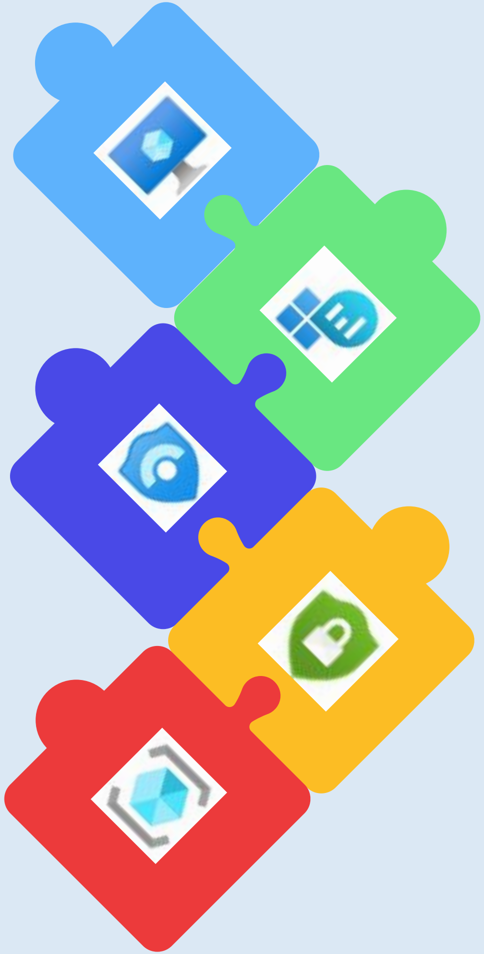
CSCI 400 Project Microsoft Azure Sentinel: Cloud-Based SIEM

- Enako (Maya) Hori, Wend Tin Basile Sam, Miguel Sanchez, Syed Farabi, Rudy, Chrisin Jacob



Overview

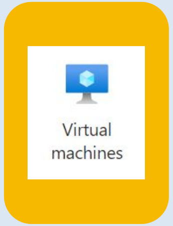
- Utilize Microsoft Azure to deepen our understanding on Security information and event management (SIEM)
- Display the cyber attack information in a graphical interface for quick reference
- Emphasize the importance of data analysis methods

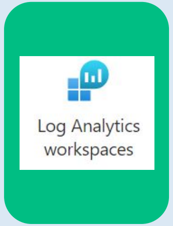
Vocabulary

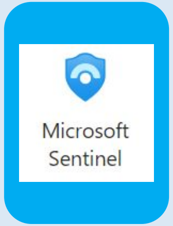
Security information and event management (Siem)	Security software that helps recognize and analyze the potential threats before they cause any harm
Honeypot	Intentionally discoverable device to lure the attacker and collect data
Application Programming Interface	Any software or rules that allow two applications to communicate with each other
Powershell	Task automation framework and scripting language

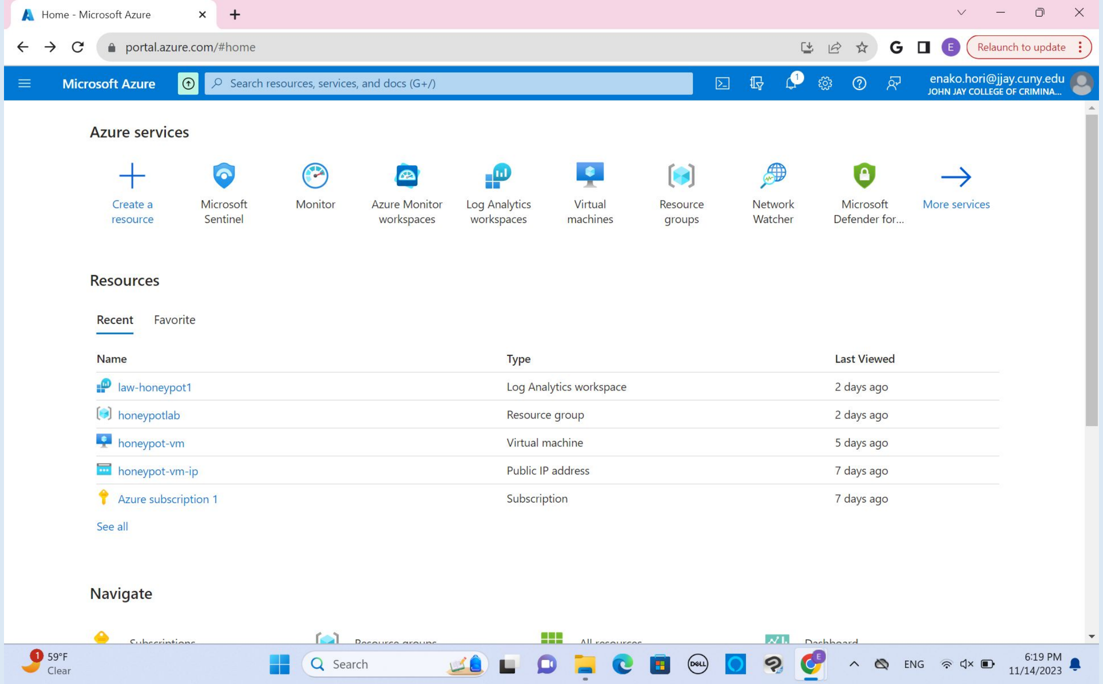
What is Microsoft Azure?

- Public cloud computing platform
- Range of cloud services and tools
- Tools that we are going to be using:









Azure services

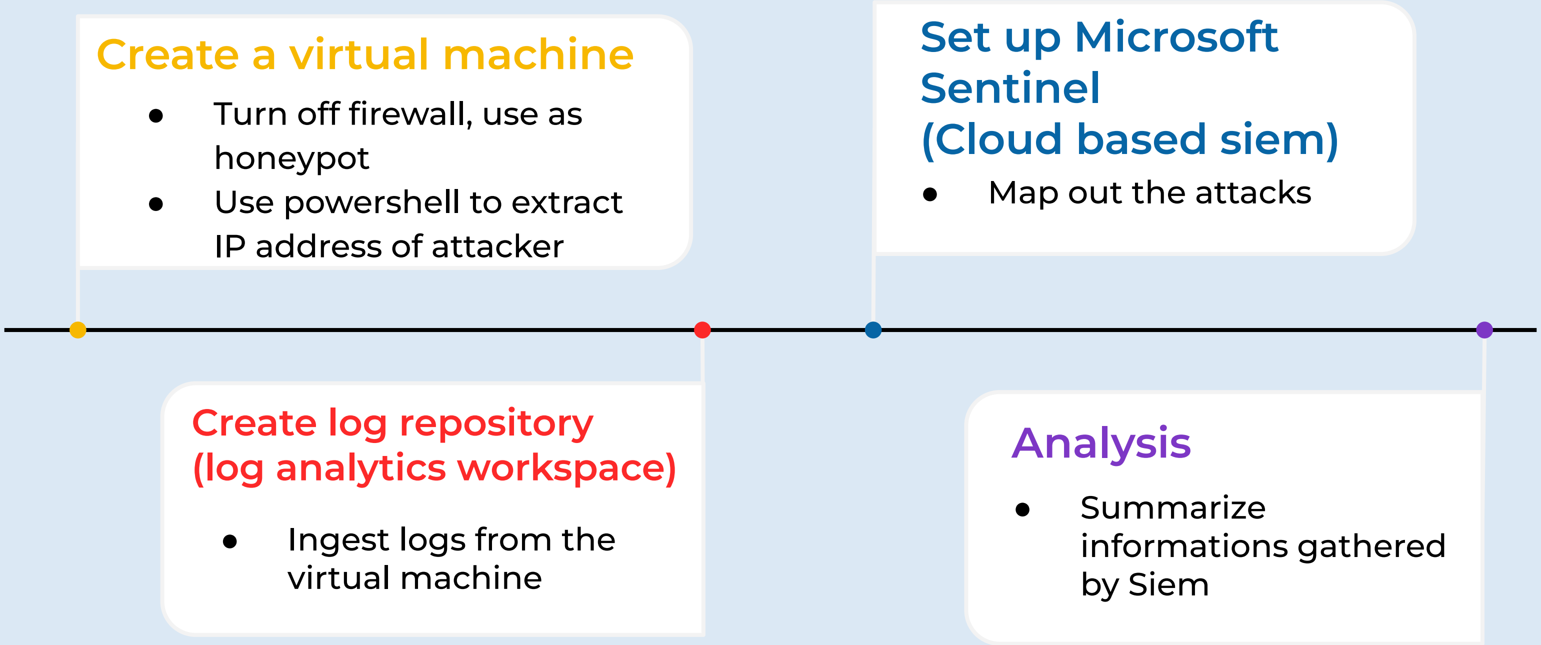
Resources

Name	Type	Last Viewed
law-honeypot1	Log Analytics workspace	2 days ago
honeypotlab	Resource group	2 days ago
honeypot-vm	Virtual machine	5 days ago
honeypot-vm-ip	Public IP address	7 days ago
Azure subscription 1	Subscription	7 days ago

