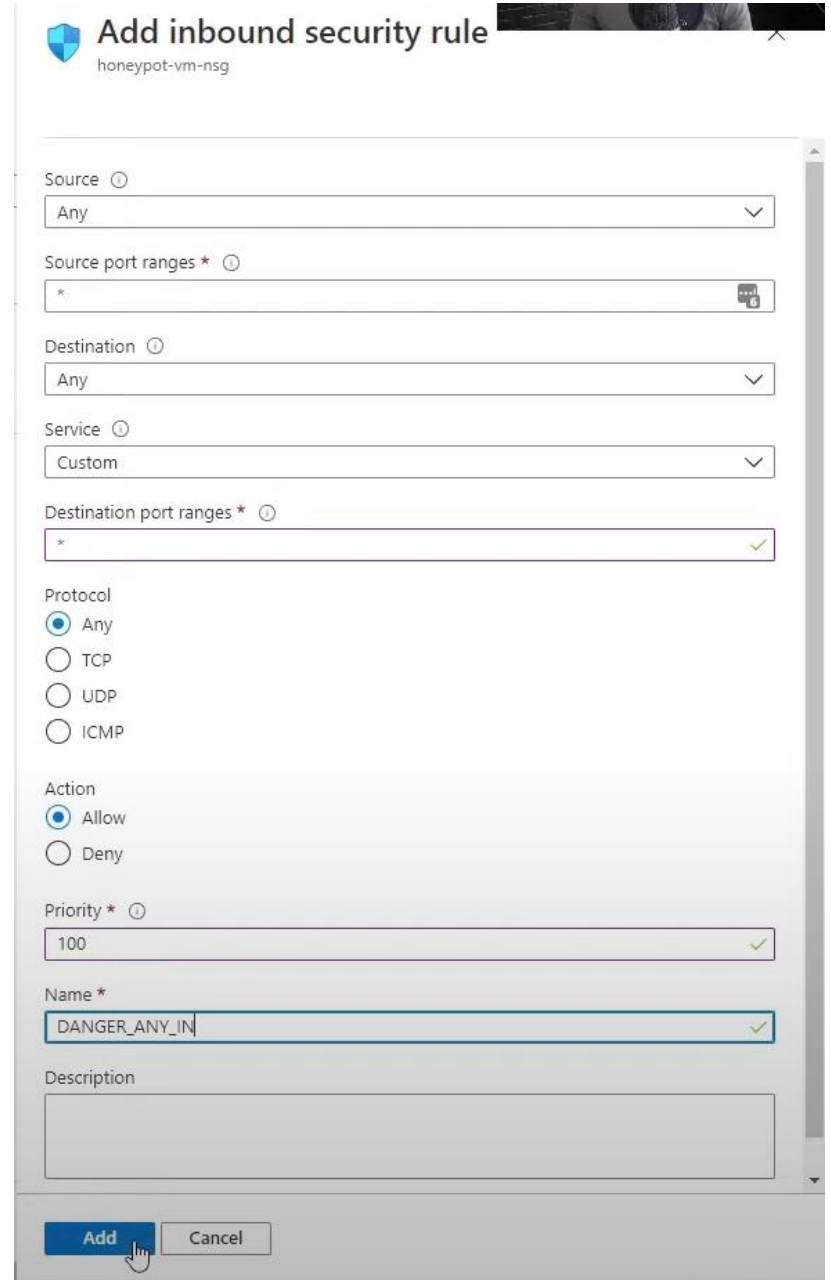


# HONEYPOT EXPERIMENT

Step-by-step instructions:

1. Create an Azure account  
<https://azure.microsoft.com/en-us/free/>
2. Create a virtual machine using Azure:

Under “NIC Security Group”, click on Advance and create a new network inbound rule  
Purpose: To allow traffic from the internet to Virtual machine. For VMs to be discoverable to the public internet



The screenshot shows the 'Add inbound security rule' dialog box in the Azure portal. The dialog is titled 'Add inbound security rule' and is for a resource named 'honeypot-vm-nsg'. The settings are as follows:

- Source:** Any
- Source port ranges:** \*
- Destination:** Any
- Service:** Custom
- Destination port ranges:** \*
- Protocol:** ☒ Any, ☐ TCP, ☐ UDP, ☐ ICMP
- Action:** ☒ Allow, ☐ Deny
- Priority:** 100
- Name:** DANGER\_ANY\_IN
- Description:** (Empty text box)

At the bottom, there are two buttons: 'Add' and 'Cancel'. A mouse cursor is pointing at the 'Add' button.

# Virtual machines

Default Directory (ezkel.ex@outlook.onmicrosoft.co...

+ Create   Switch to classic   ...

Filter for any field...

Name	
honeypotlab-vm	...

