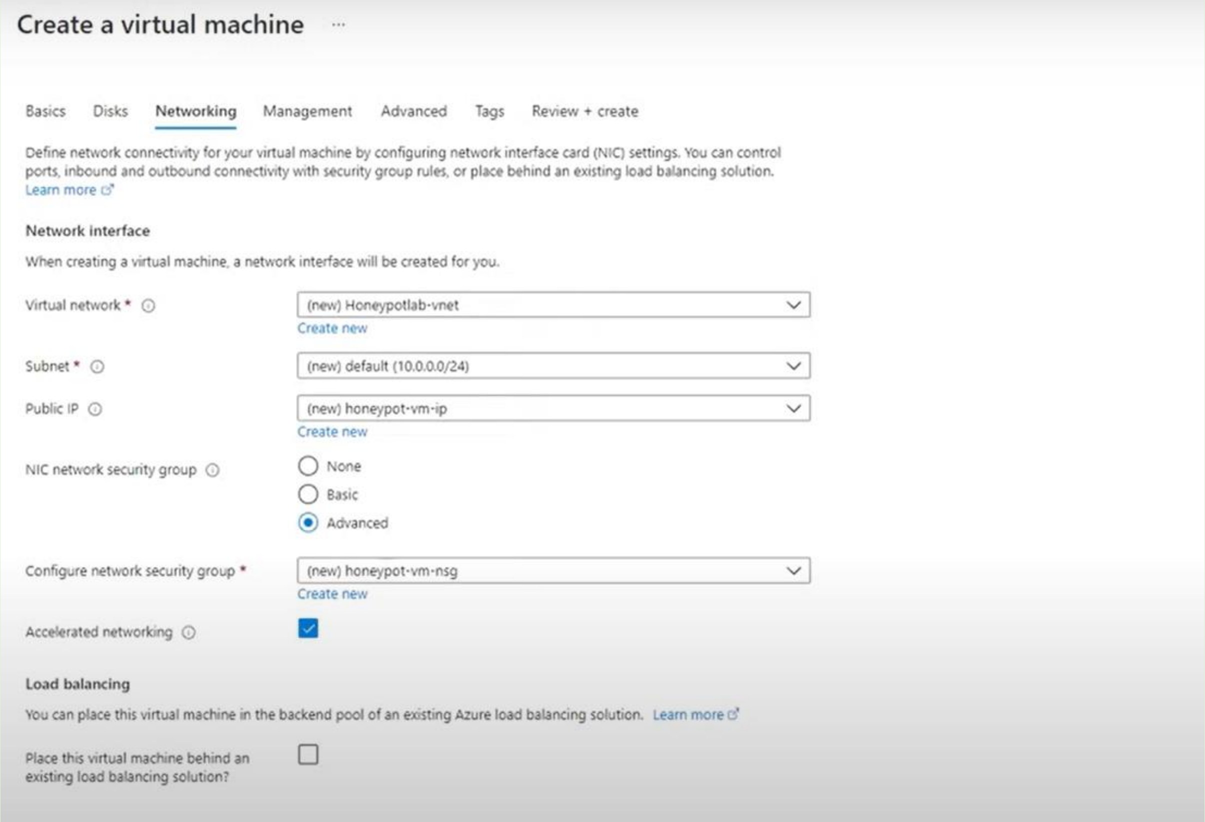
SIEM Basics with Azure Sentinel: Hands-On with Live Cyber Attacks

Create Virtual Machine



Create a virtual machine ···

Basics | Disks | **Networking** | Management | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : (new) Honeypotlab-vnet
Create new

Subnet * : (new) default (10.0.0.0/24)

Public IP : (new) honeypot-vm-ip
Create new

NIC network security group:
○ None
○ Basic
● Advanced

Configure network security group * : (new) honeypot-vm-nsg
Create new

Accelerated networking: ☑

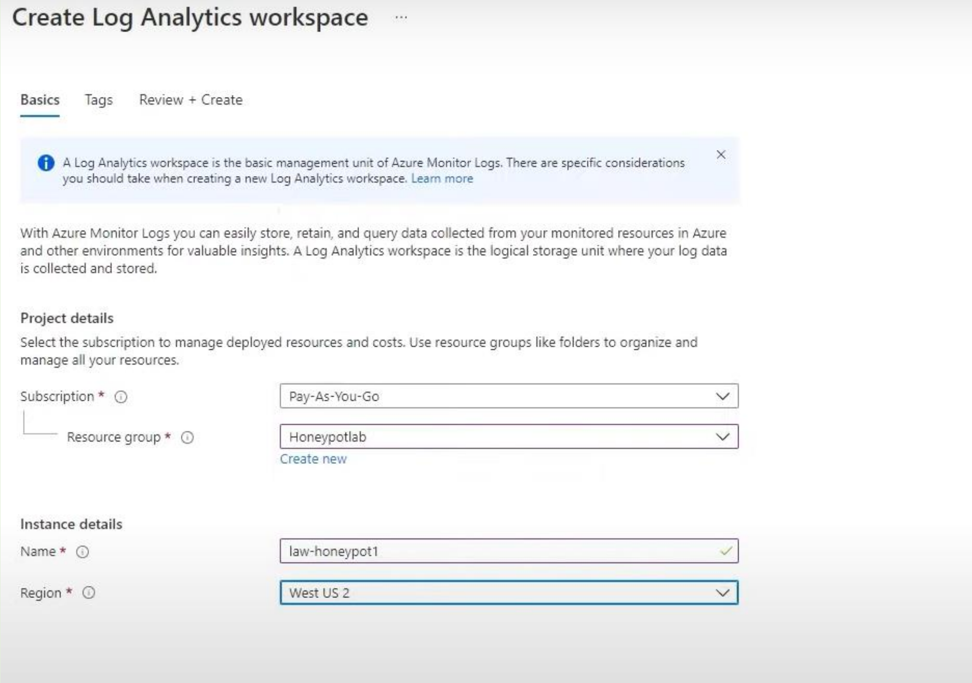
Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? □

Allow all in Firewall

Create Log Analytics Workspace



Create Log Analytics workspace ···

Basics | Tags | Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Pay-As-You-Go

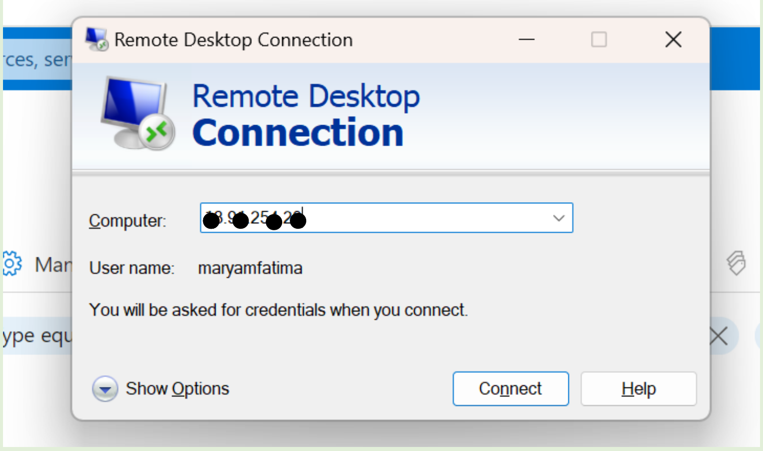
Resource group * : Honeypotlab
Create new

Instance details

Name * : law-honeypot1

Region * : West US 2

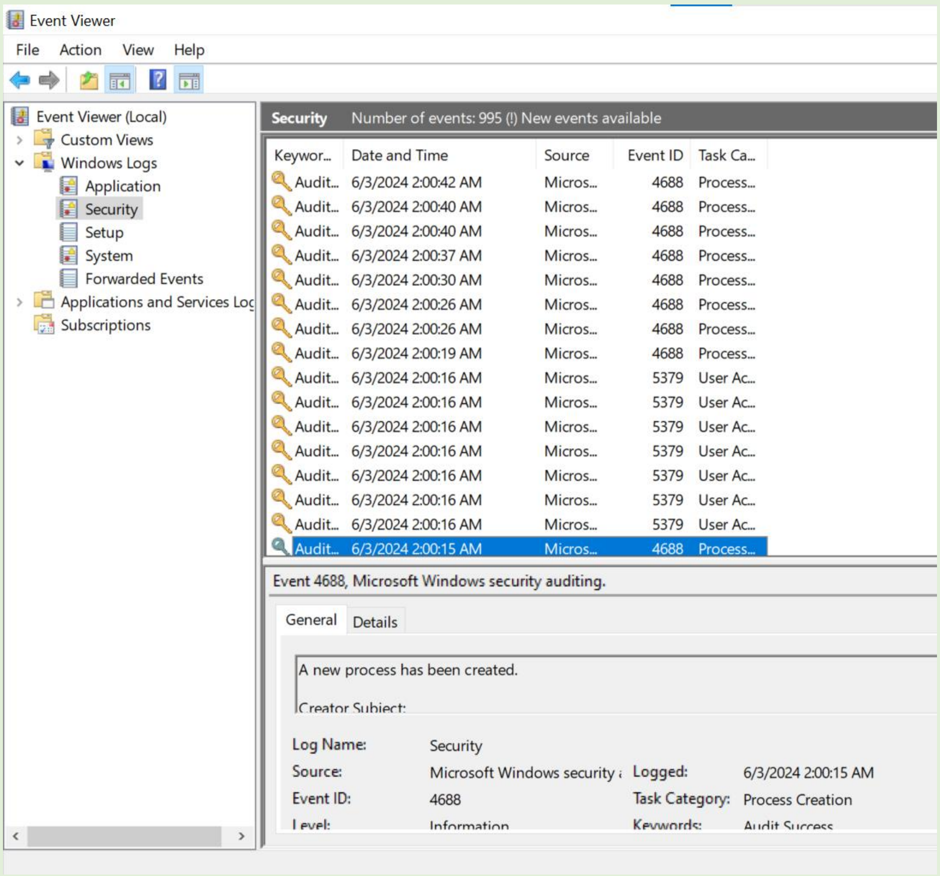
Connect Log Analytics to VM



Computer: [redacted]

User name: maryamfatima

You will be asked for credentials when you connect.