Navigate

Our Tasks

Goal: demonstrate how to collect and analyze the threats on the VM



Create a virtual machine

- Turn off firewall, use as honeypot
- Use powershell to extract IP address of attacker

Create log repository (log analytics workspace)

- Ingest logs from the virtual machine

Set up Microsoft Sentinel (Cloud based siem)

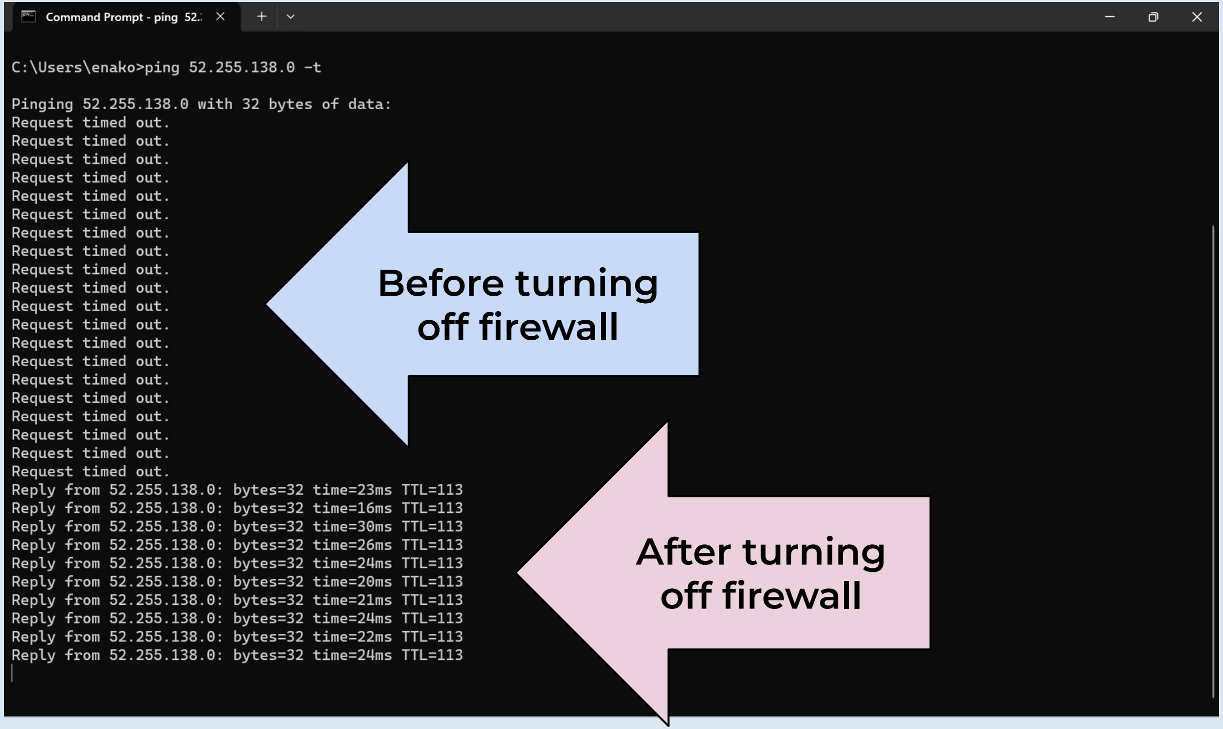
- Map out the attacks

Analysis

- Summarize informations gathered by Siem

Vulnerable Virtual Machine

- Turn off firewall
- Respond to IP Ping
- More discoverable

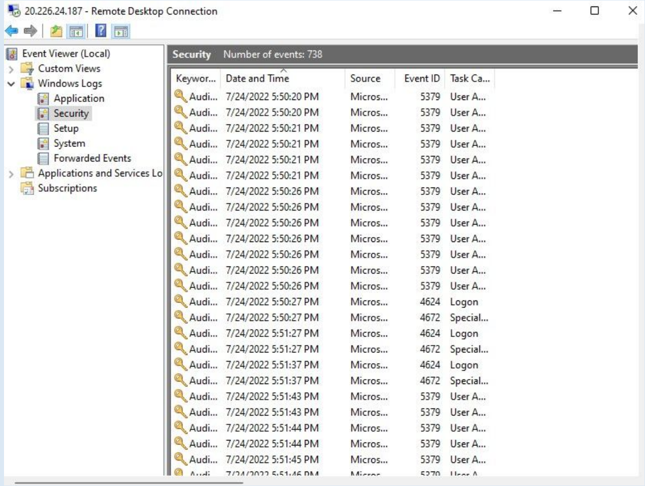


```
C:\Users\enako>ping 52.255.138.0 -t

Pinging 52.255.138.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 52.255.138.0: bytes=32 time=23ms TTL=113
Reply from 52.255.138.0: bytes=32 time=16ms TTL=113
Reply from 52.255.138.0: bytes=32 time=30ms TTL=113
Reply from 52.255.138.0: bytes=32 time=26ms TTL=113
Reply from 52.255.138.0: bytes=32 time=24ms TTL=113
Reply from 52.255.138.0: bytes=32 time=20ms TTL=113
Reply from 52.255.138.0: bytes=32 time=21ms TTL=113
Reply from 52.255.138.0: bytes=32 time=24ms TTL=113
Reply from 52.255.138.0: bytes=32 time=22ms TTL=113
Reply from 52.255.138.0: bytes=32 time=24ms TTL=113
```

Before turning off firewall

After turning off firewall

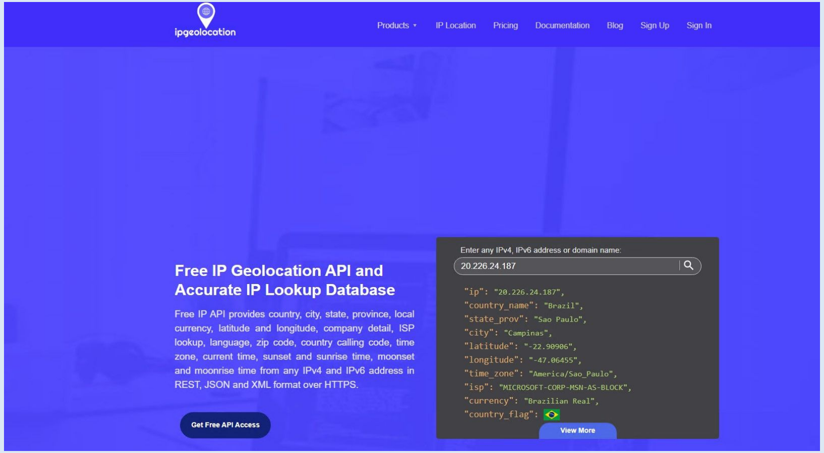
Powershell and API`



20.226.24.187 - Remote Desktop Connection

Security Number of events: 738

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audi...	7/24/2022 5:50:20 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:20 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:21 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:21 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:21 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:21 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:26 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:26 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:26 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:26 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:26 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:26 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:26 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:50:27 PM	Micros...	4624	Logon
Audi...	7/24/2022 5:50:27 PM	Micros...	4672	Special...
Audi...	7/24/2022 5:51:27 PM	Micros...	4624	Logon
Audi...	7/24/2022 5:51:27 PM	Micros...	4672	Special...
Audi...	7/24/2022 5:51:37 PM	Micros...	4624	Logon
Audi...	7/24/2022 5:51:37 PM	Micros...	4672	Special...
Audi...	7/24/2022 5:51:43 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:51:43 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:51:44 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:51:44 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:51:45 PM	Micros...	5379	User A...
Audi...	7/24/2022 5:51:46 PM	Micros...	5379	User A...

