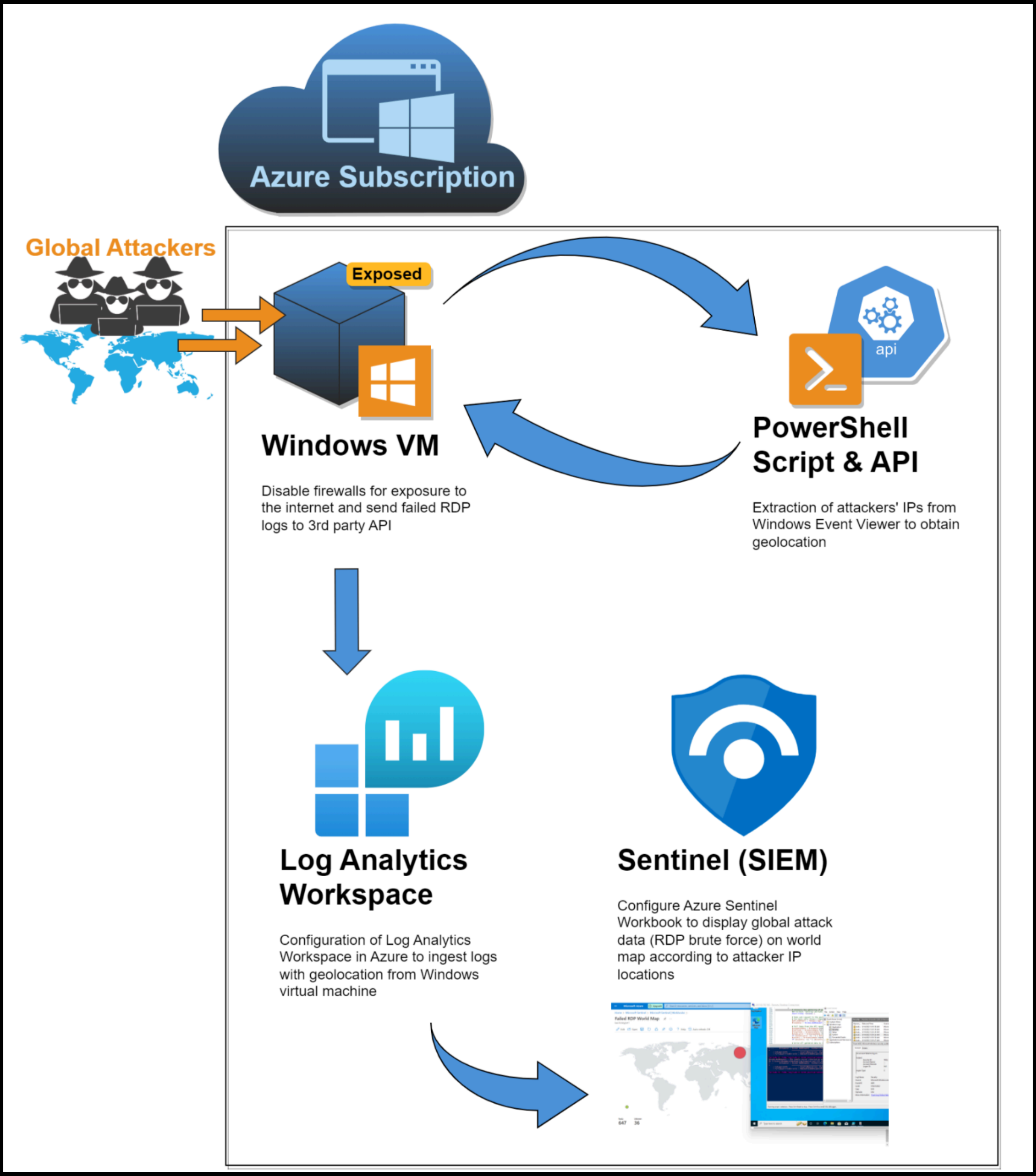
Azure SIEM Honeypot



Windows VM

Disable firewalls for exposure to the internet and send failed RDP logs to 3rd party API

