In progress

In this document I will be going over the process of setting up an SIEM with Microsoft Azure and Sentinel, exposing a VM to the open internet
and logging the attacks with Log Analytics Workspace.

You'll need an Azure account, if you are new they will give you $200 credit. Sign up or sign in at Azure.portal.com.
At the top search bar, type in Virtual Machines.
Top left corner, click the green plus sign to create a new VM.
In the main page, create a new resource group.
Use whatever you like, for this I'm going with Honeypot_Group.
Name your VM, I went with Honeypot.
Select whichever region you are in.
In the Image section, select Windows 10.
You'll need a key but you can find those if you know where to look, say a Graveyard but I don't condone criminal activity.
Leave everything up to Administrator Account as default.
Set your username.
Set your password.
Hit next until you get to Network.
Under NIC Network security group, click Advanced.
Remove the default rule that has port 22 open.
We are going to open the device up to network traffic to get some data for a SIEM.
Select Add an inbound rule.
Erase the Destination port range and put an * for all port ranges.
Leave Protocol as Any.
Leave Action as Allow.
Set priority to 100.
I left the name as AllowAnyCustomAnyInbound
Hit Add.
Click Review + Create.
Click Create.

At the top search bar time in Logs Analytics Workspaces.
Select Create.
For Resource Group, add to our created Honeypot_Group or whatever you selected.
Name the Instance, I went with LawHoneyPot1
Select your region.
Select Review + Create.
Hit Create.

Back at the main page, use the top search to find Microsoft Defended for Cloud.

Hit Skip if you are prompted for upgrade.
Click on the Key icon with your Azure Subscription.
Click on the Azure Subscription 1 entry.
Turn on Defender.
Save.
Click Setting & Monitoring.
Head back to Logs Analytics Workspaces.
Scroll down the panel on the left to Virtual Machines (deprecated)
Find your VM.
Click on the VM.
Connect.
While that is connecting, open a new tab to Poratl.Azure.

Search for Sentinel.
Click Create Microsoft Sentinel.
Select the created Workspace.

While that is connecting we can head back to the main page.
Find your VM.
Copy the public IP address.
On your own machine, open the start menu and search for Remote Desktop.
Log in with the user credentials you created.
Accept the security prompt.
In the VM, launch Edge.
Open Event Viewer.
Open the security tab and look for Event ID 4625.
Open another RDP session and connect to the VM again.
When prompted to sign in, try putting in random information to sign in.
You'll see these failed log in attempt in Event Viewer.
On the VM, search for wf.msc.
This is your VM's Firewall.
Open Windows Firewall properties.
On each tab, turn off each firewall from the Firewall State dropdown menu.
On your computer, run ping -t with your VM's IP address.
Confirm that this is able to be pinged.

Navigate to the link below.
https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1
The first line of this script has a link to https://ipgeolocation.io/.
Sign up and get your API key.
Copy this Powershell script.
Paste into a Notepad for ease of editing.
Paste the API key into the second line.
Launch Powershell ISE on the VM.

Past the Powershell.
This will keep running and log every failed login attempt.

Head back to the Azure portal to add a custom log.
Type in Log Analytics.
Go to the work space.
Search for Legacy custom logs.
Add a log.
Copy the contents of C:\Programdata\failed_rdp to a new Notepad on your computer.
Save.
Add this as a sample log.
Hit next.
Hit next again.
From the drop down menu, select windows.
Enter path as C:\ProgramData\failed_rdp.log
Hit next.
Name the custom log whatever you like.
I went with FAILED_RDP_WITH_GEO
Hit next.
Hit create.