Implementation of a SIEM using Microsoft Azure Sentinel

A. Aziz Gafoor

Table of Contents

Introduction

Using Microsoft Azure cloud computing services this project aims to create a SIEM to monitor RDP attacks on a honeypot, extracting the attackers IP address and their geolocation based on the IP address. These details are then mapped out using Microsoft Sentinel to create a visual plot of the results.

Objectives:

- Create a virtual machine using Microsoft Azure
- Remove firewall inbound rules to make the virtual machine vulnerable to attacks
- Create a PowerShell script to extract specific events from event viewer
- Link log file on virtual machine to log workspace
- Import log data into Microsoft Sentinel and extract longitude and latitude data and map using pre-existing tools

Configuring a Virtual Machine

The first stage is to create a virtual machine, Figure 1 presents the information of the virtual machine, the IP address of the virtual machine is 172.205.130.75, which is used to connect to the honeypot via RDP in order to integrate the PowerShell script to record activity.

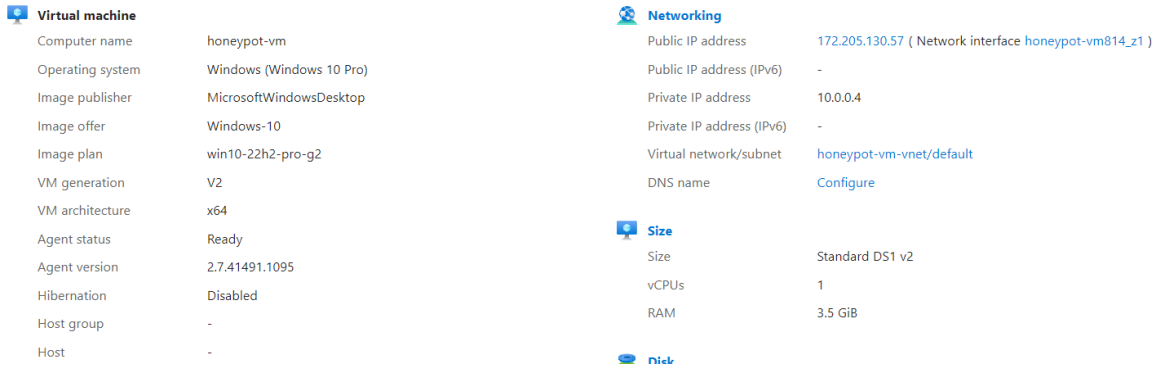

Figure 1. Virtual machine acting as a honeypot.

Figure 2 highlights the addition of the inbound security rule which makes the virtual machine vulnerable, attackers can now discover this machine and carry out RDP brute force attacks.

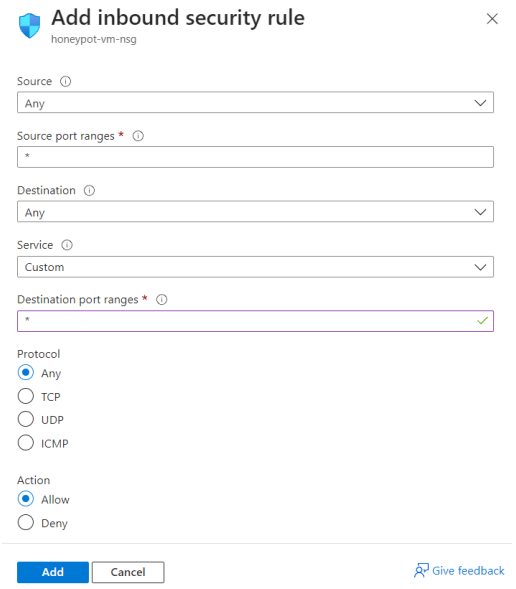

Figure 2. Inbound rule to allow connections to any destination port.

Tracking Failed RDP Logon Attempts

After the honeypot has been configured, a PowerShell script that continuously monitors failed login attempts with an event ID of 4625 is integrated into the virtual machine (see capture_4625.ps1 in the repository). This script uses the IP addresses of the attackers along with an IP geolocation API to calculate the latitude and longitude of the attackers. Then raw attacker data is then logged onto a text file called failed_rdp.txt, see appendix A.

