Analyzing Honeypot Attacks through Mapping with Azure Sentinel

The purpose of analyzing honeypot attacks is to gain insights into the tactics, techniques, and motives of malicious actors. By studying and understanding these attacks, security professionals can enhance their knowledge of emerging threats, identify vulnerabilities in systems and networks, develop more robust defense mechanisms, and ultimately improve overall cybersecurity measures. Analyzing honeypot attacks helps in detecting patterns, identifying trends, and mitigating potential risks in order to enhance the security posture of an organization or system.

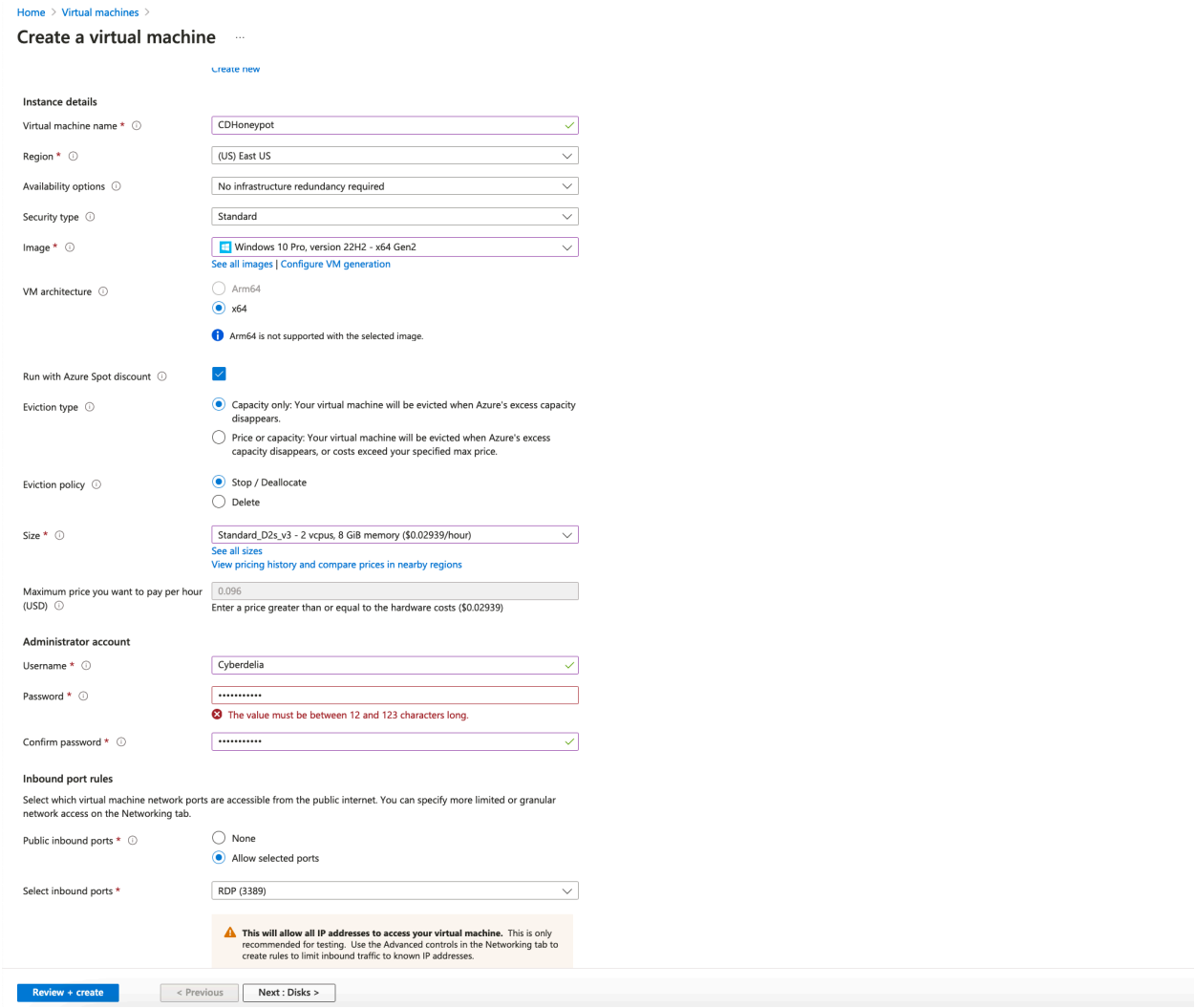
Step 1 – Create a Microsoft Azure Subscription