Security Number of events: 995 (!) New events available

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	6/3/2024 2:00:42 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:40 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:40 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:37 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:30 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:26 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:26 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:19 AM	Micros...	4688	Process...
Audit...	6/3/2024 2:00:16 AM	Micros...	5379	User Ac...
Audit...	6/3/2024 2:00:16 AM	Micros...	5379	User Ac...
Audit...	6/3/2024 2:00:16 AM	Micros...	5379	User Ac...
Audit...	6/3/2024 2:00:16 AM	Micros...	5379	User Ac...
Audit...	6/3/2024 2:00:16 AM	Micros...	5379	User Ac...
Audit...	6/3/2024 2:00:16 AM	Micros...	5379	User Ac...
Audit...	6/3/2024 2:00:16 AM	Micros...	5379	User Ac...
Audit...	6/3/2024 2:00:15 AM	Micros...	4688	Process...

Event 4688, Microsoft Windows security auditing.

General Details

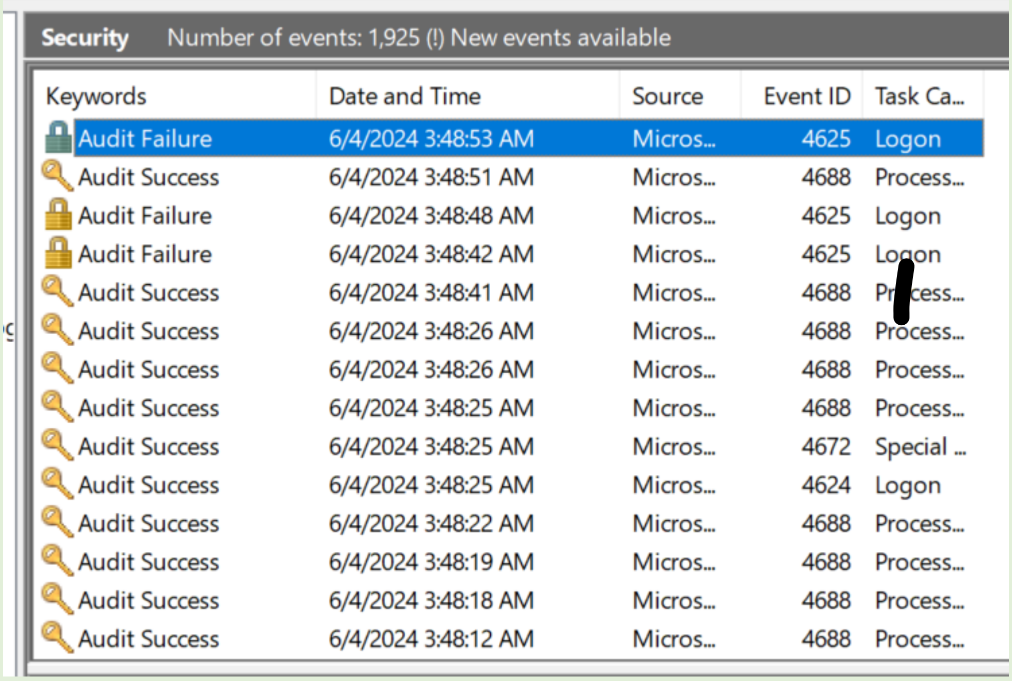
A new process has been created.

Creator Subject:

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	6/3/2024 2:00:15 AM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success

Trying to log in using wrong credentials for testing purpose

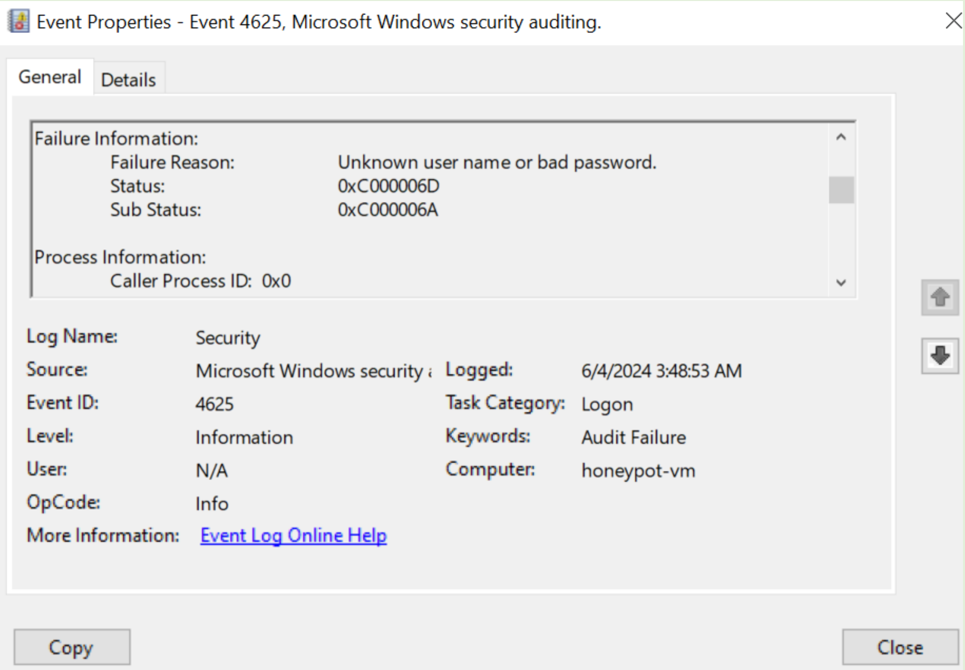
Event ID:4625 Indicating Audit failure in the security log events



Security   Number of events: 1,925 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Ca...
Audit Failure	6/4/2024 3:48:53 AM	Micros...	4625	Logon
Audit Success	6/4/2024 3:48:51 AM	Micros...	4688	Process...
Audit Failure	6/4/2024 3:48:48 AM	Micros...	4625	Logon
Audit Failure	6/4/2024 3:48:42 AM	Micros...	4625	Logon
Audit Success	6/4/2024 3:48:41 AM	Micros...	4688	Process...
Audit Success	6/4/2024 3:48:26 AM	Micros...	4688	Process...
Audit Success	6/4/2024 3:48:26 AM	Micros...	4688	Process...
Audit Success	6/4/2024 3:48:25 AM	Micros...	4688	Process...
Audit Success	6/4/2024 3:48:25 AM	Micros...	4672	Special ...
Audit Success	6/4/2024 3:48:25 AM	Micros...	4624	Logon
Audit Success	6/4/2024 3:48:22 AM	Micros...	4688	Process...
Audit Success	6/4/2024 3:48:19 AM	Micros...	4688	Process...
Audit Success	6/4/2024 3:48:18 AM	Micros...	4688	Process...
Audit Success	6/4/2024 3:48:12 AM	Micros...	4688	Process...

Detailed view of the log event 4625

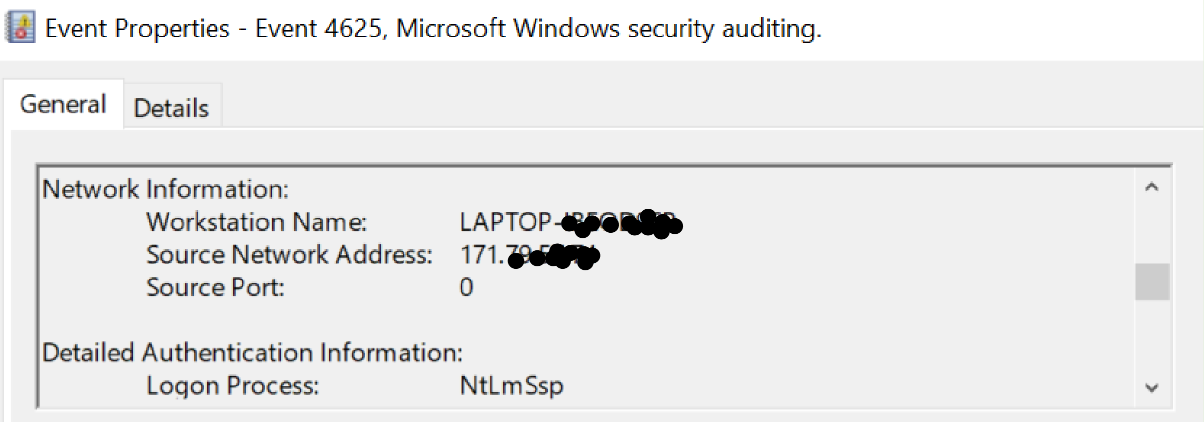


Event Properties - Event 4625, Microsoft Windows security auditing.

```
Failure Information:
        Failure Reason:        Unknown user name or bad password.
        Status:                0xC000006D
        Sub Status:            0xC000006A

Process Information:
        Caller Process ID:  0x0
```