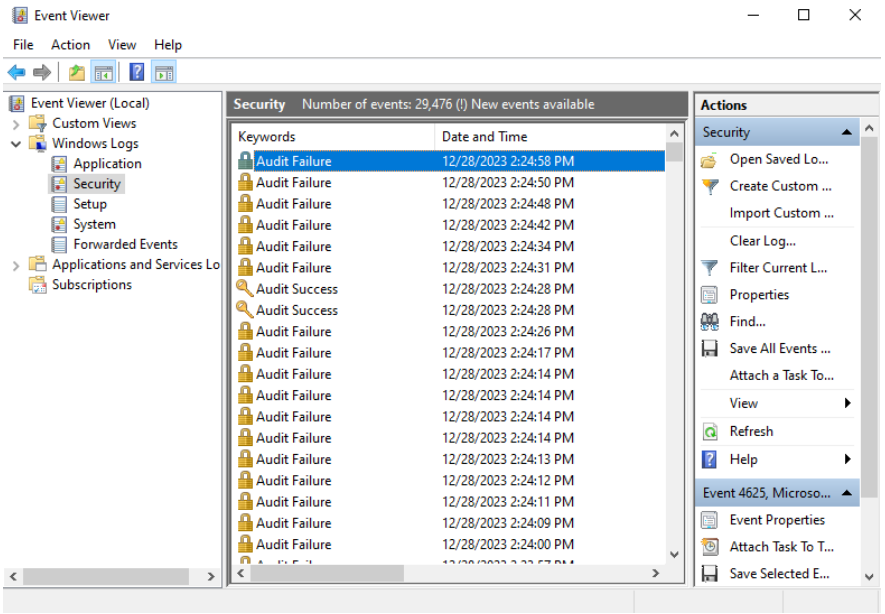

Figure 3. Example of failed logon events.

Figure 4 presents the process of exporting the log data on the honeypot to a log analytics table, this table is called through the FAILED_RDP_WITH_GEO_CL command.

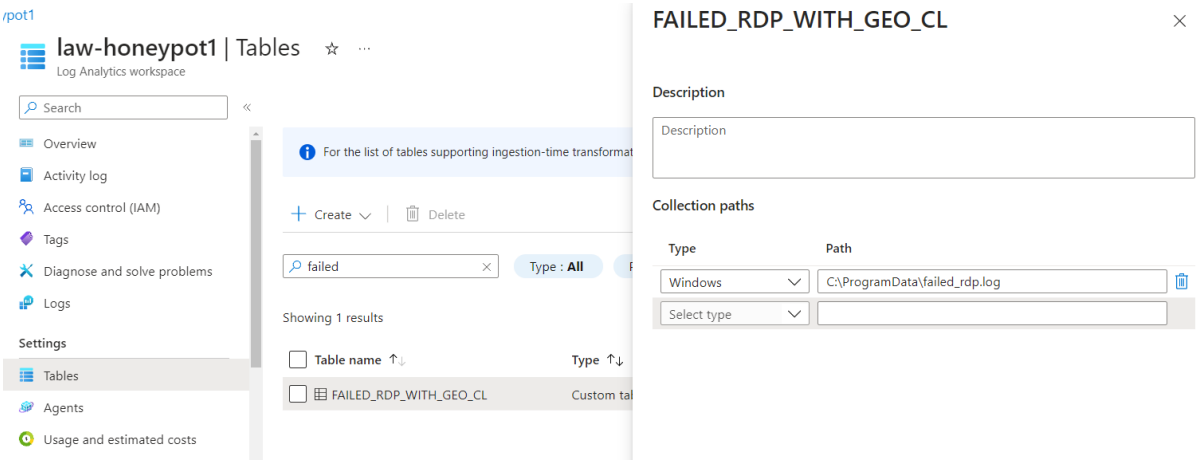

Figure 4. Exporting log data into a log analytics workspace.

The exported log data is then used in a Microsoft Sentinel workbook to visualise the log data. Figure 5 highlights the location of the workbook in the Microsoft Azure portal.