## honeypotlab-vm

Virtual machine

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
  - Connect
  - Bastion
- Networking
  - Network settings
  - Load balancing
  - Application security groups
  - Network manager
- Settings
  - Disks
  - Extensions + applications
  - Configuration
  - Advisor recommendations
  - Reprovision

Connect   Start   Restart   Stop   Hibernate (preview)   Capture   Delete   Refresh   Open in mobile   ...

### Essentials

Resource group [\(move\)](#)  
[honeypotlab](#)

Status  
Running

Location  
East US (Zone 1)

Subscription [\(move\)](#)  
[Azure subscription 1](#)

Subscription ID  
e36fb7e6-391c-47ac-9a37-6b286111785a

Availability zone  
1

Operating system  
Windows (Windows 10 Pro)

Size  
Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address  
[20.163.182.115](#)

Virtual network/subnet  
[honeypotlab-vm-vnet/default](#)

DNS name  
[Not configured](#)

Health state  
-

Time created  
5/11/2024, 5:46 PM UTC

Tags [\(edit\)](#)  
[Add tags](#)

Properties   Monitoring   Capabilities (7)   Recommendations   Tutorials

Virtual machine	
Computer name	honeypotlab-vm
Operating system	Windows (Windows 10 Pro)
VM generation	V2
VM architecture	x64

Networking	
Public IP address	<a href="#">20.163.182.115</a> ( Network interface <a href="#">honeypotlab-vm931_z1</a>
Public IP address (IPv6)	-
Private IP address	10.0.0.4



Virtual machine

Computer name	honeypotlab-vm
Operating system	Windows (Windows 10 Pro)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1117
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI



Availability + scaling

Availability zone	<a href="#">(edit)</a> 1
Availability set	-
Scale Set	-



Networking

Public IP address	20.163.182.115 ( Network <a href="#">honeypotlab-</a> ) interface <a href="#">vm931_z1</a>
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	<a href="#">honeypotlab-vm-vnet/default</a>
DNS name	<a href="#">Configure</a>



Size

Size	Standard D2s v3
vCPUs	2
RAM	8 GiB



Source image details

Source image publisher	MicrosoftWindowsDesktop
Source image offer	Windows-10
Source image plan	win10-22h2-pro-g2



Disk

OS disk
---------

Azure > Search “Log Analytics Workspace”

Look for Virtual machines, and connect the virtual machine we made from the beginning

Next, setup Azure Sentinel > “Create Azure Sentinel”

Add the honeypot virtual machine

3. Get the script in this Github:

[https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom Security Log Exporter.ps1](https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom%20Security%20Log%20Exporter.ps1)

Note: Make sure to create account and get the free API key here: <https://app.ipgeolocation.io/login>

4. Open the Powershell ISE inside the VM and insert the script and your very own API key.

5. Run the script.

## Log\_Exporter.ps1 X

```
1 # Get API key from here: https://ipgeolocation.io/
2 $API_KEY = "07024576b03c4aedba68651834d66037"
3 $LOGFILE_NAME = "failed_rdp_log"
4 $LOGFILE_PATH = "C:\ProgramData\" + ($LOGFILE_NAME)
5
6 # This filter will be used to filter failed RDP events from windows Event Viewer
7 $XMLFilter = @"
8 <QueryList>
9 <Query Id="0" Path="Security">
10 <Select Path="Security">
11 *[(System[EventID='4625'])]
12 </Select>
13 </Query>
14 </QueryList>
15 '@
16
17 <#
18 This function creates a bunch of sample log files that will be used to train the
19 Extract feature in Log Analytics workspace. If you don't have enough log files to
20 "train" it, it will fail to extract certain fields for some reason -.
21 We can avoid including these fake records on our map by filtering out all logs with
22 a destination host of "samplehost"
23 #>
24 Function Write-Sample-Log() {...}
25
26 # This block of code will create the log file if it doesn't already exist
27 if ((Test-Path $LOGFILE_PATH) -eq $false) {
28     New-Item -ItemType File -Path $LOGFILE_PATH
29     Write-Sample-Log
30 }
31
32 # Infinite Loop that keeps checking the Event Viewer logs.
33 while ($true)
34 {
35     $logs = Get-WinEvent -LogName Security -FilterXML $XMLFilter
36     $logs | ForEach-Object {
37         $log = $_
38         $lat = $log.Properties[0].Value
39         $lon = $log.Properties[1].Value
40         $dest = $log.Properties[2].Value
41         $user = $log.Properties[3].Value
42         $source = $log.Properties[4].Value
43         $state = $log.Properties[5].Value
44         $label = $log.Properties[6].Value
45         $timestamp = $log.Timestamp
46         $log | Out-File $LOGFILE_PATH -Append
47     }
48     Start-Sleep -s 10
49 }
```