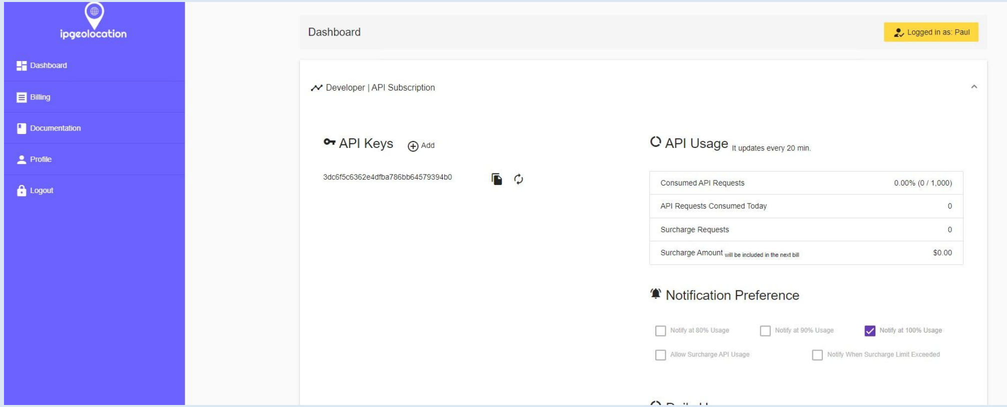


Free IP Geolocation API and Accurate IP Lookup Database

Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonset and moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.

Enter any IPv4, IPv6 address or domain name: 20.226.24.187

```
"ip": "20.226.24.187",
"country_name": "Brazil",
"state_prov": "Sao Paulo",
"city": "Campinas",
"latitude": "-22.90906",
"longitude": "-47.06455",
"time_zone": "America/Sao_Paulo",
"isp": "MICROSOFT-CORP-MSN-AS-BLOCK",
"currency": "Brazilian Real",
"country_flag":
```



Dashboard

Logged in as: Paul

Developer | API Subscription

API Keys ⊕ Add

3dc6f5c6362e4dfba786bb64579394b0

API Usage It updates every 20 min.

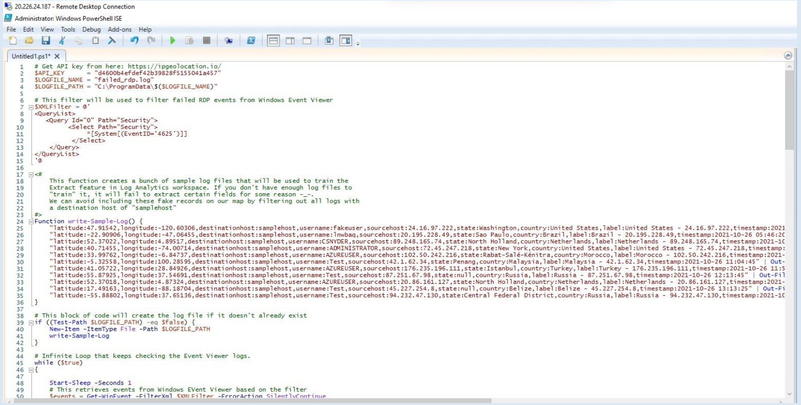
Consumed API Requests	0.00% (0 / 1,000)
API Requests Consumed Today	0
Surcharge Requests	0
Surcharge Amount will be included in the next bill	$0.00

Notification Preference

☐ Notify at 80% Usage ☐ Notify at 90% Usage ☑ Notify at 100% Usage

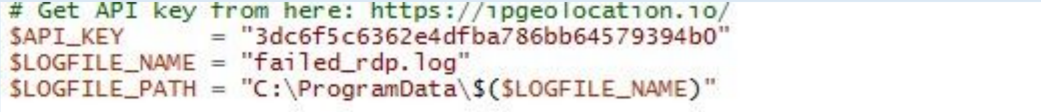
☐ Allow Surcharge API Usage ☐ Notify When Surcharge Limit Exceeded

Powershell and API

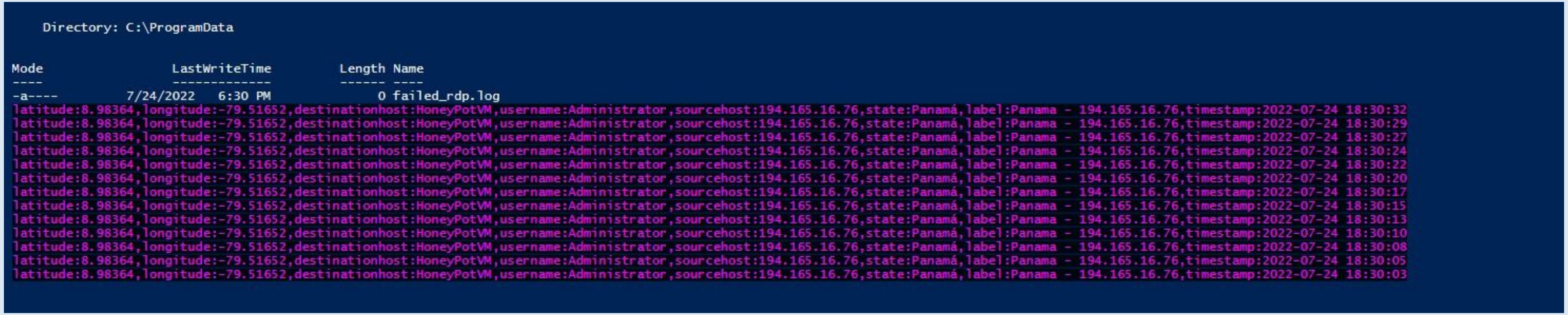


20.226.24.187 - Remote Desktop Connection
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "d4600b4efdef42b39828f5155041a457"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
          </Select>
    </Query>
</QueryList>
'@

<#
    This function creates a bunch of sample log files that will be used to train the
    Extract feature in Log Analytics workspace. If you don't have enough log files to
    "train" it, it will fail to extract certain fields for some reason -_-.
    We can avoid including these fake records on our map by filtering out all logs with
    a destination host of "samplehost"
#>
Function write-Sample-Log() {
    "latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24.16.97.222,timestamp:2021
    "latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:2C
    "latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlands - 89.248.165.74,timestamp:2021-1C
    "latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,timestamp:
    "latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Morocco - 102.50.242.216,timestamp:2021-
    "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,timestamp:2021-10-26 11:04:45" | Out-
    "latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey - 176.235.196.111,timestamp:2021-10-26 11:5
    "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,timestamp:2021-10-26 12:13:45" | Out-Fil
    "latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherlands - 20.86.161.127,timestamp:2021-
    "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,timestamp:2021-10-26 13:13:25" | Out-Fi
    "latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,country:Russia,label:Russia - 94.232.47.130,timestamp:2021-1C
}

# This block of code will create the log file if it doesn't already exist
if ((Test-Path $LOGFILE_PATH) -eq $false) {
    New-Item -ItemType File -Path $LOGFILE_PATH
    write-Sample-Log
}