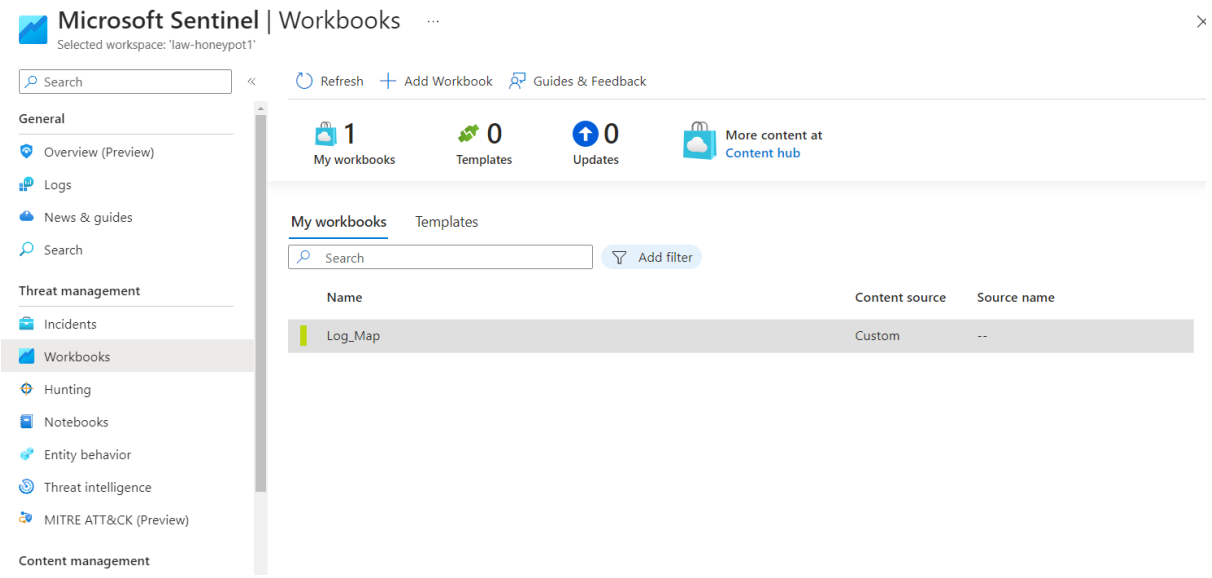

Figure 5. Microsoft Sentinel workbook to analyse extracted log data.

The log data is then formatted using a KQL script, first to extract the values and fields, then to amend the table with an 'event_count' column if there were multiple attacks from the same source host.

Log Analytics workspace Logs Query

```
FAILED_RDP_WITH_GEO_CL
| parse RawData with * "latitude:" Latitude ",longitude:" Longitude ",destinationhost:" DestinationHost ",username:" Username ",sourcehost:" Sourcehost ",state:" State ", country:" Country ",label:" Label ",timestamp:" Timestamp
| project Latitude, Longitude, DestinationHost, Username, Sourcehost, State, Country, Label, Timestamp
| where Latitude != ""
| summarize event_count=count() by Sourcehost, Latitude, Longitude, Country, Label, DestinationHost
| where DestinationHost != "samplehost"
| where Sourcehost != ""
```

Sourcehost	Latitude	Longitude	Country	Label	DestinationHost	event_count
45.141.84.51	59.88881	30.31671	Russia	Russia - 45.141.84.51	honeypot-vm	69
161.246.3.22	13.72989	100.77823	Thailand	Thailand - 161.246.3.22	honeypot-vm	24
154.53.167.3	40.19867	29.06271	Turkey	Turkey - 154.53.167.3	honeypot-vm	26
62.105.131.186	55.81657	37.53266	Russia	Russia - 62.105.131.186	honeypot-vm	12
45.136.6.104	39.89017	32.87139	Turkey	Turkey - 45.136.6.104	honeypot-vm	3
67.133.192.80	32.58997	-92.06862	United States	United States - 67.133.192.80	honeypot-vm	13
80.82.67.121	52.37022	4.89517	Netherlands	Netherlands - 80.82.67.121	honeypot-vm	3
92.46.215.250	47.09301	51.91461	Kazakhstan	Kazakhstan - 92.46.215.250	honeypot-vm	18
82.13.245.65	51.62310	-3.94086	United Kingdom	United Kingdom - 82.13.245.65	honeypot-vm	1
196.190.117.7	9.01334	38.75339	Ethiopia	Ethiopia - 196.190.117.7	honeypot-vm	1

Figure 6. KQL script to format the log table.