latitude: 31.45571, longitude: 73.08039, destinationhost: honeypotlab-vm, username: fiadmin, sourcehost: 210.79.167.92, state: Punjab, label: Pakistan - 210.79.167.92, timestamp: 2024-05-11 18:09:37  
latitude: 40.71455, longitude: -74.00714, destinationhost: honeypotlab-vm, username: pukemalaki, sourcehost: 173.52.108.235, state: New York, label: United States - 173.52.108.235, timestamp: 2024-05-11 18:11:27  
latitude: -25.51567, longitude: -54.57010, destinationhost: honeypotlab-vm, username: F2MDBCj1, sourcehost: 167.250.160.135, state: Parana, label: Brazil - 167.250.160.135, timestamp: 2024-05-11 18:14:40  
latitude: 41.01525, longitude: 28.82306, destinationhost: honeypotlab-vm, username: F3211552, sourcehost: 185.141.33.162, state: Istanbul, label: Turkey - 185.141.33.162, timestamp: 2024-05-11 18:20:09  
latitude: -12.05613, longitude: -77.02679, destinationhost: honeypotlab-vm, username: f3li, sourcehost: 181.65.169.150, state: Lima, label: Peru - 181.65.169.150, timestamp: 2024-05-11 18:24:30  
latitude: 37.55632, longitude: -122.28809, destinationhost: honeypotlab-vm, username: f792gjwH, sourcehost: 76.14.34.33, state: California, label: United States - 76.14.34.33, timestamp: 2024-05-11 18:34:13  
latitude: -26.20491, longitude: 28.04006, destinationhost: honeypotlab-vm, username: fabian.dosisto, sourcehost: 41.76.210.44, state: Gauteng, label: South Africa - 41.76.210.44, timestamp: 2024-05-11 18:49:11  
latitude: -12.05613, longitude: -77.02679, destinationhost: honeypotlab-vm, username: Fabiana, sourcehost: 181.65.169.150, state: Lima, label: Peru - 181.65.169.150, timestamp: 2024-05-11 18:54:13  
latitude: 16.82699, longitude: 96.13763, destinationhost: honeypotlab-vm, username: Fabiana, sourcehost: 202.191.103.118, state: Yangon Region, label: Myanmar - 202.191.103.118, timestamp: 2024-05-11 18:59:14  
latitude: 37.55632, longitude: -122.28809, destinationhost: honeypotlab-vm, username: Fabiane, sourcehost: 76.14.34.33, state: California, label: United States - 76.14.34.33, timestamp: 2024-05-11 19:03:49  
latitude: 33.41611, longitude: -112.00934, destinationhost: honeypotlab-vm, username: fabiganc, sourcehost: 107.178.105.70, state: Arizona, label: United States - 107.178.105.70, timestamp: 2024-05-11 19:09:12  
latitude: 61.19716, longitude: -149.87687, destinationhost: honeypotlab-vm, username: Fabrice, sourcehost: 206.174.50.207, state: Alaska, label: United States - 206.174.50.207, timestamp: 2024-05-11 19:14:19  
latitude: -25.51567, longitude: -54.57010, destinationhost: honeypotlab-vm, username: FABRICIA, sourcehost: 167.250.160.135, state: Parana, label: Brazil - 167.250.160.135, timestamp: 2024-05-11 19:19:19  
latitude: 31.45571, longitude: 73.08039, destinationhost: honeypotlab-vm, username: FABRYCIO\_YANEZ, sourcehost: 210.79.167.92, state: Punjab, label: Pakistan - 210.79.167.92, timestamp: 2024-05-11 19:24:00  
latitude: 8.95239, longitude: -79.53539, destinationhost: honeypotlab-vm, username: FAC, sourcehost: 190.219.13.26, state: Panama, label: Panama - 190.219.13.26, timestamp: 2024-05-11 19:28:51  
latitude: -26.20491, longitude: 28.04006, destinationhost: honeypotlab-vm, username: FACTHowe, sourcehost: 41.78.188.73, state: Gauteng, label: South Africa - 41.78.188.73, timestamp: 2024-05-11 19:33:54  
latitude: 19.00272, longitude: 72.82877, destinationhost: honeypotlab-vm, username: FACTSaidi, sourcehost: 116.73.21.72, state: Maharashtra, label: India - 116.73.21.72, timestamp: 2024-05-11 19:39:03  
latitude: 35.68877, longitude: 51.41503, destinationhost: honeypotlab-vm, username: FACTShack, sourcehost: 31.47.58.14, state: Tehran Province, label: Iran - 31.47.58.14, timestamp: 2024-05-11 19:43:46

## Commands X

Modules: All Refresh

Name:

A:

- Add-AppvClientConnectionGroup
- Add-AppvClientPackage
- Add-AppvPublishingServer
- Add-AppvPackage
- Add-AppvProvisionedPackage
- Add-AppvVolume
- Add-BCDataCacheExtension
- Add-BitLockerKeyProtector
- Add-BitsFile
- Add-CertificateEnrollmentPolicyServer
- Add-Computer
- Add-Content
- Add-DnsClientNrptRule
- Add-DtcClusterTMMMapping
- Add-EtwTraceProvider
- Add-History
- Add-InitiatorIdToMaskingSet
- Add-JobTrigger
- Add-KdsRootKey
- Add-LocalGroupMember
- Add-Member
- Add-MpPreference
- Add-NetEventNetworkAdapter
- Add-NetEventPacketCaptureProvider
- Add-NetEventProvider
- Add-NetEventVFPProvider
- Add-NetEventVmNetworkAdapter
- Add-NetEventVmSwitch
- Add-NetEventVmSwitchProvider
- Add-NetEventWFPProvider
- Add-NetIPHttpsCertBinding
- Add-NetLbfoTeamMember
- Add-NetLbfoTeamNic
- Add-NetNatExternalAddress
- Add-NetNatStaticMapping
- Add-NetSwitchTeamMember
- Add-ObdcDsn
- Add-PartitionAccessPath
- Add-PhysicalDisk
- Add-Printer
- Add-PrinterDriver
- Add-PrinterPort
- Add-PSNapin
- Add-SignerRule

Run Insert Copy

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

Ln 58 Col 1

90%

## Log Analytics Workspace query

Copy/paste this query when creating a workbook:

```
FAILED_RDP_WITH_GEO_CL
```

```
| extend username = extract(@"username:([^\,]+)", 1, RawData),  
          timestamp = extract(@"timestamp:([^\,]+)", 1, RawData),  
          latitude = extract(@"latitude:([^\,]+)", 1, RawData),  
          longitude = extract(@"longitude:([^\,]+)", 1, RawData),  
          sourcehost = extract(@"sourcehost:([^\,]+)", 1, RawData),  
          state = extract(@"state:([^\,]+)", 1, RawData),  
          label = extract(@"label:([^\,]+)", 1, RawData),  
          destination = extract(@"destinationhost:([^\,]+)", 1, RawData),  
          country = extract(@"country:([^\,]+)", 1, RawData)  
| where destination != "samplehost"  
| where sourcehost != ""  
| summarize event_count=count() by timestamp, label, country, state, sourcehost,  
username, destination, longitude, latitude
```

# Log Analytics work...

Default Directory

+ Create + Open recycle bin ...

Filter for any field...

Name ↑↓

law-honeypot1 ...

## law-honeypot1 | Logs

Log Analytics workspace

New Query 1\*

law-honeypot1

Select scope

Run

Time range : Last 24 hours

Save

Share

New alert rule

Export

Pin to

```
1 FAILED_RDP_WITH_GEO_CL
2 | extend
3 |   username = extract(@"username:([^\,]+)", 1, RawData),
4 |   timestamp = extract(@"timestamp:([^\,]+)", 1, RawData),
5 |   latitude = extract(@"latitude:([^\,]+)", 1, RawData),
6 |   longitude = extract(@"longitude:([^\,]+)", 1, RawData),
7 |   sourcehost = extract(@"sourcehost:([^\,]+)", 1, RawData),
8 |   state = extract(@"state:([^\,]+)", 1, RawData),
9 |   label = extract(@"label:([^\,]+)", 1, RawData),
10 |   destination = extract(@"destinationhost:([^\,]+)", 1, RawData),
11 |   country = extract(@"country:([^\,]+)", 1, RawData)
12 | where destination != "samplehost"
13 | summarize event_count=count() by timestamp, label, country, state, sourcehost, username, destination, longitude, latitude
```

Results

Chart

timestamp	label	country	state	sourcehost	username	destination	longitude	latitude
> 2024-05-11 18:59:14	Myanmar - 202.191.103.118	Myanmar	Yangon Region	202.191.103.118	Fabiana	honeypotlab-vm	96.13763	16.82699
> 2024-05-11 18:54:13	Peru - 181.65.169.150	Peru	Lima	181.65.169.150	Fabiana	honeypotlab-vm	-77.02679	-12.05613
> 2024-05-11 18:04:22	South Africa - 41.76.210.44	South Africa	Gauteng	41.76.210.44	eyzaw	honeypotlab-vm	28.04006	-26.20491
> 2024-05-11 17:59:37	China - 153.35.194.35	China	Jiangsu	153.35.194.35	Externo01	honeypotlab-vm	119.91518	32.48488
> 2024-05-11 18:09:37	Pakistan - 210.79.167.92	Pakistan	Punjab	210.79.167.92	f1admin	honeypotlab-vm	73.08039	31.45571
> 2024-05-11 18:11:27	United States - 173.52.108.235	United States	New York	173.52.108.235	pukemalaki	honeypotlab-vm	-74.00714	40.71455
> 2024-05-11 18:14:40	Brazil - 167.250.160.135	Brazil	Parana	167.250.160.135	F2MDBcj1	honeypotlab-vm	-54.57010	-25.51567
> 2024-05-11 18:20:09	Turkey - 185.141.33.162	Turkey	Istanbul	185.141.33.162	F3211552	honeypotlab-vm	28.82306	41.01525