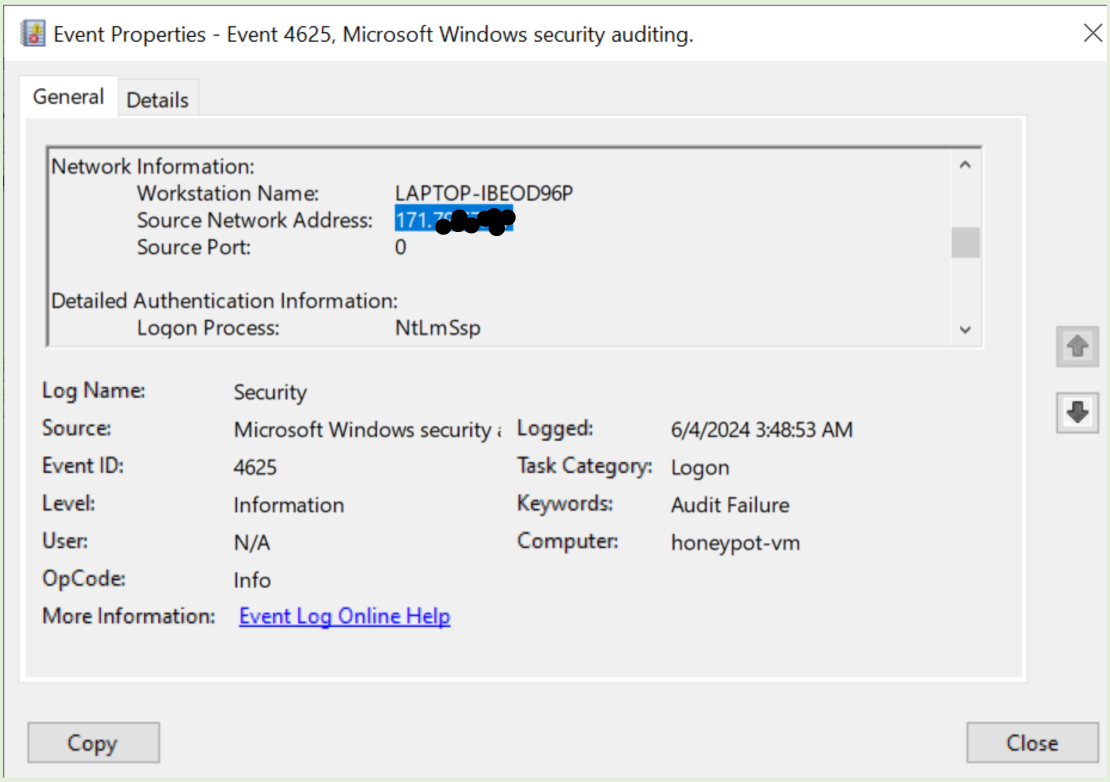
Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	6/4/2024 3:48:53 AM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	honeypot-vm
OpCode:	Info		
More Information:	Event Log Online Help		



Event Properties - Event 4625, Microsoft Windows security auditing.

```
Network Information:
        Workstation Name:        LAPTOP-[redacted]
        Source Network Address:  171.[redacted]
        Source Port:             0

Detailed Authentication Information:
        Logon Process:           NtLmSsp
```

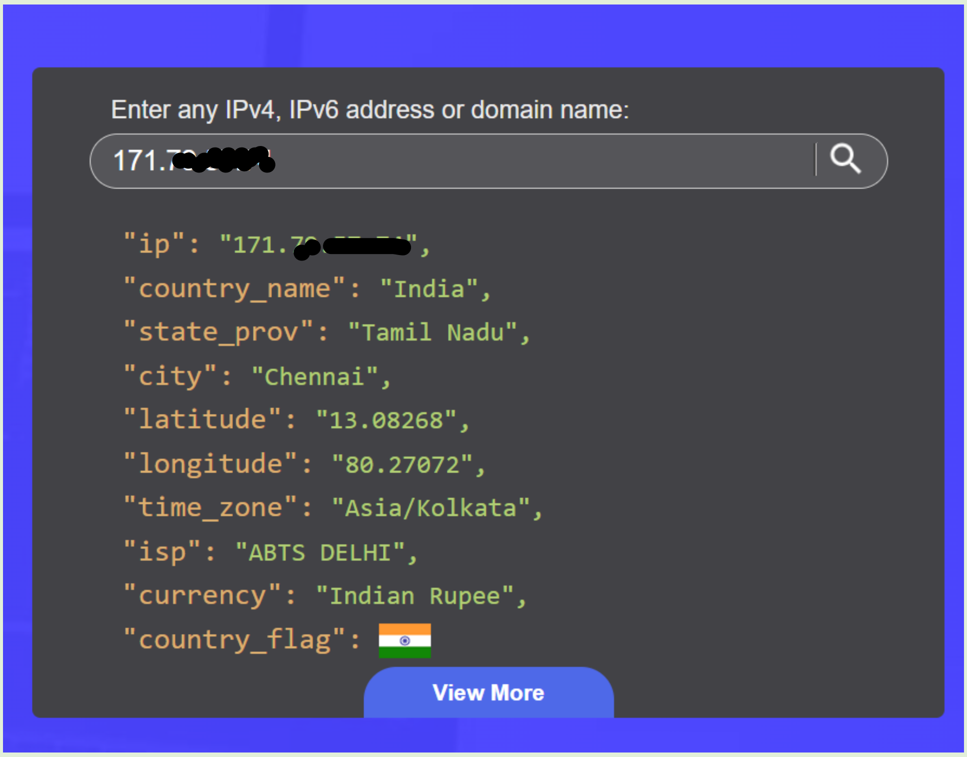

Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
Copy
Close

```
Network Information:
        Workstation Name:        LAPTOP-IBEOD96P
        Source Network Address:  171.7[redacted]
        Source Port:             0

Detailed Authentication Information:
        Logon Process:           NtLmSsp
```

```
Log Name:          Security
Source:            Microsoft Windows security a   Logged:          6/4/2024 3:48:53 AM
Event ID:          4625                           Task Category:   Logon
Level:             Information                    Keywords:        Audit Failure
User:              N/A                            Computer:        honeypot-vm
OpCode:            Info
More Information:  Event Log Online Help
```

Using the Ip address of the device logged in to find more insights using 'IP GEO LOACTION API'

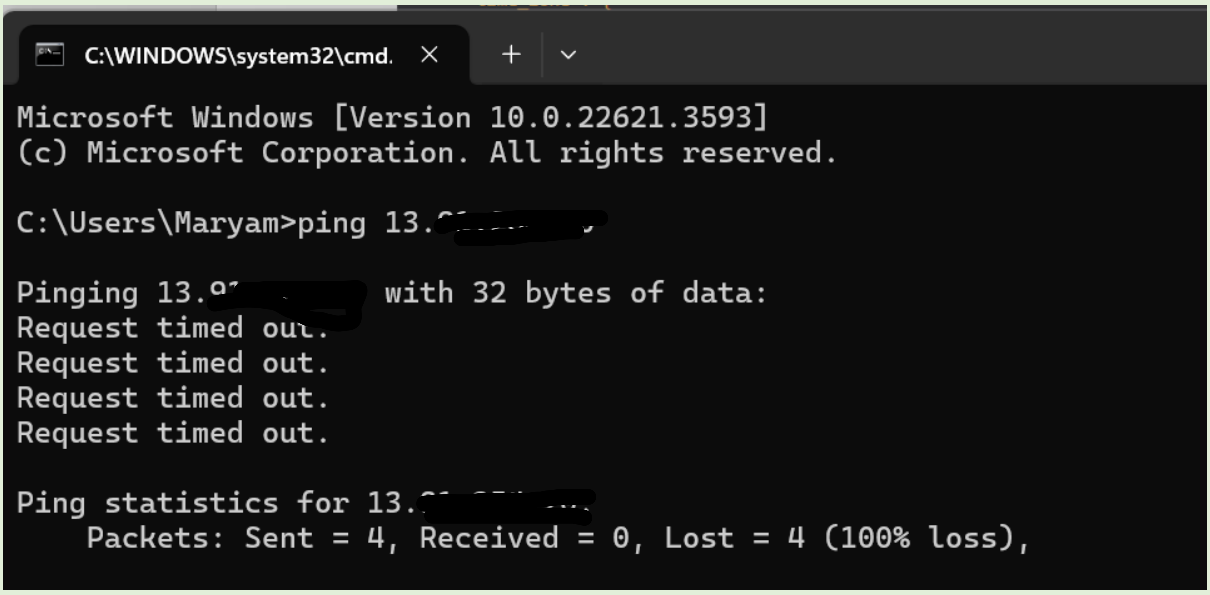


```
"ip": "171.7[redacted]",
"country_name": "India",
"state_prov": "Tamil Nadu",
"city": "Chennai",
"latitude": "13.08268",
"longitude": "80.27072",
"time_zone": "Asia/Kolkata",
"isp": "ABTS DELHI",
"currency": "Indian Rupee",
"country_flag":
```

More details on the ip address found that's been trying to intrude inside

TURN OFF THE WIREWALL:

Command prompt showing timed out since the firewalls are switched on still



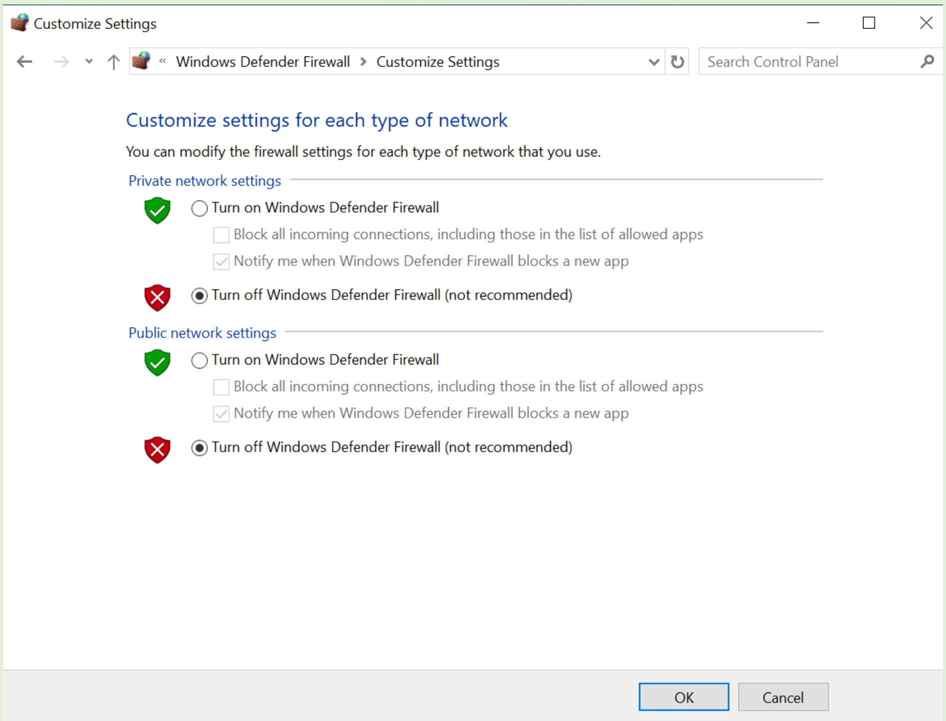
```
Microsoft Windows [Version 10.0.22621.3593]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Maryam>ping 13.[redacted]

Pinging 13.[redacted] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.[redacted]
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Switching off the firewalls



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

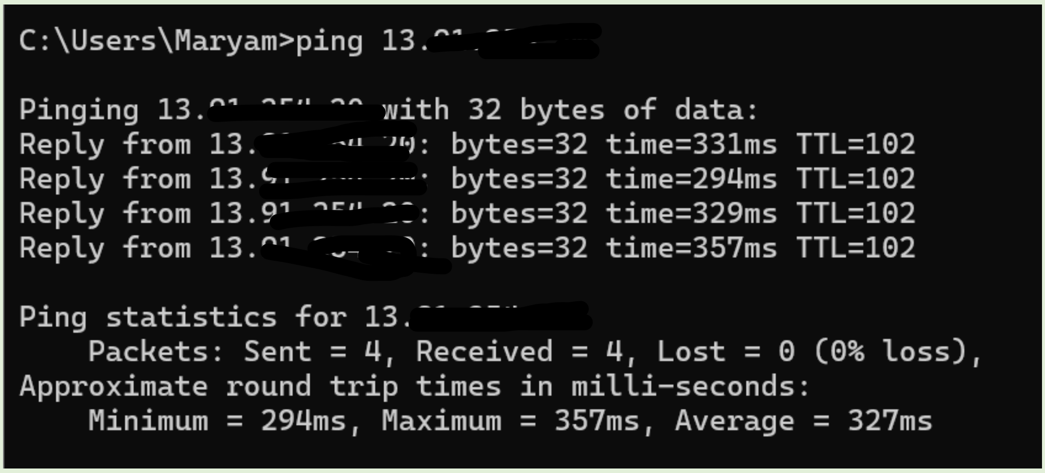
□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

OK Cancel

Responding to the ping command since the firewalls public and prvt settings are turned off

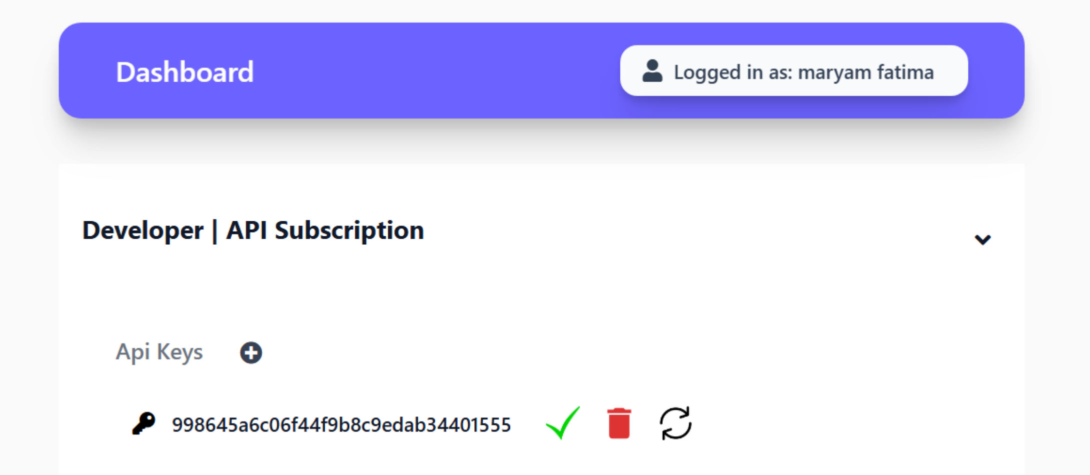


```
C:\Users\Maryam>ping 13.[redacted]

Pinging 13.[redacted] with 32 bytes of data:
Reply from 13.[redacted]: bytes=32 time=331ms TTL=102
Reply from 13.[redacted]: bytes=32 time=294ms TTL=102
Reply from 13.[redacted]: bytes=32 time=329ms TTL=102
Reply from 13.[redacted]: bytes=32 time=357ms TTL=102

Ping statistics for 13.[redacted]
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 294ms, Maximum = 357ms, Average = 327ms
```

CONNECTING THE GEOIP API WITH SHELL SCRIPT IN THE VM:



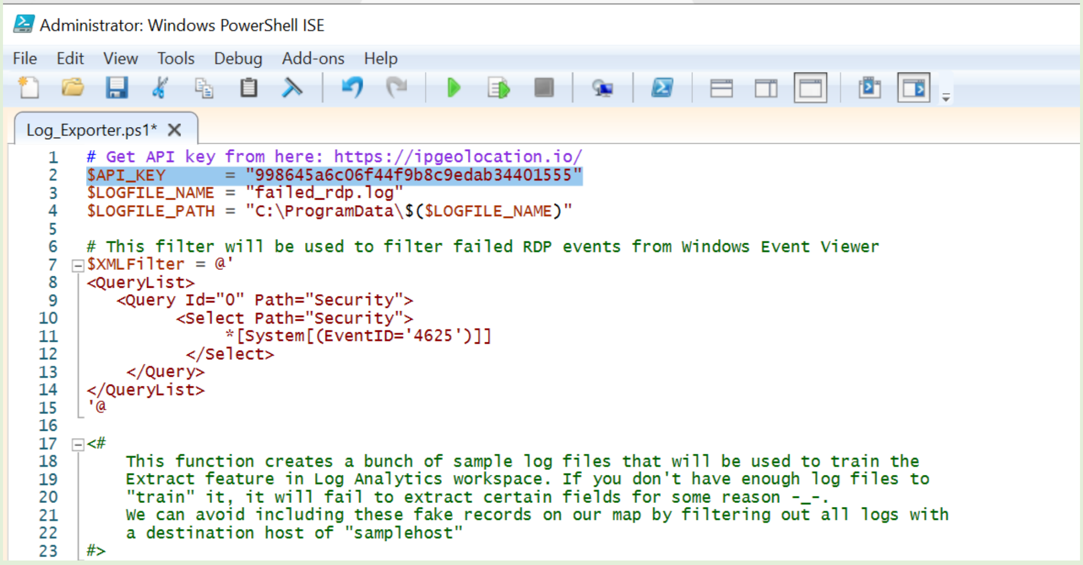
Dashboard

Logged in as: maryam fatima

Developer | API Subscription

Api Keys

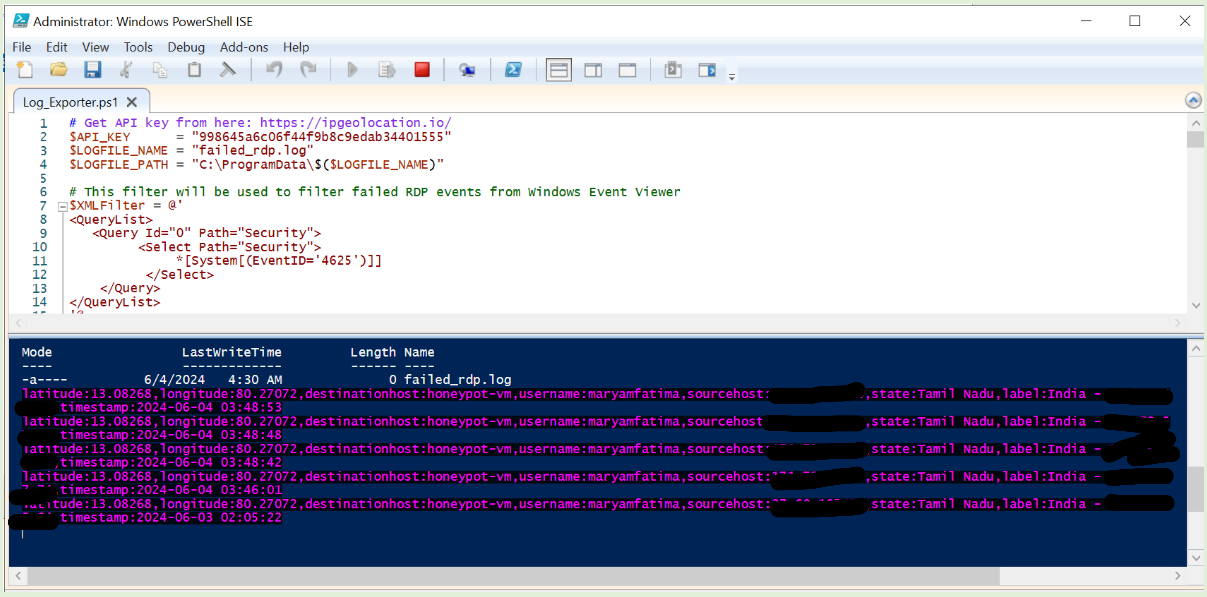
998645a6c06f44f9b8c9edab34401555