PowerShell Script & API

Extraction of attackers' IPs from Windows Event Viewer to obtain geolocation

Log Analytics Workspace

Configuration of Log Analytics Workspace in Azure to ingest logs with geolocation from Windows virtual machine

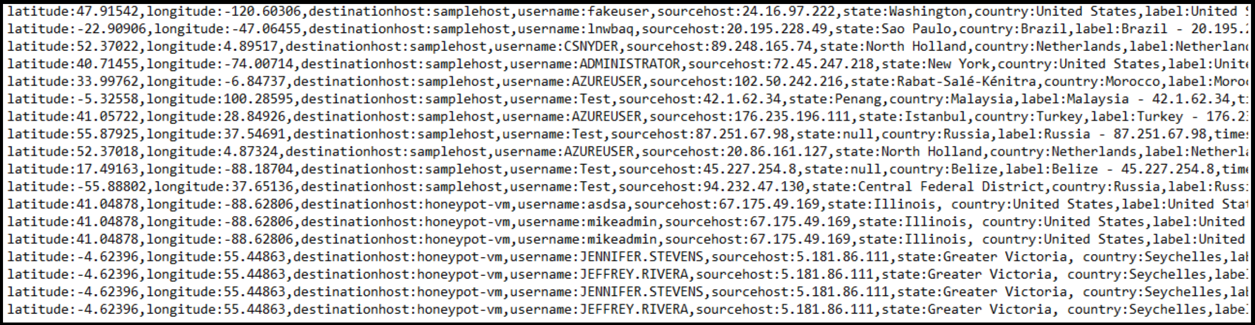
Sentinel (SIEM)

Configure Azure Sentinel Workbook to display global attack data (RDP brute force) on world map according to attacker IP locations