# Infinite Loop that keeps checking the Event Viewer logs.
while ($true)
{

    Start-Sleep -Seconds 1
    # This retrieves events from Windows EVent Viewer based on the filter
    $events = Get-WinEvent -FilterXml $XMLFilter -ErrorAction SilentlyContinue
```

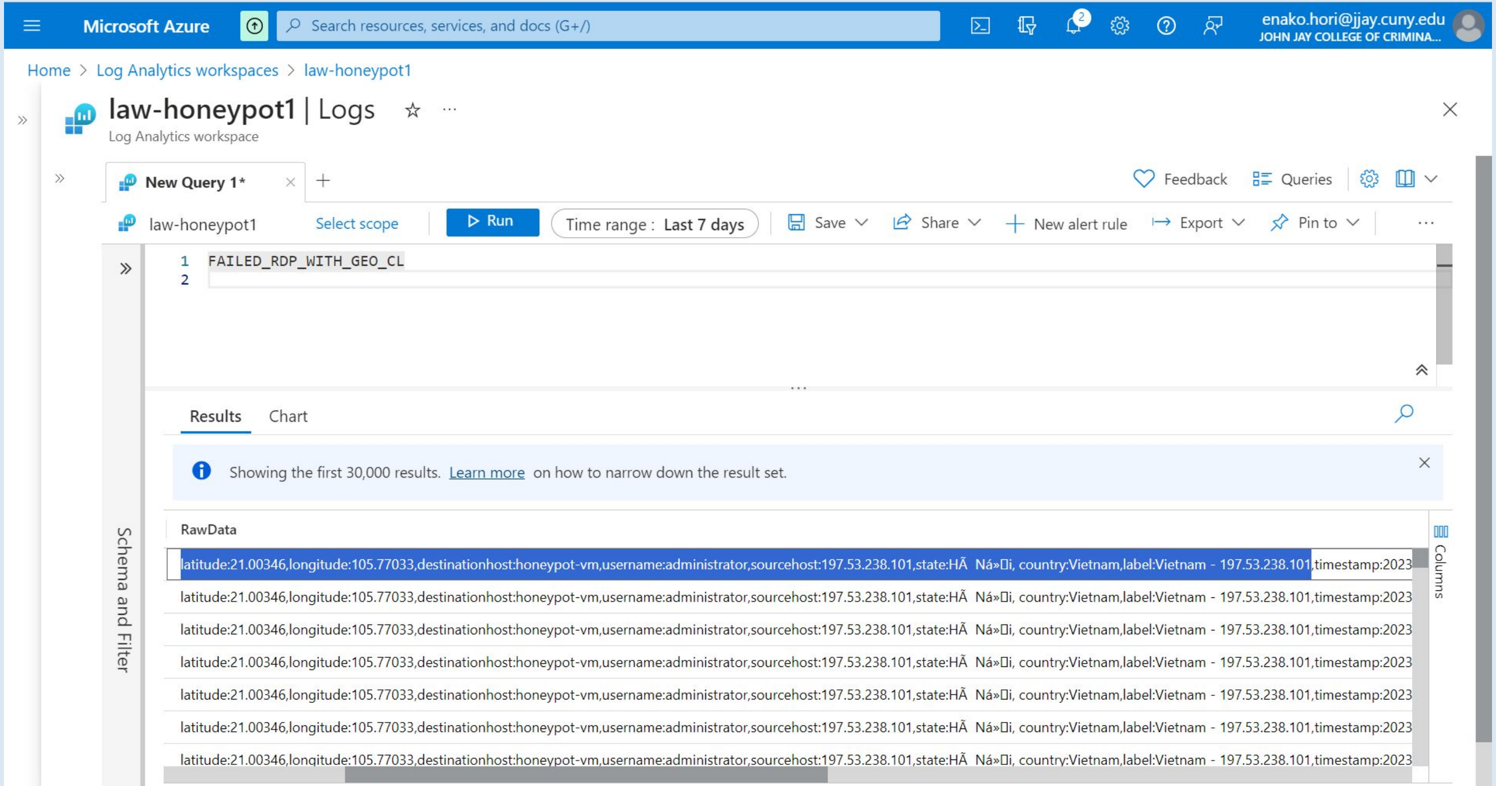


```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "3dc6f5c6362e4dfba786bb64579394b0"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"
```



```
    Directory: C:\ProgramData


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/24/2022   6:30 PM              0 failed_rdp.log
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:32
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:29
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:27
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:24
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:22
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:20
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:17
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:15
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:13
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:10
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:08
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:05
latitude:8.98364,longitude:-79.51652,destinationhost:HoneyPotVM,username:Administrator,sourcehost:194.165.16.76,state:Panamá,label:Panama - 194.165.16.76,timestamp:2022-07-24 18:30:03
```

Log Query and Table



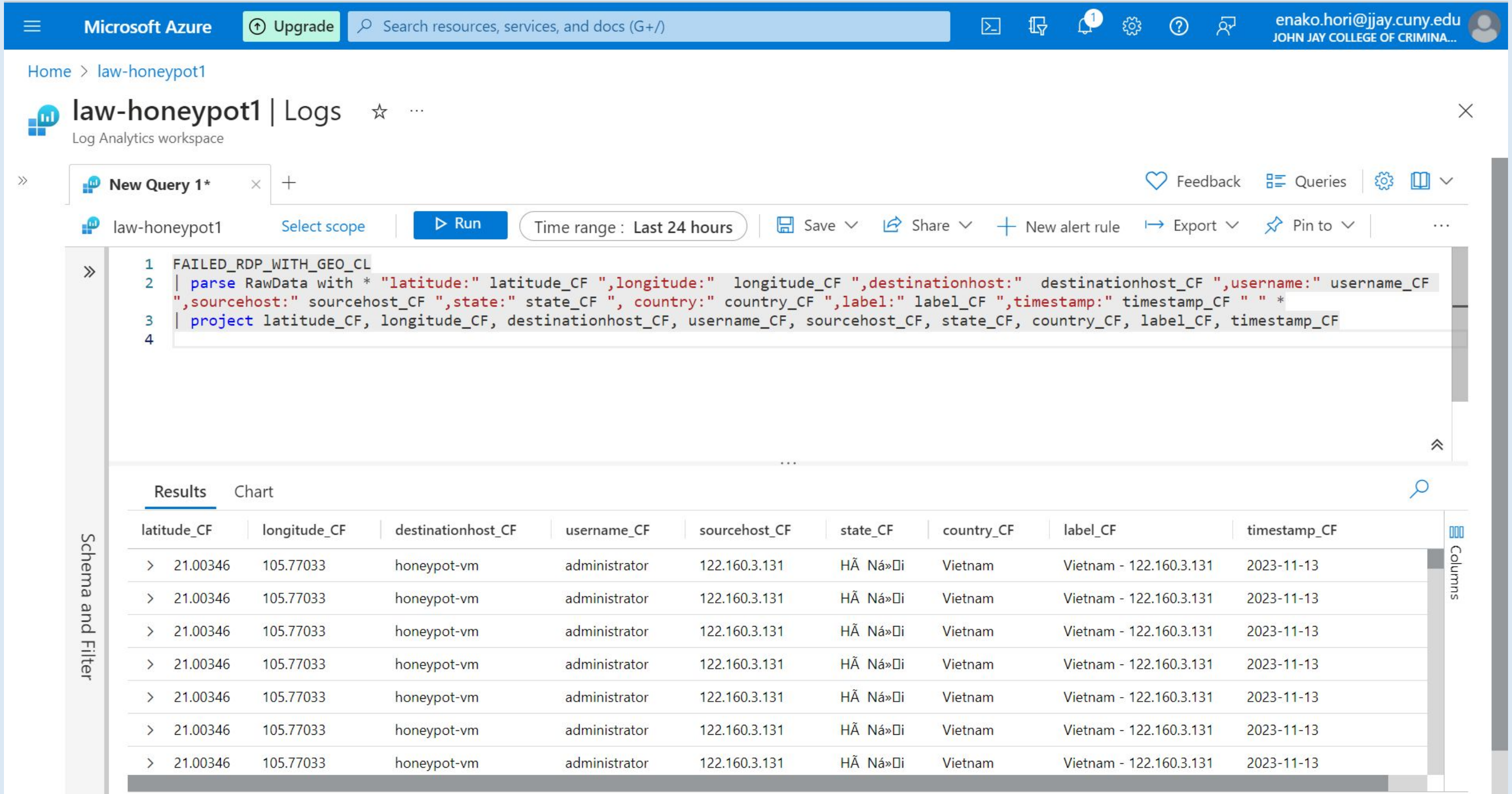
Time range : Last 7 days