To register for a free Microsoft Azure account, begin by visiting the Azure website and selecting the "Start free" or "Get started for free" option. From there, either sign in using an existing Microsoft account or create a new one. Provide the necessary information, including email, password, and personal details. Verify your identity by following the prompted steps. You'll also need to provide a payment method, although you won't be billed unless you exceed the free account limits or upgrade to a paid subscription. Agree to the terms and conditions, and upon completion, you'll have access to your free Azure account with limited resources and services. Remember to review the terms to understand the constraints and duration of the free offerings.

Step 2 - Create an Azure Virtual Machine

The specs on the virtual machine you create are up to you to decide. I will list the specs I used for my honeypot VM (virtual machine).

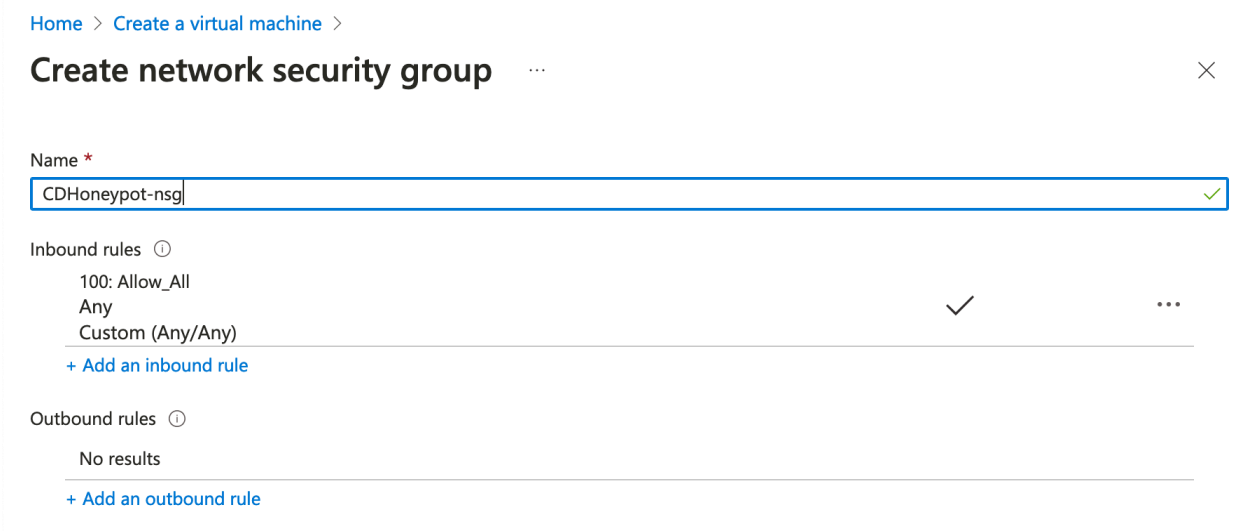
- Image: Windows 10 Pro, version 20H2 – Gen2
- Size: Standard_D2s_v3 – 2vcpus, 8 GiB memory
- Inbound Port: RDP (3389)
- OS Disk Type: Standard SSD
- NIC Network Security Group: Advanced (make a new security group)



1. In the new security group, remove the existing default inbound and outbound rules.

2. Create a new inbound security rule with the following settings

- Source: Any
- Source port ranges: *
- Destination: Any
- Service: Custom
- Destination port ranges: *
- Protocol: Any
- Action: Allow
- Priority: 100
- Name: ALLOW_ALL