```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "998645a6c06f44f9b8c9edab34401555"
$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"
#>
```


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Log_Exporter.ps1

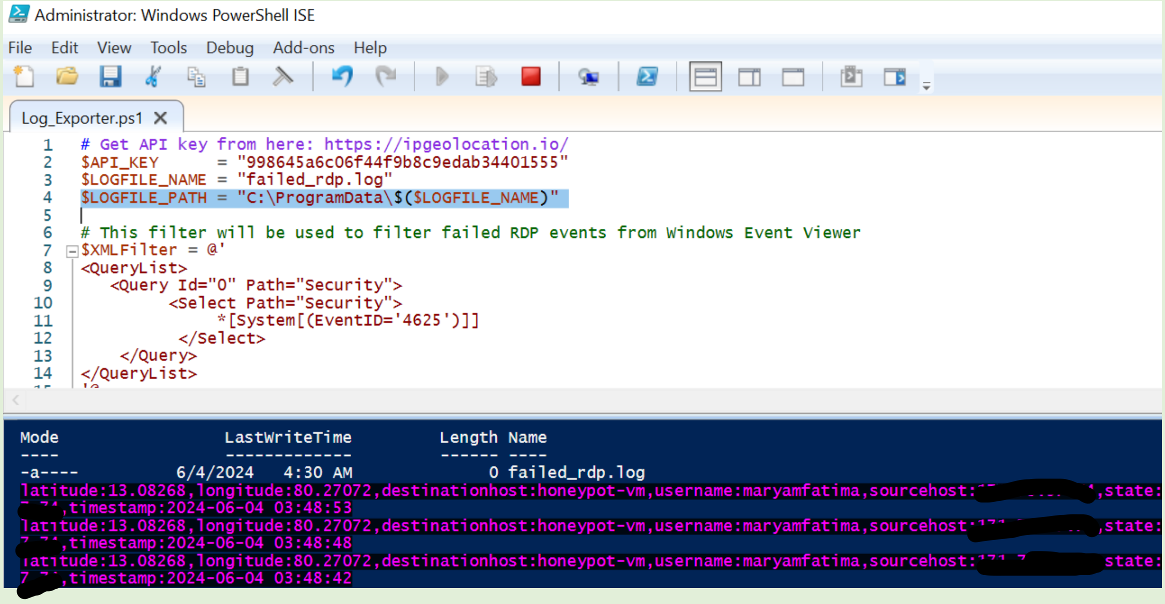
```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "998645a6c06f44f9b8c9edab34401555"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# 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>
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          6/4/2024   4:30 AM              0 failed_rdp.log
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost:[redacted],state:Tamil Nadu,label:India - [redacted]
[redacted] timestamp:2024-06-04 03:48:53
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],state:Tamil Nadu,label:India - [redacted]
[redacted] timestamp:2024-06-04 03:48:48
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted]state:Tamil Nadu,label:India - [redacted]
[redacted],timestamp:2024-06-04 03:48:42
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost:[redacted],state:Tamil Nadu,label:India - [redacted]
[redacted],timestamp:2024-06-04 03:46:01
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost:[redacted]state:Tamil Nadu,label:India - [redacted]
[redacted] timestamp:2024-06-03 02:05:22
```

Running the shellscript after changing the API

Seeing the logs through failed RDP

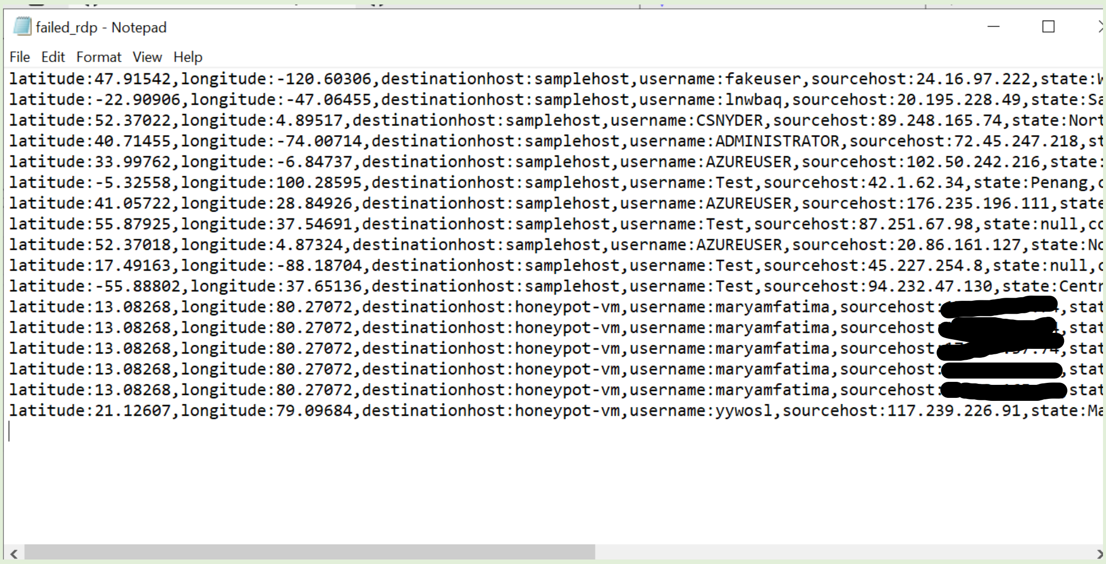

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Log_Exporter.ps1

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "998645a6c06f44f9b8c9edab34401555"
$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>
```

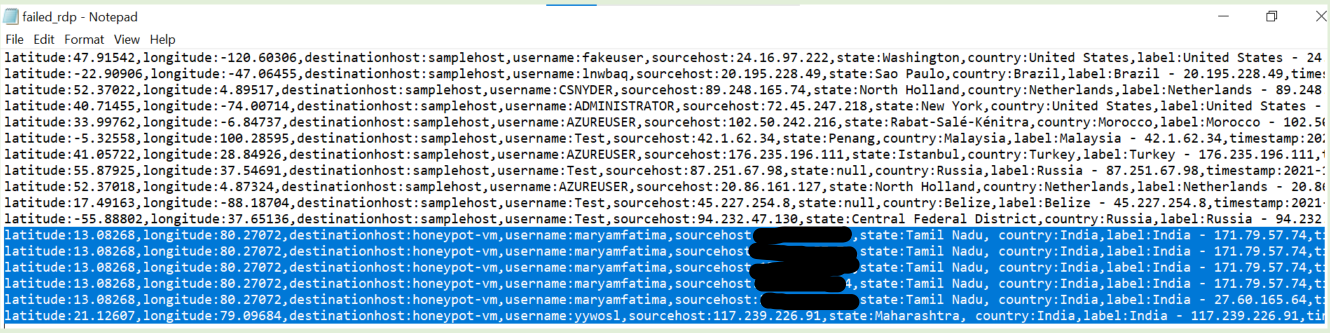
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          6/4/2024   4:30 AM              0 failed_rdp.log
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost:[redacted],state:
[redacted],timestamp:2024-06-04 03:48:53
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],state:
[redacted],timestamp:2024-06-04 03:48:48
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost:[redacted]state:
[redacted],timestamp:2024-06-04 03:48:42
```

Noting down the loaction.



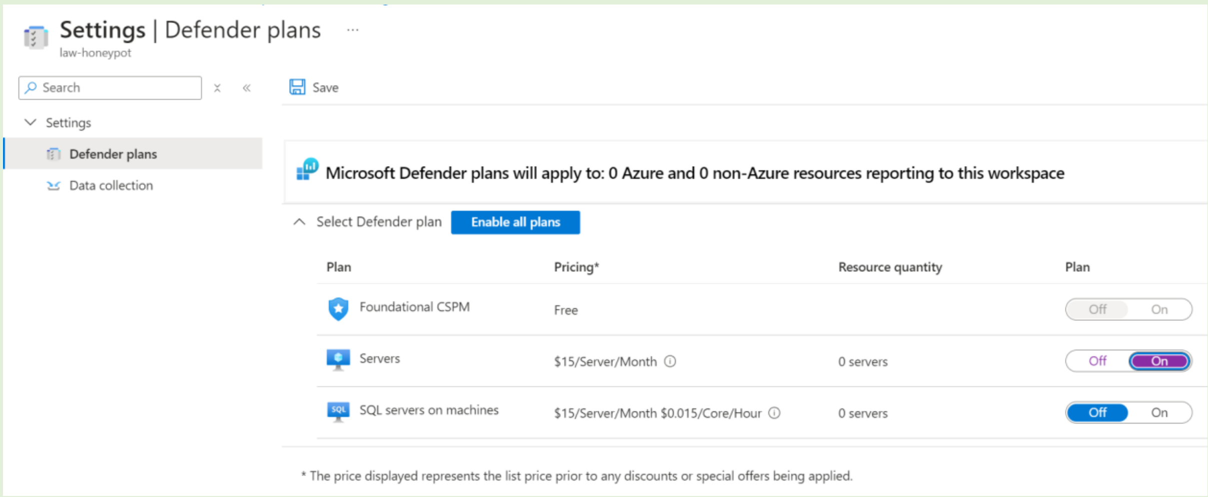
```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:W
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sa
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:Nort
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,st
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,c
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,c
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:N
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,c
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Centr
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],stat
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],stat
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],stat
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],stat
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],stat
latitude:21.12607,longitude:79.09684,destinationhost:honeypot-vm,username:yywosl,sourcehost:117.239.226.91,state:Ma
```

Logs in failed_rdp