```
FAILED_RDP_WITH_GEO_CL
```

Showing the first 30,000 results. Learn more on how to narrow down the result set.

RawData
latitude:21.00346,longitude:105.77033,destinationhost:honeypot-vm,username:administrator,sourcehost:197.53.238.101,state:HÃ Ná»□i, country:Vietnam,label:Vietnam - 197.53.238.101,timestamp:2023
latitude:21.00346,longitude:105.77033,destinationhost:honeypot-vm,username:administrator,sourcehost:197.53.238.101,state:HÃ Ná»□i, country:Vietnam,label:Vietnam - 197.53.238.101,timestamp:2023
latitude:21.00346,longitude:105.77033,destinationhost:honeypot-vm,username:administrator,sourcehost:197.53.238.101,state:HÃ Ná»□i, country:Vietnam,label:Vietnam - 197.53.238.101,timestamp:2023
latitude:21.00346,longitude:105.77033,destinationhost:honeypot-vm,username:administrator,sourcehost:197.53.238.101,state:HÃ Ná»□i, country:Vietnam,label:Vietnam - 197.53.238.101,timestamp:2023
latitude:21.00346,longitude:105.77033,destinationhost:honeypot-vm,username:administrator,sourcehost:197.53.238.101,state:HÃ Ná»□i, country:Vietnam,label:Vietnam - 197.53.238.101,timestamp:2023
latitude:21.00346,longitude:105.77033,destinationhost:honeypot-vm,username:administrator,sourcehost:197.53.238.101,state:HÃ Ná»□i, country:Vietnam,label:Vietnam - 197.53.238.101,timestamp:2023
latitude:21.00346,longitude:105.77033,destinationhost:honeypot-vm,username:administrator,sourcehost:197.53.238.101,state:HÃ Ná»□i, country:Vietnam,label:Vietnam - 197.53.238.101,timestamp:2023

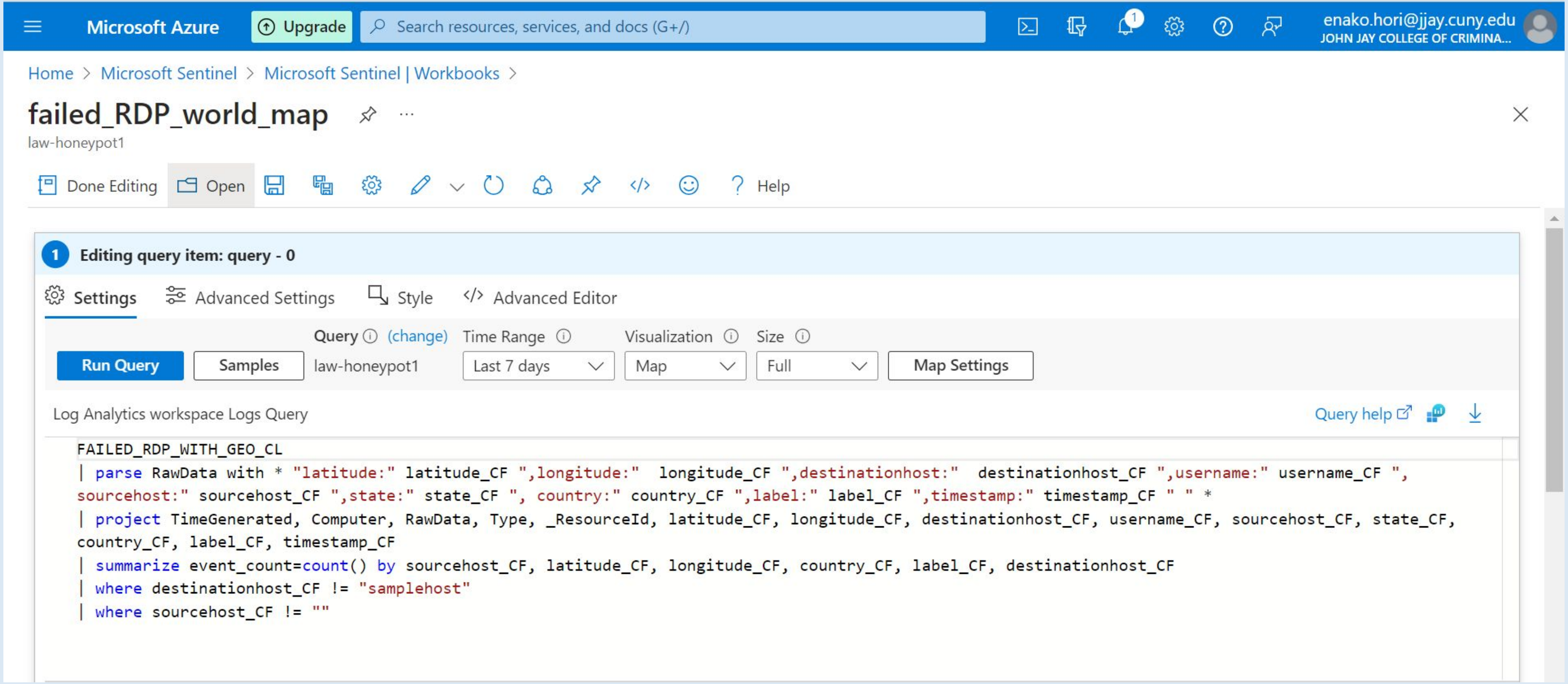
Log Query and Table