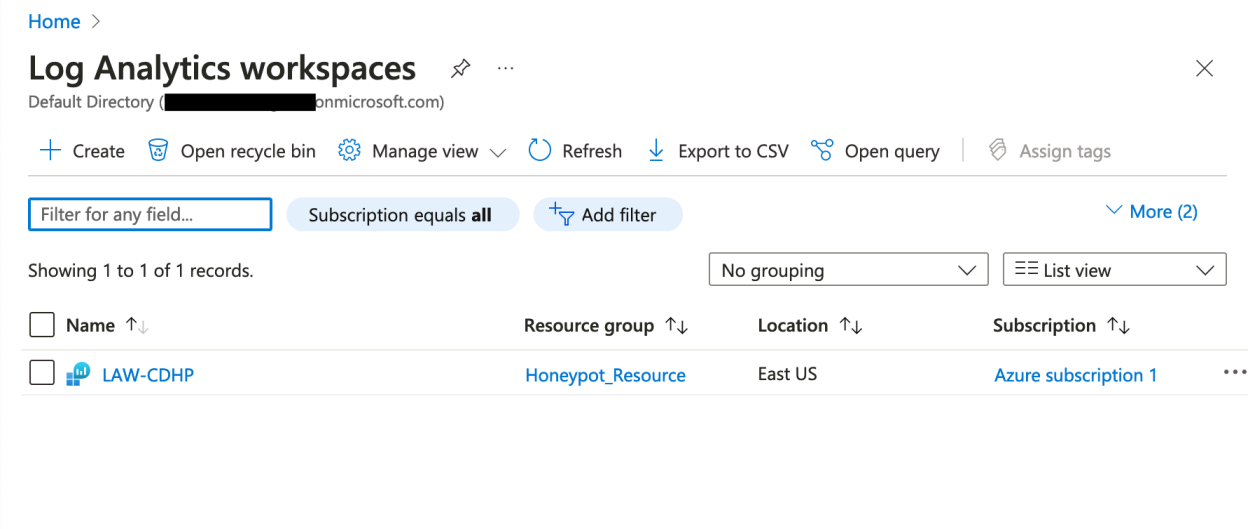


Step 3 - Building the Log Analytics Workspace

Create a new Log Analytics Workspace so that Azure Sentinel can connect to the log data and then map it.

Use the same resource group when creating a new workspace.

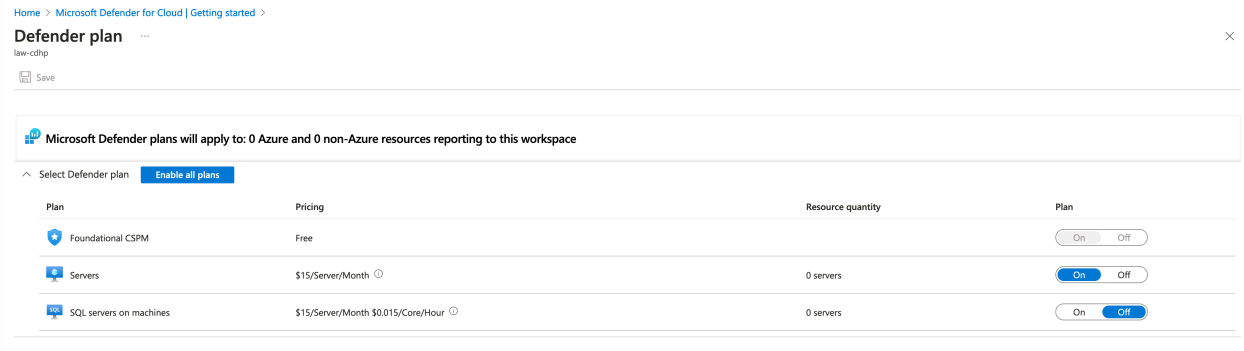
The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported after August 31, 2024, Azure is most likely incorporating this into Azure Monitor Agent, should follow pretty similar steps.*



Step 4 - Microsoft Defender for Cloud Configuration

Head-over to Microsoft Defender for Cloud and install it on the subscription if you haven't done so previously.
Once the agent has been installed, go to the **Environment Settings** option in the left menu and select your subscription.

