Microsoft Azure SIEM (Sentinel) and Honeypot

### Setting up the Environment

1. Setup Virtual Machine:
   1. This virtual machine will be used to create a honeypot.
   2. We are utilizing the free version included with Azure for Windows 10 2h22 gen2
   3. We created a new virtual machine with a new resource group we called “HoneypotLabs”.
   4. We create a new network security group by deleting the default and set the inbound traffic to allow from any source and destination all the port ranges and protocol. We called the rule “Any\_In”.
   5. We finally click review + create to finish up the creation of the virtual machine.
2. Setup Log Analytics Workspace:
   1. Create this to query to ingest logs from the Windows Virtual Machine using the Windows Event Logs.
   2. Create our own custom log that contains geographic analytics.
   3. SIEM (Azure Sentinel) will be used to connect to the workspace to display the log geodata.
   4. To start we will create a LAW (log analytic workspace) we connected to our resource group that we created during the Virtual Machine setup.
   5. We then name the instance of the LAW (e.g law-honeypot1) and select the region for the instance (East US 2). (Proceed to step 3a)
   6. We then go back to Log Analytics Workspace to connect it to the virtual machine that we created earlier.
3. Setup Microsoft Defender for Cloud:
   1. Used to enable the ability to gather logs from the VM into the LAW.
   2. We go into the settings for Defender Plans for the resource group and enable Microsoft Defender, We enable everything except SQL server on machines.
   3. Then we set the Data Collection setting to “All Events”. (Proceed to step 2f)
4. Setup Azure Sentinel:
   1. This is our SIEM that is gonna ingest our logs.
   2. We just have to connect it to our Log Analytic Workspace.

### Remote Desktop into Virtual Machine

1. We just have to log into the Virtual Machine using the credentials we made during the VM Setup portion of the lab.
2. We open the Event Viewer to view our logs. We want to focus on Event ID 4625 for the call such as Audit Failure.
3. Double clicking on the event properties shows us more details such as the account and the reason for the failure. It also displays the Network information such as the workstation name and the source IP Address from where the connection attempt was made.
4. We are going to utilize an IP geolocation API to take the IP and display the geographic details attached to the IP address and use it to display it on our geographical map through Sentinel.
5. We disable the firewall on the VM because it is a Honeypot and we do not care that this allows all traffic to inherently go through to the VM.
6. We ping the VM’s IP Address through our home computer using ICMP pings.
7. We then download Josh Makador Powershell script that Exports the logs for us.
8. Create an account from the API (ipgeolocation.io) and get your API key to add to the script.
9. The script looks at the event security logs and grabs all the events where there was an audit failure on login for RDP.
10. The failed\_rdp.log file that is created from the script starts with some sample data that is going to be used to train our law data and the failed authentications are appended to the end of the log file.

### Custom Log Ingesting on the LAW

1. Click on Tables, then click create, we then utilize the new custom log (mma-based).
2. The log is stored on our virtual machine so we start off by copying the contents of the log file and just creating a local copy on our host machine. We used this to train our law.
3. We then set the collection path to the Windows vm’s location where we stored the log file.
4. We can check this by querying the custom log that we made and piping it and parsing the raw data to separate the labels/categories.

### Sentinel Workbook

1. In Sentinel we want to create a new workbook. In this workbook we want to create our own widget setup.
2. We want to add the query that we have created earlier and we want to summarize the event counts by their labels/categories and we filter out our sample data and any data that has no source ip address.
3. This is displayed using the map filter with Latitude/Longitude and the event counts are labeled using the Labels we made earlier which should be “Country - IP address”
4. In Sentinel there are different tools that you can use to help you detect threats and incidents and set triggers from alerts.
5. So far the limit for this implementation is that I had run out of API calls due to only being on the free plan.