Results and Conclusion

The formatted log data is then plotted on a map with the size and colour of each point scaled to the number of events from the same location, the data below highlights the brute force RDP attacks over a time span of 10 minutes.

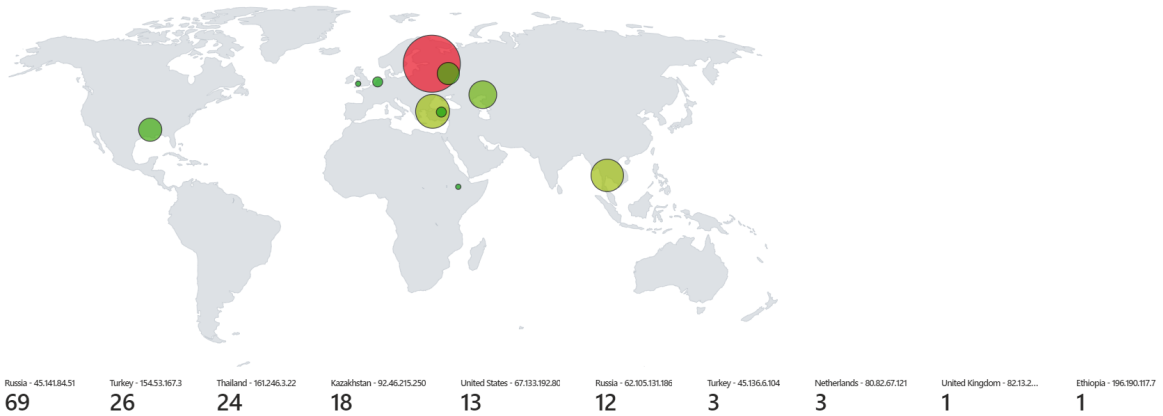

Figure 7. Mapping formatted log data onto a world map.

The 'capture_4625.ps1' script continuously monitors the virtual machine for new log on failures and updates the log on the virtual machine, the map detailing the attacks has been configured to refresh every hour by extracting and formatting the log data on the virtual machine.