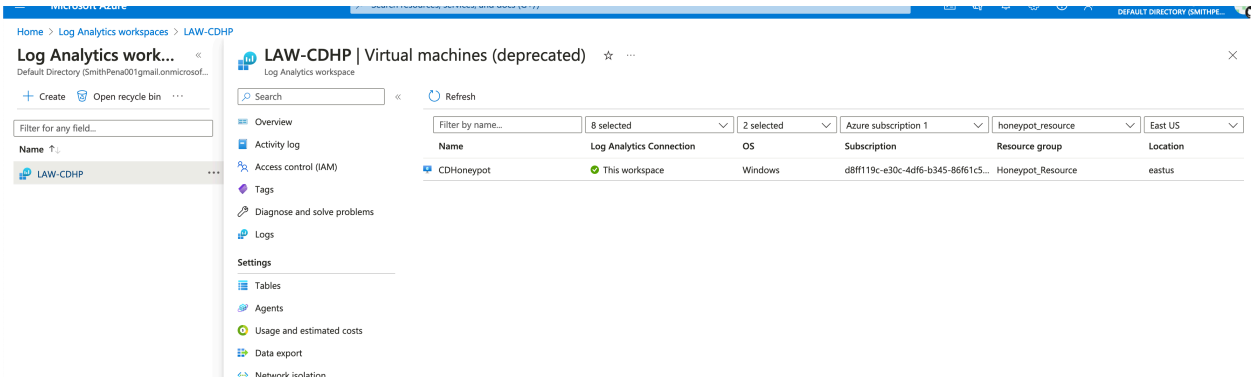
I have disabled a few of the plans such as SQL servers on machine since we won't be needing it in this case. Save your cash bruh



Now click the **Data collection** menu option and select the radio button for **All Events** and save the settings.

Step 5 - Link the Virtual Machine and the Log Analytics Workspace

Once the Log Analytics Workspace has been set up, you can proceed to establish a connection with the previously provisioned Virtual Machine. Navigate to the Workspace interface and locate the menu option labeled "Virtual machines." Within this section, select your honeypot machine and proceed to connect it with the workspace.