```
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24
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,time
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlands - 89.248
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States -
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country:Morocco,label:Morocco - 102.5
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:20
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,
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-
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Netherlands,label:Netherlands - 20.8
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
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
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted],state:Tamil Nadu, country:India,label:India - 171.79.57.74,t
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted]state:Tamil Nadu, country:India,label:India - 171.79.57.74,t
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted]state:Tamil Nadu, country:India,label:India - 171.79.57.74,t
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost[redacted]4,state:Tamil Nadu, country:India,label:India - 171.79.57.74,t
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:maryamfatima,sourcehost:[redacted]state:Tamil Nadu, country:India,label:India - 27.60.165.64,t
latitude:21.12607,longitude:79.09684,destinationhost:honeypot-vm,username:yywosl,sourcehost:117.239.226.91,state:Maharashtra, country:India,label:India - 117.239.226.91,ti
```

Exact logs being recorded

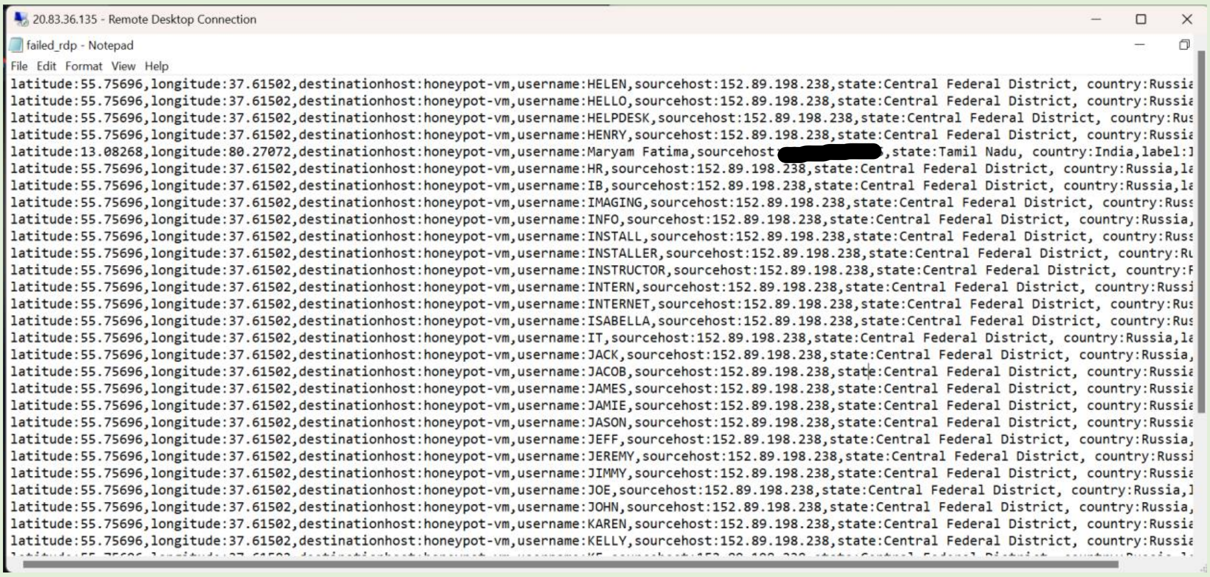


Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace

Plan	Pricing*	Resource quantity	Plan
Foundational CSPM	Free		Off On
Servers	$15/Server/Month ⓘ	0 servers	Off [✓ On]
SQL servers on machines	$15/Server/Month $0.015/Core/Hour ⓘ	0 servers	[✓ Off] On

* The price displayed represents the list price prior to any discounts or special offers being applied.

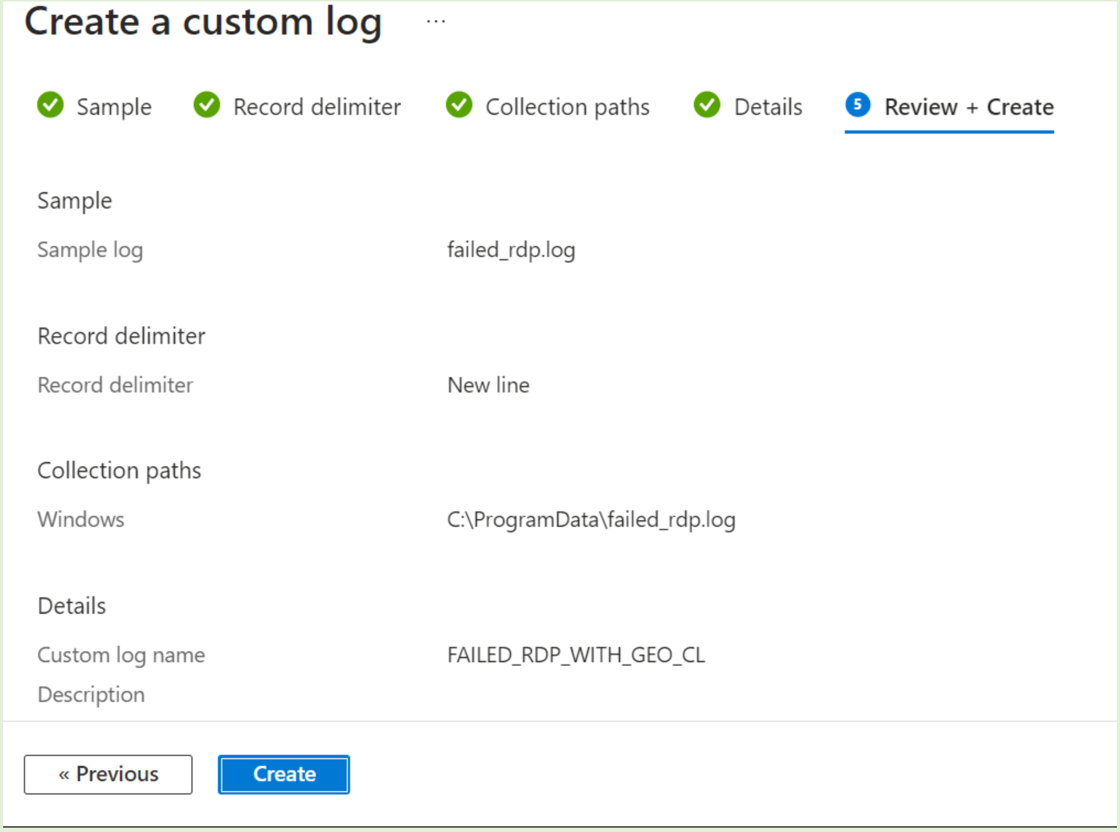
Collecting the logs in failed_rdp after connecting to the API:



20.83.36.135 - Remote Desktop Connection
failed_rdp - Notepad
File Edit Format View Help