Appendix A. Log Data

failed_rdp - Notepad

File Edit Format View Help

```
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:2021-10-26 03:28:29
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 05:46:20
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:2021-10-26 06:12:56
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:2021-10-26 10:44:07
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:2021-10-26 11:03:13
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
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 11:50:47
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
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:2021-10-26 12:33:46
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
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:2021-10-26 14:25:33
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:SHABEENA,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:35:48
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMIN,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:35:47
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:35:46
latitude:40.19867,longitude:29.06271,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:154.53.167.3,state:Bursa, country:Turkey,label:Turkey - 154.53.167.3,timestamp:2023-12-26 10:35:37
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:CHANTAL,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:35:36
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:SUMMA,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:35:24
latitude:55.81657,longitude:37.53266,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:62.105.131.186,state:Central Federal District, country:Russia,label:Russia - 62.105.131.186,timestamp:2023-12-26 10:35:22
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:SHLPREC,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:35:21
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:35:20
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMIN,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:35:19
latitude:40.19867,longitude:29.06271,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:154.53.167.3,state:Bursa, country:Turkey,label:Turkey - 154.53.167.3,timestamp:2023-12-26 10:35:16
latitude:39.89017,longitude:32.87139,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:45.136.6.104,state:Ankara, country:Turkey,label:Turkey - 45.136.6.104,timestamp:2023-12-26 10:35:12
latitude:32.58997,longitude:-92.06862,destinationhost:honeypot-vm,username:HP,sourcehost:67.133.192.80,state:Louisiana, country:United States,label:United States - 67.133.192.80,timestamp:2023-12-26 10:35:11
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:HUI,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:35:07
latitude:52.37022,longitude:4.89517,destinationhost:honeypot-vm,username:ROOT,sourcehost:80.82.67.121,state:North Holland, country:Netherlands,label:Netherlands - 80.82.67.121,timestamp:2023-12-26 10:35:00
latitude:40.19867,longitude:29.06271,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:154.53.167.3,state:Bursa, country:Turkey,label:Turkey - 154.53.167.3,timestamp:2023-12-26 10:34:55
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:DENISE,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:34:52
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:RAJU,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:34:41
latitude:55.81657,longitude:37.53266,destinationhost:honeypot-vm,username:ADMIN,sourcehost:62.105.131.186,state:Central Federal District, country:Russia,label:Russia - 62.105.131.186,timestamp:2023-12-26 10:34:39
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:SANDPIPERTRUC,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:34:38
latitude:40.19867,longitude:29.06271,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:154.53.167.3,state:Bursa, country:Turkey,label:Turkey - 154.53.167.3,timestamp:2023-12-26 10:34:34
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:34:30
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:34:26
latitude:32.58997,longitude:-92.06862,destinationhost:honeypot-vm,username:USER,sourcehost:67.133.192.80,state:Louisiana, country:United States,label:United States - 67.133.192.80,timestamp:2023-12-26 10:34:24
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:TARUN,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:34:18
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:MIGRATION,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:34:17
latitude:40.19867,longitude:29.06271,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:154.53.167.3,state:Bursa, country:Turkey,label:Turkey - 154.53.167.3,timestamp:2023-12-26 10:34:13
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:34:12
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:JOHANNE,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:34:10
latitude:47.09301,longitude:51.91461,destinationhost:honeypot-vm,username:ADMIN,sourcehost:92.46.215.250,state:Atyrau Region, country:Kazakhstan,label:Kazakhstan - 92.46.215.250,timestamp:2023-12-26 10:34:09
latitude:47.09301,longitude:51.91461,destinationhost:honeypot-vm,username:ADMIN,sourcehost:92.46.215.250,state:Atyrau Region, country:Kazakhstan,label:Kazakhstan - 92.46.215.250,timestamp:2023-12-26 10:34:07
latitude:55.81657,longitude:37.53266,destinationhost:honeypot-vm,username:ASUS,sourcehost:62.105.131.186,state:Central Federal District, country:Russia,label:Russia - 62.105.131.186,timestamp:2023-12-26 10:33:57
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:DATACENTER,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:33:55
latitude:47.09301,longitude:51.91461,destinationhost:honeypot-vm,username:ADMIN,sourcehost:92.46.215.250,state:Atyrau Region, country:Kazakhstan,label:Kazakhstan - 92.46.215.250,timestamp:2023-12-26 10:33:53
latitude:40.19867,longitude:29.06271,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:154.53.167.3,state:Bursa, country:Turkey,label:Turkey - 154.53.167.3,timestamp:2023-12-26 10:33:52
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:33:51
latitude:32.58997,longitude:-92.06862,destinationhost:honeypot-vm,username:ADMIN,sourcehost:67.133.192.80,state:Louisiana, country:United States,label:United States - 67.133.192.80,timestamp:2023-12-26 10:33:42
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:DENTAL,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:33:40
latitude:13.72989,longitude:100.77823,destinationhost:honeypot-vm,username:ADMIN,sourcehost:161.246.3.22,state:Krung Thep Maha Nakhon, country:Thailand,label:Thailand - 161.246.3.22,timestamp:2023-12-26 10:33:36
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:LANCELOT,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:33:32
latitude:40.19867,longitude:29.06271,destinationhost:honeypot-vm,username:ADMINISTRATOR,sourcehost:154.53.167.3,state:Bursa, country:Turkey,label:Turkey - 154.53.167.3,timestamp:2023-12-26 10:33:31
latitude:59.88881,longitude:30.31671,destinationhost:honeypot-vm,username:DIMAS,sourcehost:45.141.84.51,state:Northwestern Federal District, country:Russia,label:Russia - 45.141.84.51,timestamp:2023-12-26 10:33:25
```

Figure A.1. Extracted event data log file.