the rule
* Finalize the rule creation by clicking **Add**.

A screenshot of a computer

Description automatically generated

8. Complete Virtual Machine Deployment:

* select **review+create**, then select **create**.

**Create Log Analytics Workspace**

1. Initiate Log Analytics Workspace Creation:

* Begin by searching for **Log Analytics** workspace and clicking **Create**.

2. Select Resource Group:

* Choose the existing resource group you previously created for this lab.

3. Provide Instance Details:

* Assign a descriptive name to your Log Analytics workspace.
* Select the region that aligns with the region of your virtual machine.
* Click **Review + create** and then **Create** to initiate the workspace deployment.

4. Enable Microsoft Defender for Cloud:

* Search for **Microsoft Defender for cloud** and navigate to the **Getting started** section.
* Select the Log Analytics workspace you just created (you might need to scroll down to locate it).
* Under **Select defender plan**, activate the **Servers** plan.

**Create Microsoft Sentinel**

1. Initiate Microsoft Sentinel Setup:

* Search for **Microsoft Sentinel** and initiate its creation by clicking **Create**.

2. Choose Resource Group and Provide Details:

* Select the **resource group** you're currently using for the lab.
* Within **Instance details**, assign a descriptive name to your workspace and choose the appropriate region.
* Click **Review + create**, followed by **Create** to establish the workspace.

3. Configure Data Connectors:

* In **Microsoft Sentinel**, navigate to **Configuration** and select **Data connectors**.
* Search for **Windows security event** and click **Manage**.
* Select either **Security events via legacy agent** or **Windows security events via MMA** as your preferred method (this tutorial utilizes the legacy agent).
* Proceed by clicking **Open connector page**.

4. Stream All Security Events:

* Under **Instructions**, locate the option to Select which events to stream.
* Enable **All events** to ensure comprehensive coverage.
* Apply the configuration changes by clicking **Apply changes**.

Logging RDP-Attack Events

1. Retrieve Virtual Machine's Public IP Address:

* Navigate to **Virtual machines** and select the VM designated for this lab.
* Under the Overview tab, locate and copy the public IP address for subsequent use.

2. Establish Remote Desktop Connection:

* On your physical PC, launch **Remote Desktop Connection**.
* Enter the copied VM's public IP address in the **Computer** field and your VM's username in the **Username** field.
* Click **Connect** and provide your VM's credentials when prompted by the Windows Security window.

3. Implement Failed Login Tracking:

* Within your VM, open **PowerShell ISE**.
* Paste the code from <https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1> (or write your own in C#) to log failed login attempts into a log file.
* Prior to running the code:
  + Obtain an API key from [ipgeolocation.io](https://ipgeolocation.io/).
  + Replace the existing API key placeholder within the code with your obtained key.
* Execute the code to initiate logging.

A computer screen shot of a computer screen

Description automatically generated

* Wait for events to occur.

4. Gather Log Data:

* Access the log file and copy its contents.
* Return to your physical PC and paste the copied data into a text editor.
* Save the text file for subsequent use.

5. Create Custom Log Table in Log Analytics Workspace:

* Access Microsoft Azure and navigate to **Log Analytics workspaces**.
* Select your workspace and proceed to **Table** tab.
* Initiate table creation by choosing **Create with MMA-based**.

6. Utilize Sample Log and Specify Delimiter:

* Use the saved log file from your PC as the **Sample log**.
* Click **Next**.
* For **Record delimiter,** select **new line**.
* Click **Next**.

7. Define Collection Paths:

* Under **Collection paths**:
  + Type **Windows** as the type.
  + Refer back to your VM to obtain the exact log file path.
  + Paste the path into the corresponding field.
* Click **Next**.

8. Name the Custom Log Table:

* Assign a descriptive name to your custom log table.
* Click **Next**, followed by **Create**.
* The newly created table will be searchable within your workspace.

9. Query the Log Table:

* Navigate to **Logs** tab.
* Construct a query using the log table name and **securityEvents**.
* Execute the query to verify data visibility (allow some time for results to populate if necessary).

**Create Mapping Visualization**

8. Create a Workbook in Microsoft Sentinel:

* Search for **Microsoft Sentinel** and select your workspace.
* Navigate to **Workbook** section and click **Add** workbook.

10. Add a Query:

* Click **Add** and then **Add query**.

11. Extract and Visualize Data:

* Paste the provided code into the query editor to extract relevant information from the raw log table into a refined format.

FAILED\_RDP\_CL

|extend username = extract(@"username:([^,]+)",1,RawData),

timestamp = extract(@"timestamp:([^,]+)",1,RawData),

latitude = extract(@"latitude:([^,]+)",1,RawData),

longitude = extract(@"longitude:([^,]+)",1,RawData),

sourcehost = extract(@"sourcehost:([^,]+)",1,RawData),

state = extract(@"state:([^,]+)",1,RawData),

label = extract(@"label:([^,]+)",1,RawData),

destination = extract(@"destinationhost:([^,]+)",1,RawData),

country = extract(@"country:([^,]+)",1,RawData)

|where destination != "samplehost"

|where sourcehost != ""

|summarize eventCount = count() by timestamp,label,country,state,sourcehost,username,destination,longitude,latitude

* Under **Visualization**, select **Map** to geographically represent the data.
* Click **Run query** to execute the query and generate the map visualization.

12. Observe Attack Coordination Map:

* A screenshot of a computer

  Description automatically generatedThe resulting map will visually depict attack coordination patterns, aiding in threat identification and analysis.