```
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:HELEN,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:HELLO,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:HELPDESK,sourcehost:152.89.198.238,state:Central Federal District, country:Rus
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:HENRY,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:13.08268,longitude:80.27072,destinationhost:honeypot-vm,username:Maryam Fatima,sourcehost[redacted],state:Tamil Nadu, country:India,label:I
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:HR,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,la
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:IB,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,la
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:IMAGING,sourcehost:152.89.198.238,state:Central Federal District, country:Russ
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:INFO,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:INSTALL,sourcehost:152.89.198.238,state:Central Federal District, country:Russ
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:INSTALLER,sourcehost:152.89.198.238,state:Central Federal District, country:Ru
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:INSTRUCTOR,sourcehost:152.89.198.238,state:Central Federal District, country:R
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:INTERN,sourcehost:152.89.198.238,state:Central Federal District, country:Russi
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:INTERNET,sourcehost:152.89.198.238,state:Central Federal District, country:Rus
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:ISABELLA,sourcehost:152.89.198.238,state:Central Federal District, country:Rus
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:IT,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,la
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JACK,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JACOB,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JAMES,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JAMIE,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JASON,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JEFF,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JEREMY,sourcehost:152.89.198.238,state:Central Federal District, country:Russi
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JIMMY,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JOE,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,l
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:JOHN,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:KAREN,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:KELLY,sourcehost:152.89.198.238,state:Central Federal District, country:Russia
latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:KE,sourcehost:152.89.198.238,state:Central Federal District, country:Russia,la
```

Conncting the custom log in Azure



Create a custom log ···

Sample

Sample log	failed_rdp.log

Record delimiter

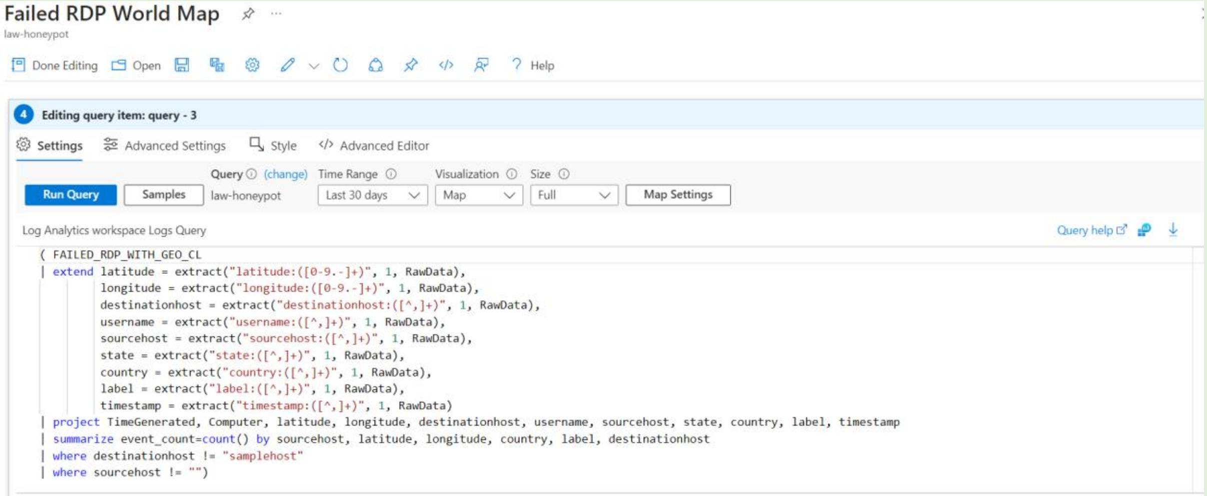
Record delimiter	New line

Collection paths

Windows	C:\ProgramData\failed_rdp.log

Details

Custom log name	FAILED_RDP_WITH_GEO_CL
Description	



Failed RDP World Map

law-honeypot

4 Editing query item: query - 3

Query (change): law-honeypot

Time Range: Last 30 days

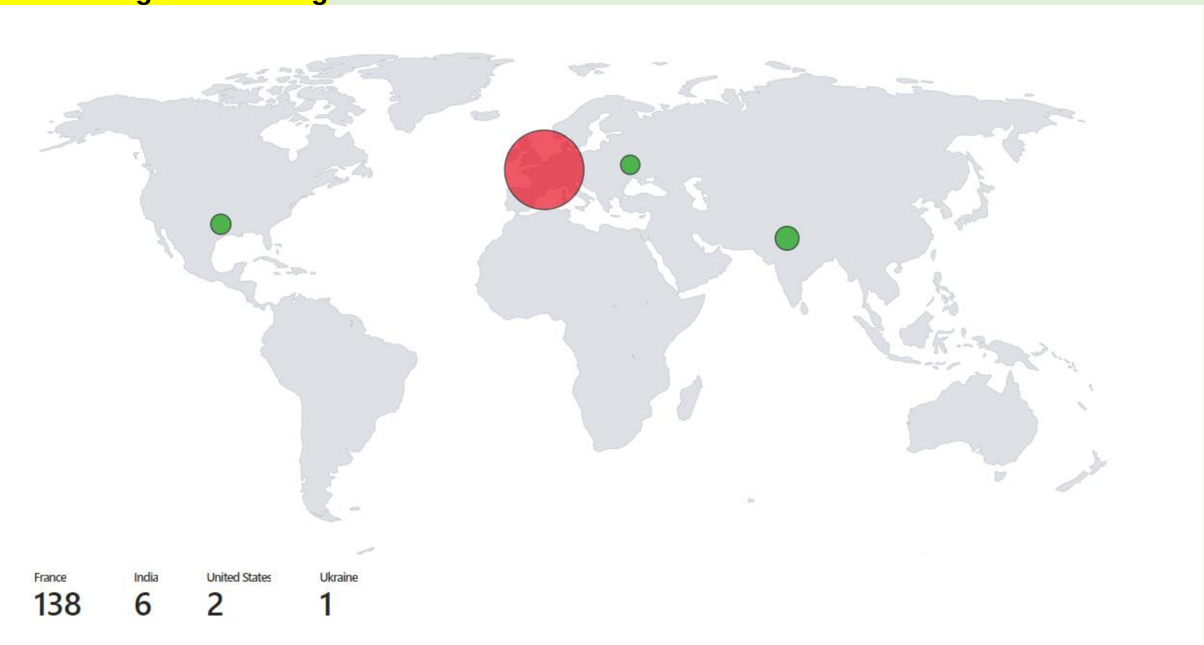
Visualization: Map

Size: Full

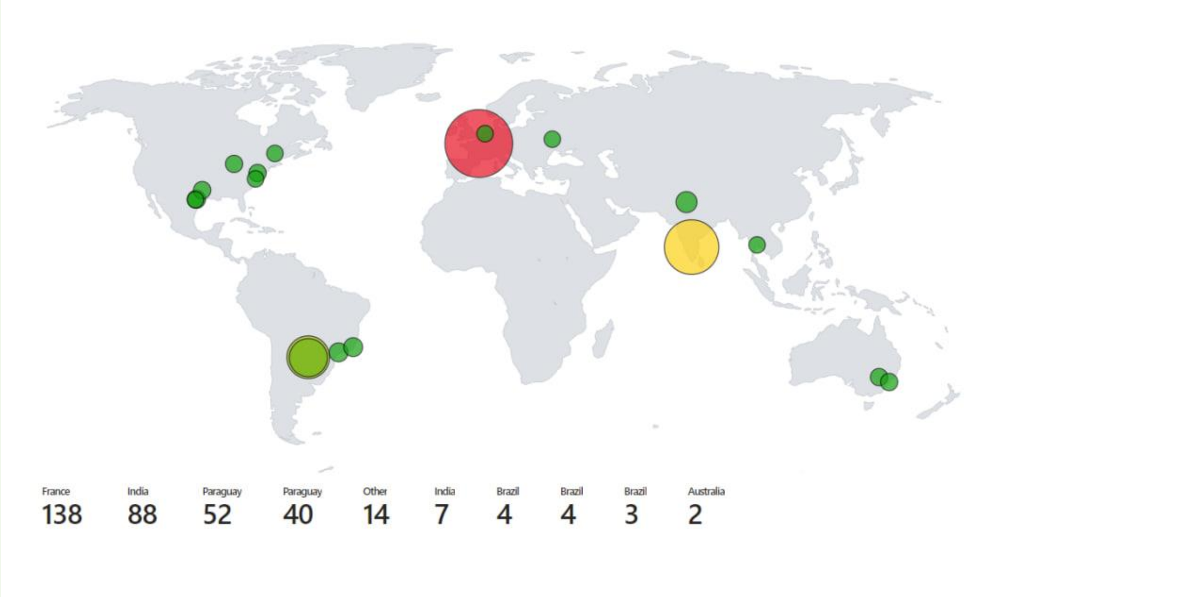
Log Analytics workspace Logs Query