```
FAILED_RDP_WITH_GEO_CL
| parse RawData with * "latitude:" latitude_CF ",longitude:"  longitude_CF ",destinationhost:"  destinationhost_CF ",username:" username_CF
",sourcehost:" sourcehost_CF ",state:" state_CF ", country:" country_CF ",label:" label_CF ",timestamp:" timestamp_CF " " *
| project latitude_CF, longitude_CF, destinationhost_CF, username_CF, sourcehost_CF, state_CF, country_CF, label_CF, timestamp_CF
```

latitude_CF	longitude_CF	destinationhost_CF	username_CF	sourcehost_CF	state_CF	country_CF	label_CF	timestamp_CF
> 21.00346	105.77033	honeypot-vm	administrator	122.160.3.131	HÃ Ná»□i	Vietnam	Vietnam - 122.160.3.131	2023-11-13
> 21.00346	105.77033	honeypot-vm	administrator	122.160.3.131	HÃ Ná»□i	Vietnam	Vietnam - 122.160.3.131	2023-11-13
> 21.00346	105.77033	honeypot-vm	administrator	122.160.3.131	HÃ Ná»□i	Vietnam	Vietnam - 122.160.3.131	2023-11-13
> 21.00346	105.77033	honeypot-vm	administrator	122.160.3.131	HÃ Ná»□i	Vietnam	Vietnam - 122.160.3.131	2023-11-13
> 21.00346	105.77033	honeypot-vm	administrator	122.160.3.131	HÃ Ná»□i	Vietnam	Vietnam - 122.160.3.131	2023-11-13
> 21.00346	105.77033	honeypot-vm	administrator	122.160.3.131	HÃ Ná»□i	Vietnam	Vietnam - 122.160.3.131	2023-11-13
> 21.00346	105.77033	honeypot-vm	administrator	122.160.3.131	HÃ Ná»□i	Vietnam	Vietnam - 122.160.3.131	2023-11-13

Data Visualization



failed_RDP_world_map

law-honeypot1

1 Editing query item: query - 0

Query (change): law-honeypot1

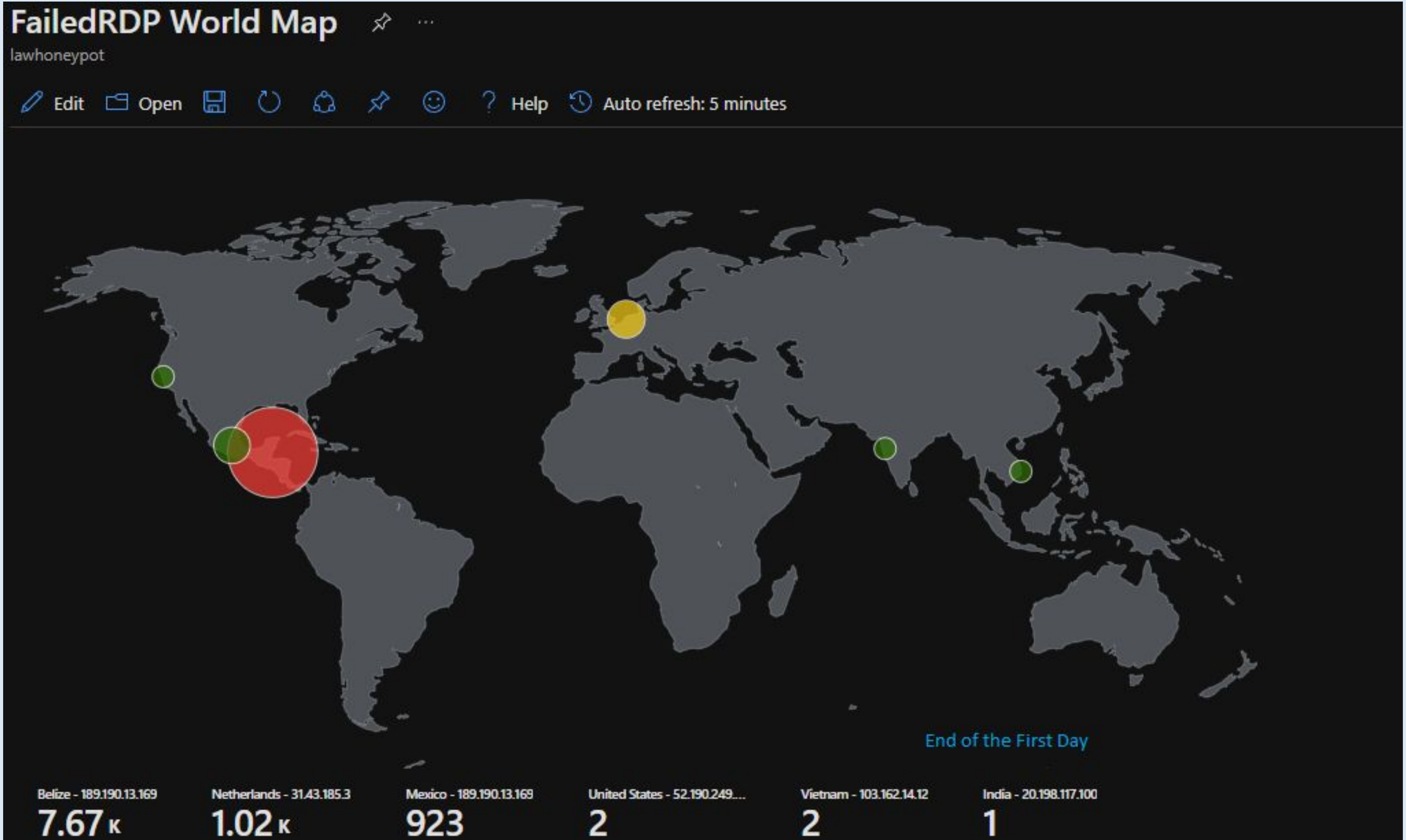
Time Range: Last 7 days

Visualization: Map

Size: Full

Log Analytics workspace Logs Query