0s 408ms

Display time (UTC+00:00)

Query details

1 - 8 of 11



## Microsoft Sentinel

Copy/paste this query when creating a new workbook:

FAILED\_RDP\_WITH\_GEO\_CL

```
| extend username = extract(@"username:([^\,]+)", 1, RawData),  
        timestamp = extract(@"timestamp:([^\,]+)", 1, RawData),  
        latitude = extract(@"latitude:([^\,]+)", 1, RawData),  
        longitude = extract(@"longitude:([^\,]+)", 1, RawData),  
        sourcehost = extract(@"sourcehost:([^\,]+)", 1, RawData),  
        state = extract(@"state:([^\,]+)", 1, RawData),  
        label = extract(@"label:([^\,]+)", 1, RawData),  
        destination = extract(@"destinationhost:([^\,]+)", 1, RawData),  
        country = extract(@"country:([^\,]+)", 1, RawData)  
| where destination != "samplehost"  
| where sourcehost != ""  
| summarize event_count=count() by timestamp, label, country, state, sourcehost,  
username, destination, longitude, latitude
```

# Failed RDP World Map

law-honeypot1

Done Editing Open Settings Code Refresh Alerts Link Code ? Help

1 Editing query item: query - 0

Settings

Advanced Settings

Style

Advanced Editor

Query (change)

Time Range

Visualization

Size

Map Settings

Run Query

Samples

law-honeypot1

Last 24 hours

Map

Large

Log Analytics workspace Logs Query

Query help

FAILED\_RDP\_WITH\_GEO\_CL

extend

username = extract(@"username:([^\,]+)", 1, RawData),

timestamp = extract(@"timestamp:([^\,]+)", 1, RawData),

latitude = extract(@"latitude:([^\,]+)", 1, RawData),

longitude = extract(@"longitude:([^\,]+)", 1, RawData),

sourcehost = extract(@"sourcehost:([^\,]+)", 1, RawData),

state = extract(@"state:([^\,]+)", 1, RawData),

label = extract(@"label:([^\,]+)", 1, RawData),


destination = extract(@"destinationhost:([^\,]+)", 1, RawData),

country = extract(@"country:([^\,]+)", 1, RawData)

where destination != "samplehost"

where sourcehost != ""

summarize event\_count=count() by timestamp, label, country, state, sourcehost, username, destination, longitude, latitude