Basic Overview of How this works

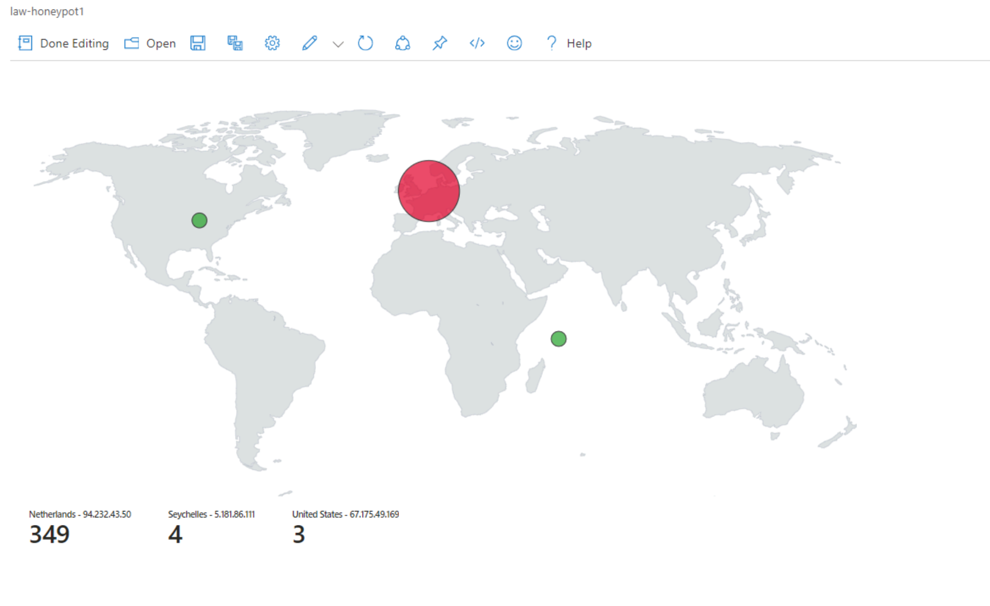
Procedure

1. **Create a Honeypot Virtual Machine:**
    a. Establish an Azure virtual machine named "honeypot-vm" using Windows 10 Pro (version 21H2).
    b. Implement security measures, including strong access controls, recommended region selection, and inbound port rules allowing RDP (3389).
    c. Configure networking settings with a focus on security, creating a Network Security Group to manage inbound rules.
2. **Create a Log Analytics Workspace:**
    a. Establish a Log Analytics workspace named "honeypot-log" in the same resource group as the virtual machine.
    b. This workspace will ingest Windows Event Viewer logs and custom logs with geographic data to map potential attacker locations.
3. **Configure Microsoft Defender for Cloud:**
    a. Enable specific Defender plans for Cloud Security Posture Management and Servers.
    b. Utilize data collection settings to capture "All Events" for comprehensive security monitoring.
4. **Connect Log Analytics Workspace to Virtual Machine:**
    a. Establish a connection between the Log Analytics workspace and the Honeypot Virtual Machine for centralized log management.
5. **Configure Microsoft Sentinel:**
    a. Create Microsoft Sentinel and associate it with the Log Analytics workspace to enable advanced threat detection and response capabilities.
6. **Disable the Firewall in Virtual Machine:**
    a. Temporarily disable the Windows Defender Firewall in the virtual machine to allow for easier discoverability.
7. **Scripting the Security Log Exporter:**
    a. Develop a PowerShell script to export data from the Windows Event Viewer, including IP geolocation information.
    b. The script continuously produces log data, extracting latitude and longitude, creating a new log file named "failed_rdp.log."
    c. Data should like like the data below



```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlan
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:Unit
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Moro
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Malaysia - 42.1.62.34,t
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey - 176.2
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russia - 87.251.67.98,time
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherl
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Belize - 45.227.254.8,tim
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,country:Russia,label:Russ
latitude:41.04878,longitude:-88.62806,destinationhost:honeypot-vm,username:asdsa,sourcehost:67.175.49.169,state:Illinois, country:United States,label:United Sta
latitude:41.04878,longitude:-88.62806,destinationhost:honeypot-vm,username:mikeadmin,sourcehost:67.175.49.169,state:Illinois, country:United States,label:United
latitude:41.04878,longitude:-88.62806,destinationhost:honeypot-vm,username:mikeadmin,sourcehost:67.175.49.169,state:Illinois, country:United States,label:United
latitude:-4.62396,longitude:55.44863,destinationhost:honeypot-vm,username:JENNIFER.STEVENS,sourcehost:5.181.86.111,state:Greater Victoria, country:Seychelles,la
latitude:-4.62396,longitude:55.44863,destinationhost:honeypot-vm,username:JEFFREY.RIVERA,sourcehost:5.181.86.111,state:Greater Victoria, country:Seychelles,labe
latitude:-4.62396,longitude:55.44863,destinationhost:honeypot-vm,username:JENNIFER.STEVENS,sourcehost:5.181.86.111,state:Greater Victoria, country:Seychelles,la
latitude:-4.62396,longitude:55.44863,destinationhost:honeypot-vm,username:JEFFREY.RIVERA,sourcehost:5.181.86.111,state:Greater Victoria, country:Seychelles,labe
```

8. **Create Custom Log in Log Analytics Workspace:**
   a. Import additional data from the IP Geolocation service into Azure Sentinel using a custom log named "FAILED_RDP_WITH_GEO."
9. **Query the Custom Log:**
   a. Run queries in Log Analytics Workspaces to verify and analyze the available data from the custom log.
10. **Extract Fields from Custom Log:**
    a. Extract relevant fields from the raw log data to create separate fields for different types of information.
11. **Map Data in Microsoft Sentinel:**
    a. Utilize Microsoft Sentinel to visualize and analyze the data, creating a world map of failed RDP attempts.
12. **Event Viewer Display and Custom PowerShell Script:**
    a. Display Event Viewer logs of failed RDP attempts and implement a custom PowerShell script parsing data from a third-party API.



law-honeypot1

Netherlands - 94.232.43.50
349

Seychelles - 5.181.86.111
4

United States - 67.175.49.169
3