How to create SIEM with Azure sentinel

Portal.azure.com

1. Create Virtual Machine in Azure
   1. Delete current firewall and allow for all ports to be open
   2. Review and Create
2. Create L-A-W, log analytics workspace
3. Set Security by enabling Defender \*Changed from Video\*
   1. Microsoft Defender for Cloud ->> Environmental settings
   2. Enable Server Protection
   3. Disable SQL server plan
   4. Enable all Events to be recorded
4. Back to Log analytics workspace to Connect
   1. Virtual machine -> law-honeypot1
   2. Connect
5. Create a Microsoft Sentinel
   1. Create and select our honeypot server
6. Log into virtual machine
   1. RDP from computer to the IP 20.125.147.24 of our created machine
   2. Check security logs in Event Viewer to see attempted log ins
   3. Failed log ins will have IP address which we use for location purposes
7. Pinging 20.125.147.24 from our computer gets a request timeout \*NOT WORKING\*
   1. Disable firewall on virtual computer
   2. Wf.msc ->
   3. Windows firewall properties->
   4. Domain ->
   5. Firewall state -> off
   6. Private -> off
   7. Public -> off
   8. Now ping 20.125.147.24 and get a response
8. Figured out how to ping from local by adding Network inbound port rule
   1. Virtual machine-> network -> Add
   2. Port 0 open and allow for any protocol and any source
9. Use Powershell Script to scan Event Viewer for IP address and convert to Location with Geoloctaion API
   1. Copy and save powershell script <https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1>
   2. Go to <https://app.ipgeolocation.io/> to get API key
   3. Copy API key into powershell script
   4. Output is in C:\ProgramData as failed\_rdp.txt
10. Add custom logs to our Log Analytics Workspace
    1. Log analytics workspace
    2. Law-honeypot1 -> custom logs
    3. Copy text data from VM to a .log file on local computer
    4. Set collection path to C:\ProgramData\failed\_rdp.log
    5. Logs -> SecurityEvent shows the Event Viewer data in VM
    6. Logs-> FAILED\_RDP\_GEO is our geo data
11. Extract Fields from Raw Data
    1. Log Analitics Workspace -> Logs
    2. FAILED\_RDP\_GEO\_CL - > run
    3. Right-Click on one result to train data Extract Fields \*NEW\*
    4. latitude
    5. longitude
    6. destinationhost
    7. username
    8. sourcehost
    9. state
    10. country
    11. label
    12. timestamp
    13. Enable new fields by clicking Columns and checkboxing each field.\*NEW\*
12. Add new workbook in Microsoft Sentinel
    1. New workbook
    2. Delete widgets
    3. Add query
    4. Log analytics workspace Logs Query =>
    5. FAILED\_RDP\_WITH\_GEO\_CL | summarize event\_count=count() by sourcehost\_CF, latitude\_CF, longitude\_CF, country\_CF, label\_CF, destinationhost\_CF | where destinationhost\_CF != "samplehost" | where sourcehost\_CF != ""
    6. Visualization – World MAP
    7. Set Longitude and Latitude
    8. Save workbook and set auto-refresh to 5minutes