```
FAILED_RDP_WITH_GEO_CL
| parse RawData with * "latitude:" latitude_CF ",longitude:"  longitude_CF ",destinationhost:"  destinationhost_CF ",username:" username_CF ",
sourcehost:" sourcehost_CF ",state:" state_CF ", country:" country_CF ",label:" label_CF ",timestamp:" timestamp_CF " " *
| project TimeGenerated, Computer, RawData, Type, _ResourceId, latitude_CF, longitude_CF, destinationhost_CF, username_CF, sourcehost_CF, state_CF,
country_CF, label_CF, timestamp_CF
| summarize event_count=count() by sourcehost_CF, latitude_CF, longitude_CF, country_CF, label_CF, destinationhost_CF
| where destinationhost_CF != "samplehost"
| where sourcehost_CF != ""
```

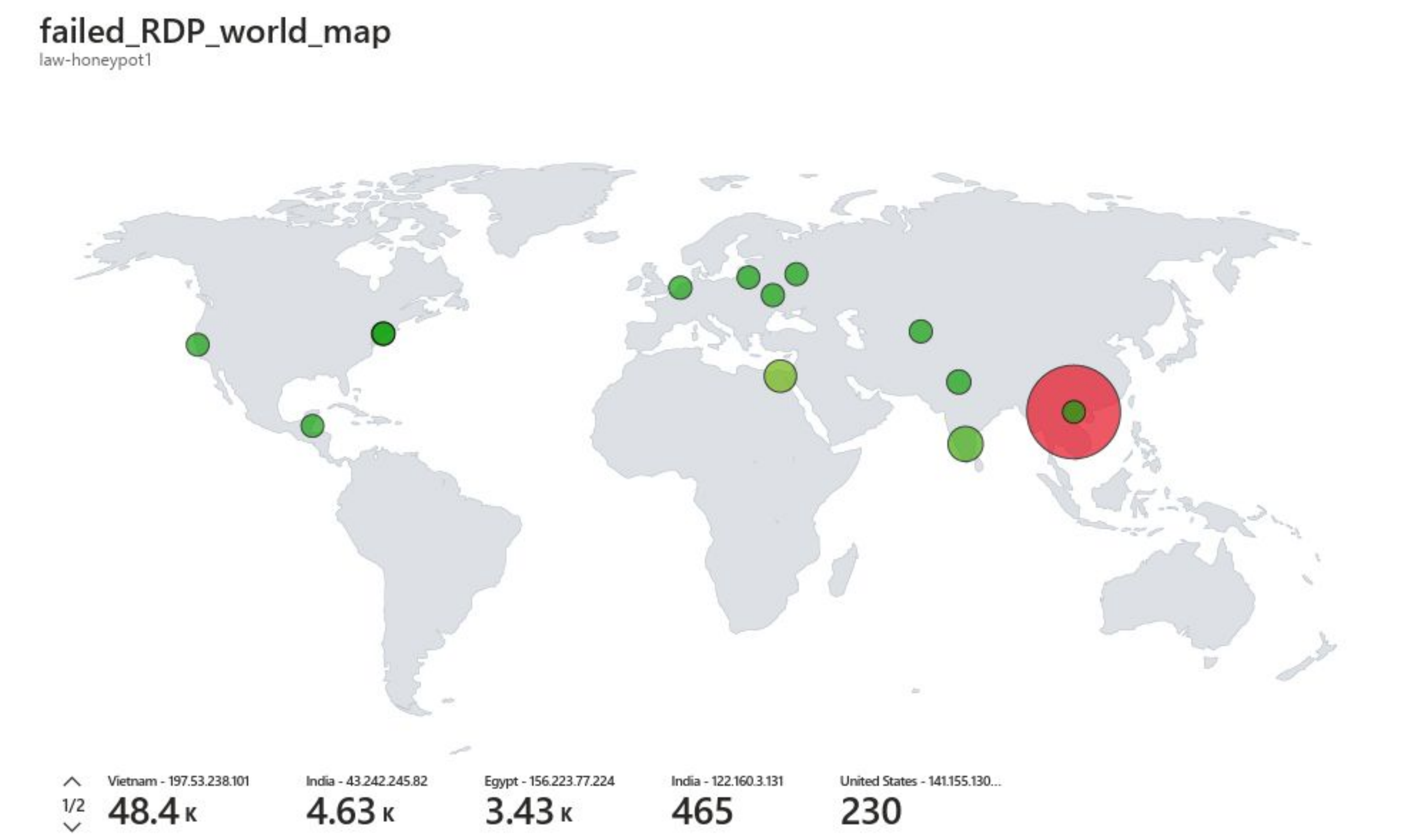


FailedRDP World Map

lawhoneypot

End of the First Day

Belize - 189.190.13.169	Netherlands - 31.43.185.3	Mexico - 189.190.13.169	United States - 52.190.249....	Vietnam - 103.162.14.12	India - 20.198.117.100
7.67 K	1.02 K	923	2	2	1



failed_RDP_world_map

law-honeypot1

Vietnam - 197.53.238.101
48.4 K

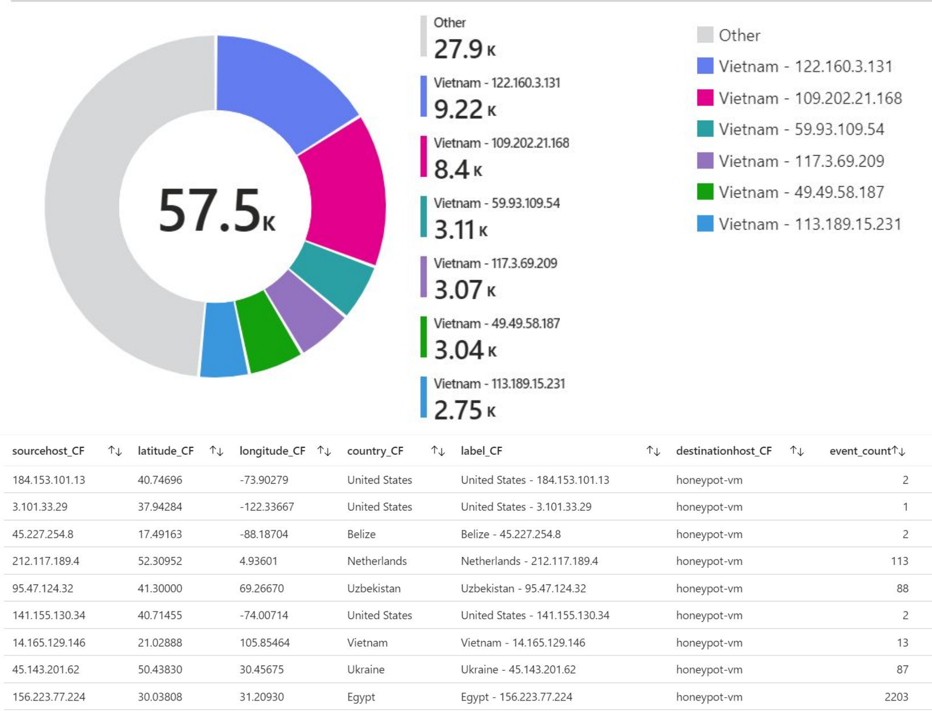
India - 43.242.245.82
4.63 K

Egypt - 156.223.77.224
3.43 K

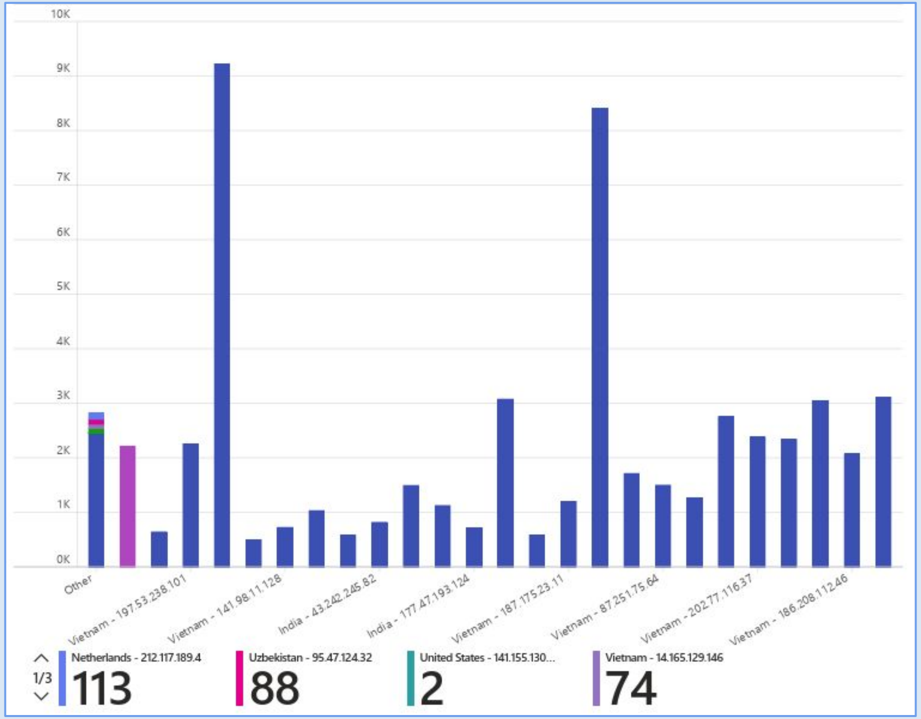
India - 122.160.3.131
465

United States - 141.155.130...
230

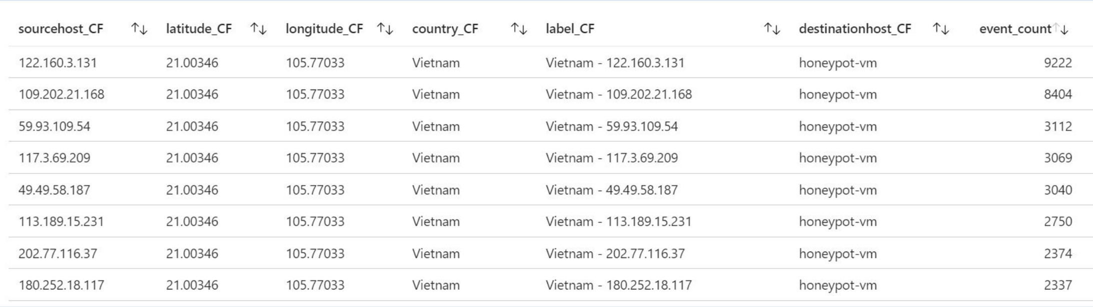
Collected Data



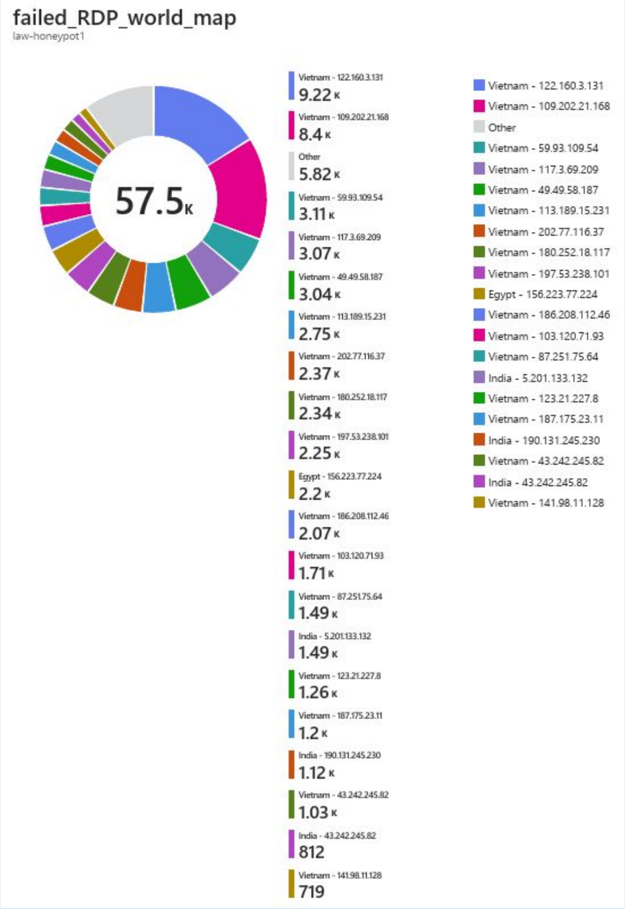
sourcehost_CF ↑↓	latitude_CF ↑↓	longitude_CF ↑↓	country_CF ↑↓	label_CF ↑↓	destinationhost_CF ↑↓	event_count↑↓
184.153.101.13	40.74696	-73.90279	United States	United States - 184.153.101.13	honeypot-vm	2
3.101.33.29	37.94284	-122.33667	United States	United States - 3.101.33.29	honeypot-vm	1
45.227.254.8	17.49163	-88.18704	Belize	Belize - 45.227.254.8	honeypot-vm	2
212.117.189.4	52.30952	4.93601	Netherlands	Netherlands - 212.117.189.4	honeypot-vm	113
95.47.124.32	41.30000	69.26670	Uzbekistan	Uzbekistan - 95.47.124.32	honeypot-vm	88
141.155.130.34	40.71455	-74.00714	United States	United States - 141.155.130.34	honeypot-vm	2
14.165.129.146	21.02888	105.85464	Vietnam	Vietnam - 14.165.129.146	honeypot-vm	13
45.143.201.62	50.43830	30.45675	Ukraine	Ukraine - 45.143.201.62	honeypot-vm	87
156.223.77.224	30.03808	31.20930	Egypt	Egypt - 156.223.77.224	honeypot-vm	2203



Further Detailed Data



sourcehost_CF ↑↓	latitude_CF ↑↓	longitude_CF ↑↓	country_CF ↑↓	label_CF ↑↓	destinationhost_CF ↑↓	event_count ↑↓
122.160.3.131	21.00346	105.77033	Vietnam	Vietnam - 122.160.3.131	honeypot-vm	9222
109.202.21.168	21.00346	105.77033	Vietnam	Vietnam - 109.202.21.168	honeypot-vm	8404