## Map Settings



### Layout Settings

Location Info using ⓘ

Latitude/Longitude ▾

Latitude \* ⓘ

latitude ▾

Longitude \* ⓘ

longitude ▾

Size by ⓘ

event\_count ▾

Aggregation for location ⓘ

Sum of values ▾

Minimum region size ⓘ

20

Maximum region size ⓘ

70

Default region size ⓘ

10

Minimum value ⓘ

(auto) ✓

Maximum value ⓘ

(auto) ✓

Opacity of items on Map ⓘ

0.7

### Color Settings

Coloring Type ⓘ

None Thresholds **Heatmap**



## Map Settings



Opacity of items on Map ⓘ

0.7

### Color Settings

Coloring Type ⓘ

None Thresholds **Heatmap**

Color by ⓘ

event\_count ▾

Aggregation for color ⓘ

Sum of values ▾

Color palette

Green to Red ▾

Minimum value ⓘ

(auto) ✓

Maximum value ⓘ

(auto) ✓

### Metric Settings

Metric Label ⓘ

label ▾

Metric Value ⓘ

event\_count ▾

Create 'Others' group after ⓘ

10

Aggregate 'Others' metrics by ⓘ

Sum of values ▾

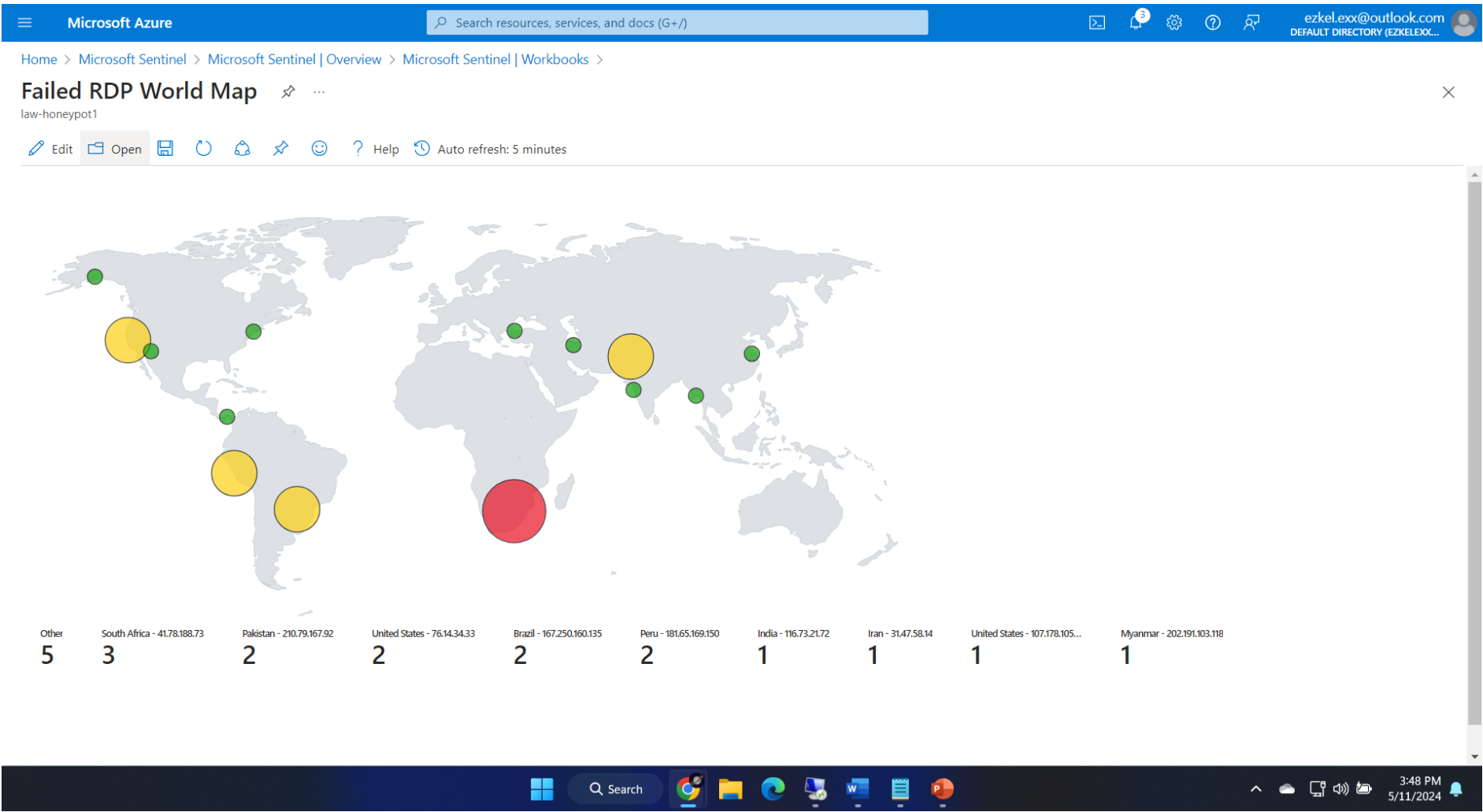
☐ Custom formatting ⓘ

**Apply**

Save and Close

Cancel

# Result as of 3:48 PM 5/11/2024



```
PS C:\Users\zekeadmin> C:\Users\zekeadmin\Desktop\Log_Exporter.ps1
# The term 'e' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At C:\Users\zekeadmin\Desktop\Log_Exporter.ps1:1 char:1
+ # Get API key from here: https://ipgeolocation.io/
+ ~
+ CategoryInfo          : ObjectNotFound: (#:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

Directory: C:\ProgramData