```
( FAILED_RDP_WITH_GEO_CL
| extend latitude = extract("latitude:([0-9.-]+)", 1, RawData),
         longitude = extract("longitude:([0-9.-]+)", 1, RawData),
         destinationhost = extract("destinationhost:([^,]+)", 1, RawData),
         username = extract("username:([^,]+)", 1, RawData),
         sourcehost = extract("sourcehost:([^,]+)", 1, RawData),
         state = extract("state:([^,]+)", 1, RawData),
         country = extract("country:([^,]+)", 1, RawData),
         label = extract("label:([^,]+)", 1, RawData),
         timestamp = extract("timestamp:([^,]+)", 1, RawData)
| project TimeGenerated, Computer, latitude, longitude, destinationhost, username, sourcehost, state, country, label, timestamp
| summarize event_count=count() by sourcehost, latitude, longitude, country, label, destinationhost
| where destinationhost != "samplehost"
| where sourcehost != "")
```

France Begins Attacking

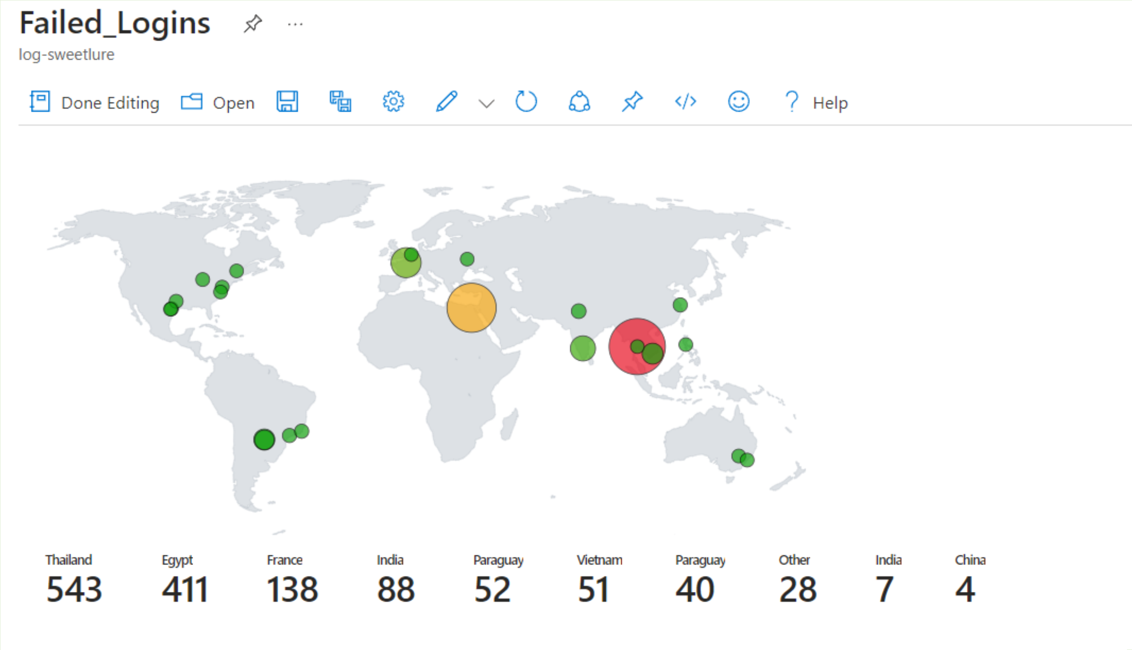


India Joins the attack



France	India	Paraguay	Paraguay	Other	India	Brazil	Brazil	Brazil	Australia
138	88	52	40	14	7	4	4	3	2

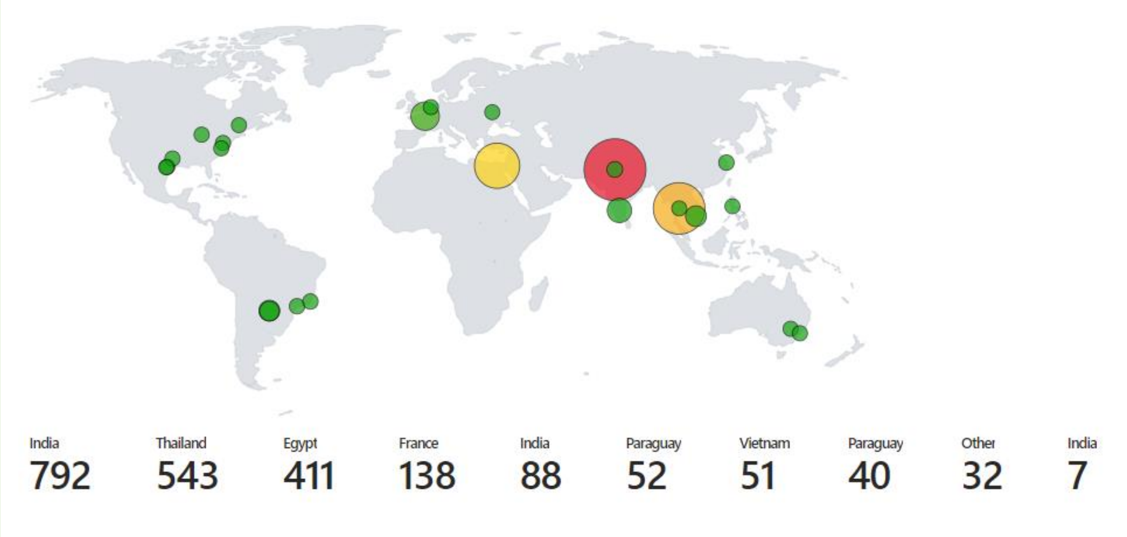
The rest of the world joins the attack



Failed_Logins

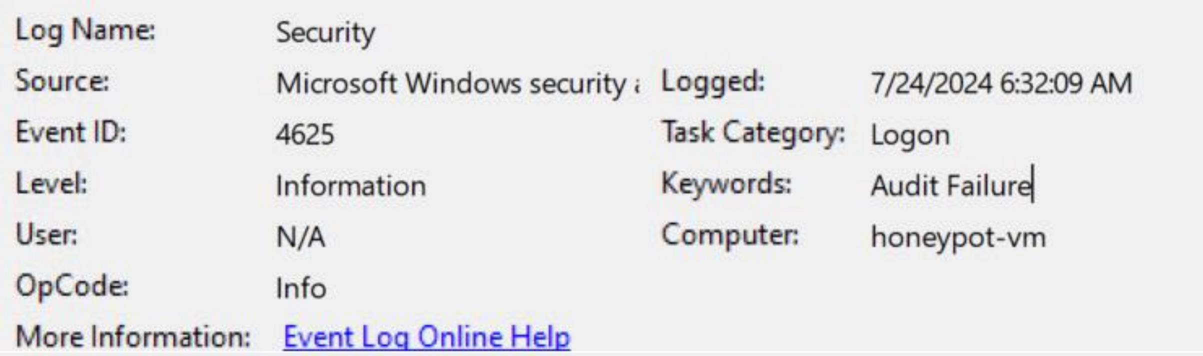
log-sweetlure

Thailand	Egypt	France	India	Paraguay	Vietnam	Paraguay	Other	India	China
543	411	138	88	52	51	40	28	7	4



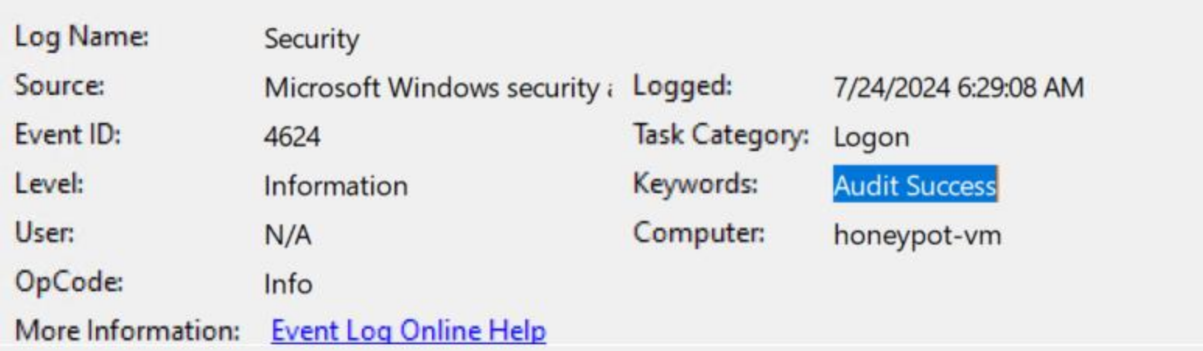
India	Thailand	Egypt	France	India	Paraguay	Vietnam	Paraguay	Other	India
792	543	411	138	88	52	51	40	32	7

Key Notes:



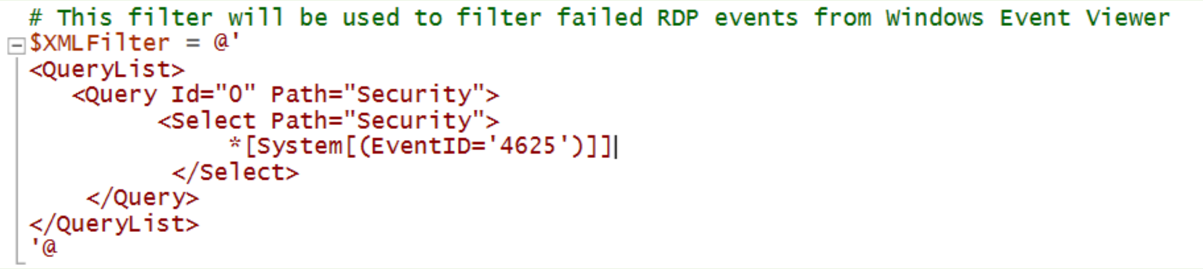
Log Name:	Security		
Source:	Microsoft Windows security ;	Logged:	7/24/2024 6:32:09 AM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	honeypot-vm
OpCode:	Info		
More Information:	Event Log Online Help		

logon (failure) 4625



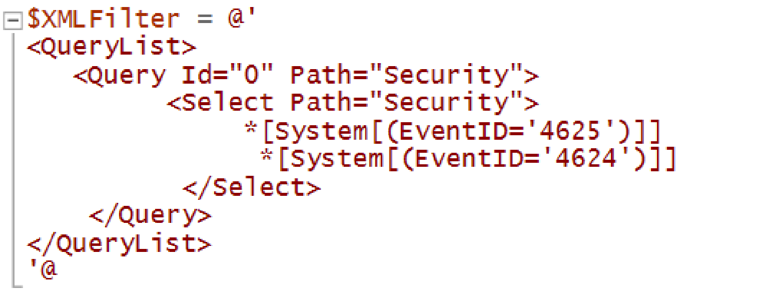
Log Name:	Security		
Source:	Microsoft Windows security ;	Logged:	7/24/2024 6:29:08 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	honeypot-vm
OpCode:	Info		
More Information:	Event Log Online Help		

logon (success) 4624



```
# 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>
'@
```

Code before alterations. Logs only the login failure events



```
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
               *[System[(EventID='4624')]]
          </Select>
    </Query>
</QueryList>
'@
```

Code after alterations. Logs both the success and failure