59.93.109.54	21.00346	105.77033	Vietnam	Vietnam - 59.93.109.54	honeypot-vm	3112
117.3.69.209	21.00346	105.77033	Vietnam	Vietnam - 117.3.69.209	honeypot-vm	3069
49.49.58.187	21.00346	105.77033	Vietnam	Vietnam - 49.49.58.187	honeypot-vm	3040
113.189.15.231	21.00346	105.77033	Vietnam	Vietnam - 113.189.15.231	honeypot-vm	2750
202.77.116.37	21.00346	105.77033	Vietnam	Vietnam - 202.77.116.37	honeypot-vm	2374
180.252.18.117	21.00346	105.77033	Vietnam	Vietnam - 180.252.18.117	honeypot-vm	2337



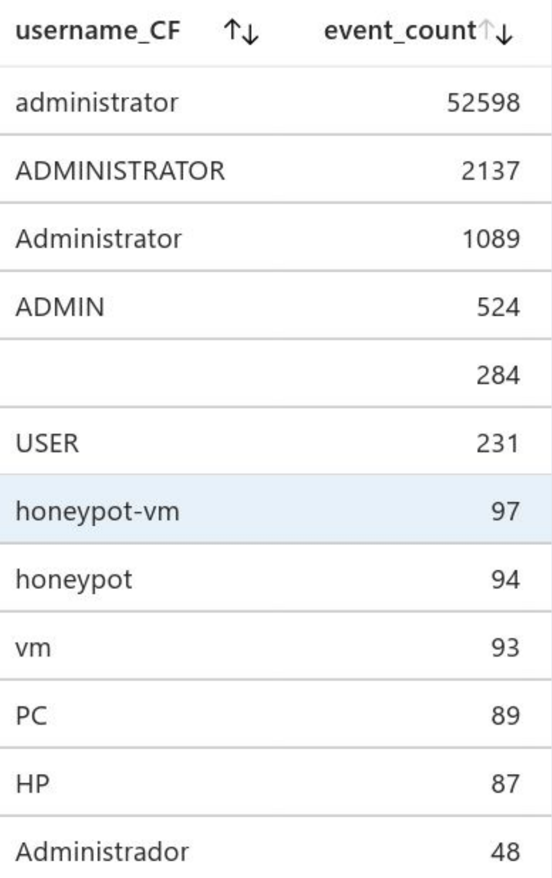
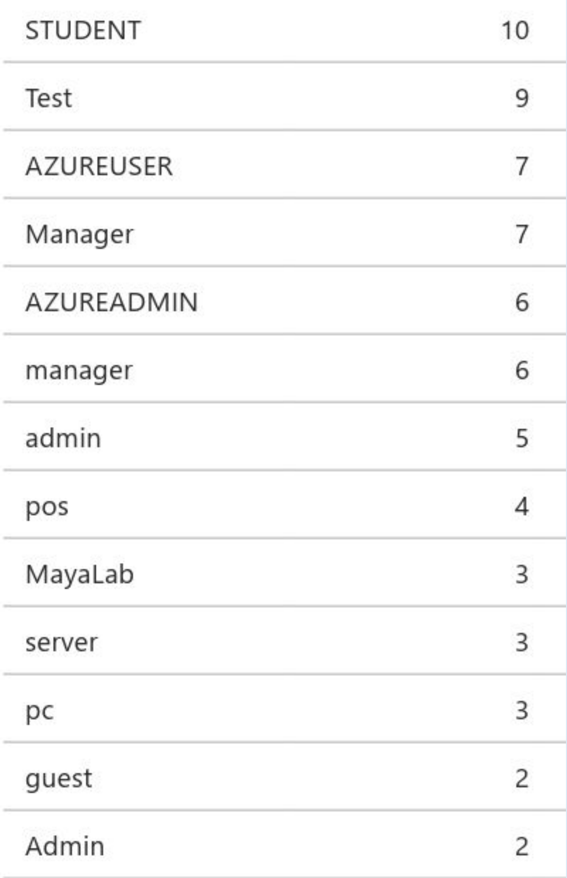
48.4k Attacks from vietnam
84% of all attacks recorded
4.63k attacks from India, 8% of all attacks

Vietnam - 122.160.3.131 tried brute force attack 9222 times, 16% of all attacks
At least 16 different IP address

Further Detailed Data

Most used usernames are admin related: 56353 attacks, 98%

Other usernames include a word “honeypot” or “azure”

username_CF ↑↓	event_count ↑↓
administrator	52598
ADMINISTRATOR	2137
Administrator	1089
ADMIN	524
	284
USER	231
honeypot-vm	97
honeypot	94
vm	93
PC	89
HP	87
Administrador	48
STUDENT	10
Test	9
AZUREUSER	7
Manager	7
AZUREADMIN	6
manager	6
admin	5
pos	4
MayaLab	3
server	3
pc	3
guest	2
Admin	2

Overall analysis

- The attacks come from various countries and it varies on the virtual machine
- In our case, there tends to be one country that performs the majority of attacks with significantly few number of attacks from other countries
- The username such as Admin, student, and user were often used for the brute force attacks
  - It is safer to change the username to something that is not easy to guess

Summary

- Azure Sentinel stands out as a robust and forward-looking Security Information and Event Management (SIEM) solution,
- Incorporates power of cloud-native architecture and seamless integration with Microsoft Azure services.
- Advanced threat detection capabilities, automated response mechanisms, and customizable reporting tools
- Scalability, cost-efficiency, and interoperability with third-party solutions
- Azure Sentinel emerges as a compelling choice for businesses seeking a comprehensive and agile approach to security, whether in on-premises or cloud environments.

References

- Josh Makador - https://youtu.be/RoZeVbbZ0o0?si=_xodlLhTd00ZHw9j
- Siem tutorial | Azure sentinel tutorial

https://www.youtube.com/watch?v=RoZeVbbZ0o0&t=866s

- Powershell script

https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1

- IP geolocation API

https://ipgeolocation.io/