```

Mode                               LastWriteTime                      Length Name
----
-a----- 5/11/2024 6:09 PM                      0 failed_rdp.log
latitude:-26.20491,longitude:28.04006,destinationhost:honeyptlab-vm,username:eyzaw,sourcechost:41.76.210.44,state:Gauteng
,label:South Africa - 41.76.210.44,timestamp:2024-05-11 18:04:22
latitude:32.48488,longitude:119.91518,destinationhost:honeyptlab-vm,username:Extern001,sourcechost:153.35.194.35,state:Ji
angsu,label:China - 153.35.194.35,timestamp:2024-05-11 17:59:37
latitude:31.45571,longitude:73.08039,destinationhost:honeyptlab-vm,username:fiadmin,sourcechost:210.79.167.92,state:Punja
b,label:Pakistan - 210.79.167.92,timestamp:2024-05-11 18:09:37
latitude:40.74455,longitude:74.00714,destinationhost:honeyptlab-vm,username:pukemalaki,sourcechost:173.52.108.235,state:New York,label
:United States - 173.52.108.235,timestamp:2024-05-11 18:11:27
latitude:-25.51567,longitude:-54.57010,destinationhost:honeyptlab-vm,username:F2MD8Cj1,sourcechost:167.250.160.135,state:Parana,label:B
razil - 167.250.160.135,timestamp:2024-05-11 18:14:40
latitude:41.01525,longitude:28.82306,destinationhost:honeyptlab-vm,username:F3211552,sourcechost:185.141.33.162,state:Istanbul,label:Tu
rkey - 185.141.33.162,timestamp:2024-05-11 18:20:09
latitude:-12.05613,longitude:-77.02679,destinationhost:honeyptlab-vm,username:F311,sourcechost:181.65.169.150,state:Lima,label:Peru - 1
81.65.169.150,timestamp:2024-05-11 18:24:30
latitude:37.55632,longitude:-122.28809,destinationhost:honeyptlab-vm,username:F792gJwH,sourcechost:76.14.34.33,state:California,label:U
nited States - 76.14.34.33,timestamp:2024-05-11 18:34:13
latitude:-26.20491,longitude:28.04006,destinationhost:honeyptlab-vm,username:Fabian.dosisto,sourcechost:41.76.210.44,state:Gauteng,label
:South Africa - 41.76.210.44,timestamp:2024-05-11 18:49:11
latitude:-12.05613,longitude:-77.02679,destinationhost:honeyptlab-vm,username:Fabiiana,sourcechost:181.65.169.150,state:Lima,label:Peru
- 181.65.169.150,timestamp:2024-05-11 18:54:13
latitude:16.82699,longitude:96.13763,destinationhost:honeyptlab-vm,username:Fabi ana,sourcechost:202.191.103.118,state:Yangon Region,label
:Myanmar - 202.191.103.118,timestamp:2024-05-11 18:59:14
latitude:37.55632,longitude:-122.28809,destinationhost:honeyptlab-vm,username:Fabi ane,sourcechost:76.14.34.33,state:California,label:Un
ited States - 76.14.34.33,timestamp:2024-05-11 19:03:49
latitude:33.45612,longitude:-111.08934,destinationhost:honeyptlab-vm,username:fabigana,sourcechost:107.178.105.70,state:Arizona,label:U
nited States - 107.178.105.70,timestamp:2024-05-11 19:09:12
latitude:61.19716,longitude:-149.87687,destinationhost:honeyptlab-vm,username:FabrIce,sourcechost:206.174.50.207,state:Alaska,label:Uni
ted States - 206.174.50.207,timestamp:2024-05-11 19:14:19
latitude:-25.51567,longitude:-54.57010,destinationhost:honeyptlab-vm,username:FABRICIA,sourcechost:167.250.160.135,state:Parana,label:B
razil - 167.250.160.135,timestamp:2024-05-11 19:19:19
latitude:31.45571,longitude:73.08039,destinationhost:honeyptlab-vm,username:FABRYCYO_YANEZ,sourcechost:210.79.167.92,state:Punjab,label
:Pakistan - 210.79.167.92,timestamp:2024-05-11 19:24:00
latitude:8.95239,longitude:-79.53539,destinationhost:honeyptlab-vm,username:FAC,sourcechost:190.219.13.26,state:Panama,label:Panama -
190.219.13.26,timestamp:2024-05-11 19:28:51
latitude:-26.20491,longitude:28.04006,destinationhost:honeyptlab-vm,username:FACTHowe,sourcechost:41.78.188.73,state:Gauteng,label:Sout
h Africa - 41.78.188.73,timestamp:2024-05-11 19:33:54
latitude:19.00272,longitude:72.82877,destinationhost:honeyptlab-vm,username:FACTSaïdi,sourcechost:116.73.21.72,state:Maharashtra,label:
India - 116.73.21.72,timestamp:2024-05-11 19:39:03
latitude:35.68877,longitude:51.41503,destinationhost:honeyptlab-vm,username:FACTShack,sourcechost:31.47.58.14,state:Tehran Province,label
:Iran - 31.47.58.14,timestamp:2024-05-11 19:43:46
latitude:-26.20491,longitude:28.04006,destinationhost:honeyptlab-vm,username:FACTRACI0N1,sourcechost:41.76.210.44,state:Gauteng,label:South Africa - 41.
76.210.44,timestamp:2024-05-11 19:48:26
latitude:32.48488,longitude:119.91518,destinationhost:honeyptlab-vm,username:Facturaci0n,sourcechost:153.35.194.35,state:Jiangsu,label:China - 153.35.194
.35,timestamp:2024-05-11 19:53:46
latitude:-26.20491,longitude:28.04006,destinationhost:honeyptlab-vm,username:faithrelations,sourcechost:41.78.188.73,state:Gauteng,label:South Africa - 4
1.78.188.73,timestamp:2024-05-11 20:03:40

```

Script 

Commands ✕

Modules:

Refresh

Name:

A:

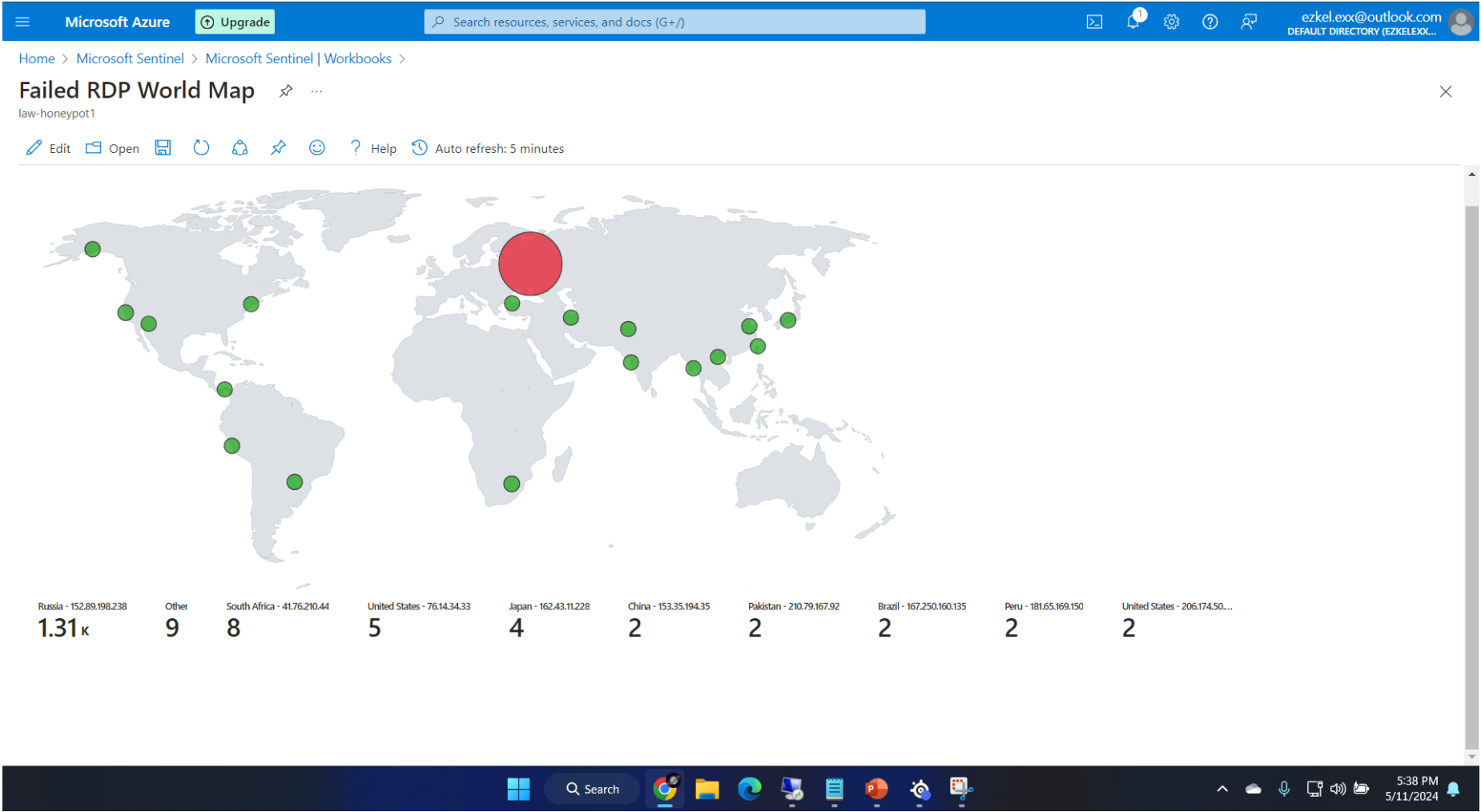
Add-AppClientConnectionGroup  
Add-AppClientPackage  
Add-AppPublishingServer  
Add-AppPackage  
Add-AppxProvisionedPackage  
Add-AppxVolume  
Add-BCDataCacheExtension  
Add-BitLockerKeyProtector  
Add-BitsFile  
Add-CertificateEnrollmentPolicyServer  
Add-Computer  
Add-Content  
Add-OnsClientNprrp  
Add-DtcClusterTMMapping  
Add-EtwTraceProvider  
Add-History  
Add-InitiatorIdToMaskingSet  
Add-JobTrigger  
Add-KdsRootKey  
Add-LocalGroupMember  
Add-Member  
Add-MpPreference  
Add-NetEventNetworkAdapter  
Add-NetEventPacketCaptureProvider  
Add-NetEventProvider  
Add-NetEventVFPProvider  
Add-NetEventVmNetworkAdapter  
Add-NetEventVmSwitch  
Add-NetEventVmSwitchProvider  
Add-NetEventWFPProvider  
Add-NetEventWFPProvider  
Add-NetHttpCertBinding  
Add-NetLbfoTeamMember  
Add-NetLbfoTeamNic  
Add-NetNatExternalAddress  
Add-NetNatStaticMapping  
Add-NetSwitchTeamMember  
Add-OdbcDsn  
Add-PartitionAccessPath  
Add-PhysicalDisk  
Add-Printer  
Add-PrinterDriver  
Add-PrinterPort  
Add-PSSnapin  
Add-SlignerRule

Run Insert Copy

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

Ln 64 Col 1  90%

# Result as of 5:38 PM 5/11/2024



Source: <https://www.youtube.com/watch?v=RoZeVbbZ0o0>