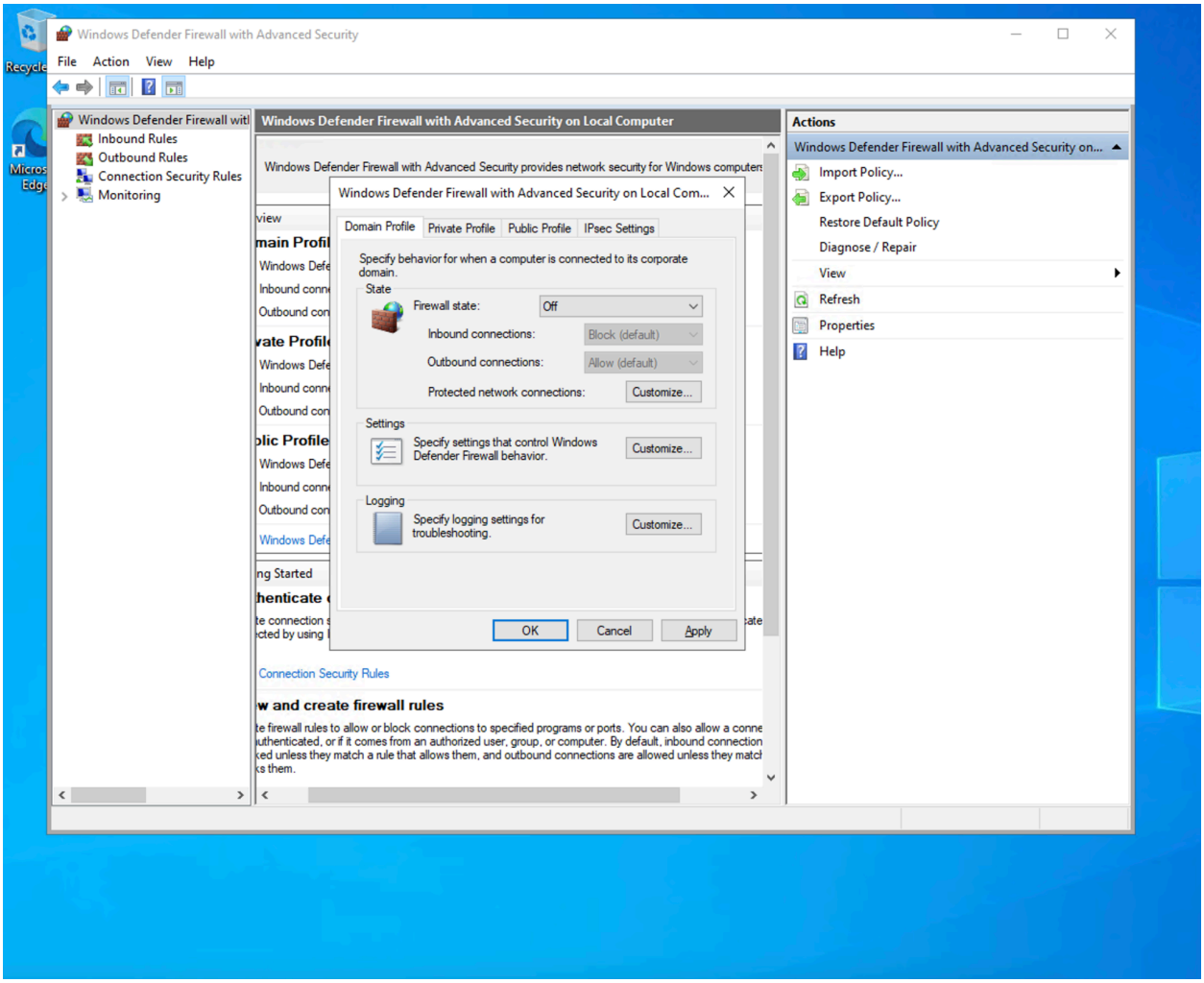
Step 6 - Setting Up Microsoft Sentinel

If you haven't used Microsoft Sentinel before, you might need to add the Microsoft Sentinel plan to your subscription. After adding it to your subscription, you can proceed to connect it with the previously created Log Analytics Workspace.

Step 7 - Turn off the Firewall in the Virtual Machine

Now log on to the previously created Virtual Machine and turn off the following options, this will allow the RDP to be visible to the open internet through ICMP echo requests.

On Domain Profile tab, change Firewall state: Off
On Private Profile tab, change Firewall state: Off
On Public Profile tab, change Firewall state: Off



You can check if the RDP is visible to the internet by pinging it on your host machine.

Step 8 - Building the Security Log Exporter

Josh Makador developed this script specifically for this project. The only part of the script that requires modification is the $API_KEY on line 2.

You can find the script at the following GitHub repository:

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

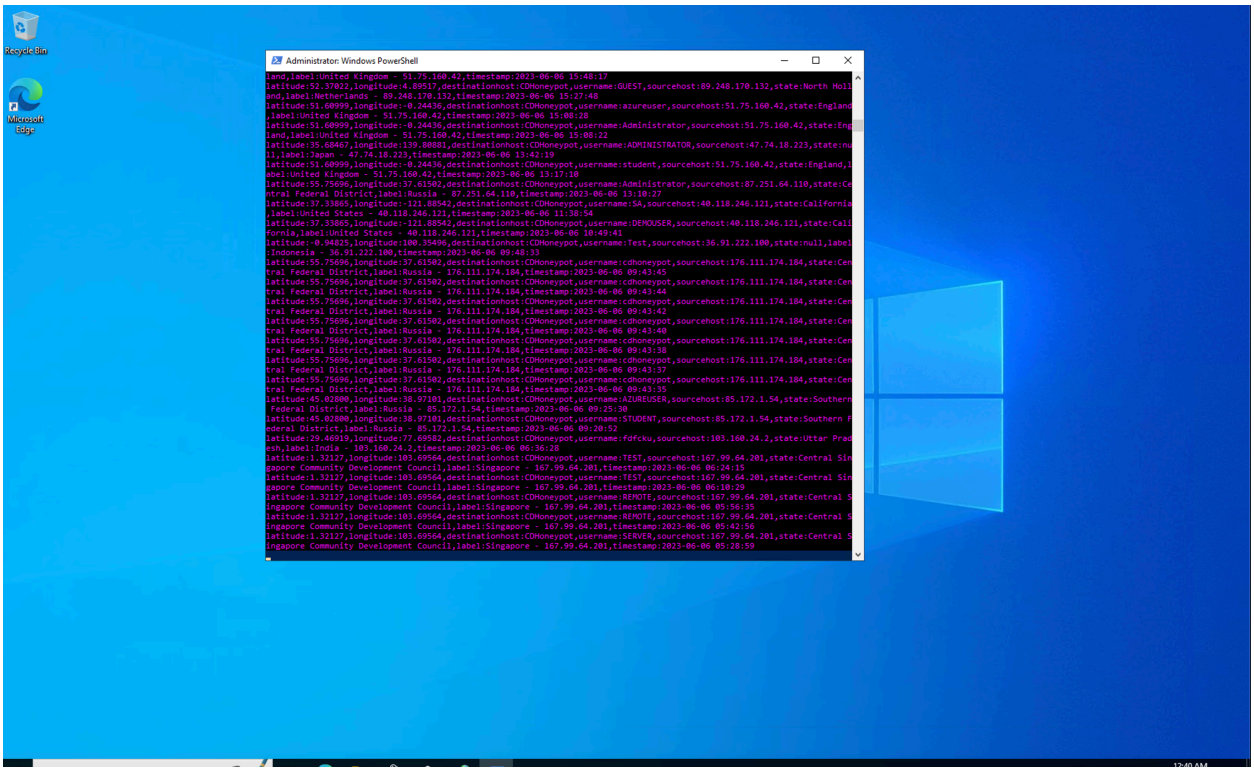
Save this PowerShell script in the virtual machine.

Next, create an account with Free IP Geolocation API and Accurate IP Geolocation Database.
This account allows up to 1000 API calls per day for free. While this may be sufficient, it is recommended to pay the $15 monthly fee for 150,000 requests per month to access more data. If desired, you can cancel your subscription after completing the project to avoid the higher request limit fee.

Once you have registered with the IP Geolocation service, obtain your API key and update line 2 in the PowerShell script with your key.

The script will export data from the Windows Event Viewer, which will then be imported into the IP Geolocation service. It will extract the latitude and longitude and create a new log file called "failed_rdp.log" located at C:\ProgramData\failed_rdp.log.

Execute the script in the PowerShell ISE within the virtual machine. It will continuously generate log data from this point onwards.



Step 9 - Import the honeypot logs into Log Analytics Workspace

We will now proceed to generate a custom log to import additional data from the IP Geolocation service into Azure Sentinel.

Head over to the Log Analytics Workspace, Click on your workspace and then tables, then create a custom log.

Azure will prompt you to upload a log file. As the log is located on the virtual machine, you will need to copy its contents into a new log file on your host machine and then proceed to upload that log file to Azure. This step is crucial for training the Log Analytics Workspace to extract specific data elements from the actual logs.

When creating a custom log, you will be asked to provide a collection path. Ensure the collection path adheres to the following settings.

- Type: Windows
- Path: C:\ProgramData\failed_rdp.log
- Name: FailedRDP_CL

Home > Log Analytics workspaces > LAW-CDHP | Tables >

Create a custom log

1 Sample | 2 Record delimiter | 3 Collection paths | 4 Details | 5 Review + Create

Upload a sample of the custom log. The wizard will parse and display the entries in this file. Learn more

Sample log

Select a sample log *

Select a file

Home > Log Analytics workspaces > LAW-CDHP | Tables >

Create a custom log

✓ Sample | ✓ Record delimiter | ✓ Collection paths | ✓ Details | 5 Review + Create

Sample

Sample log	failed_rdp.log

Record delimiter

Record delimiter	New line

Collection paths

Windows	C:\ProgramData\failed_rdp.log

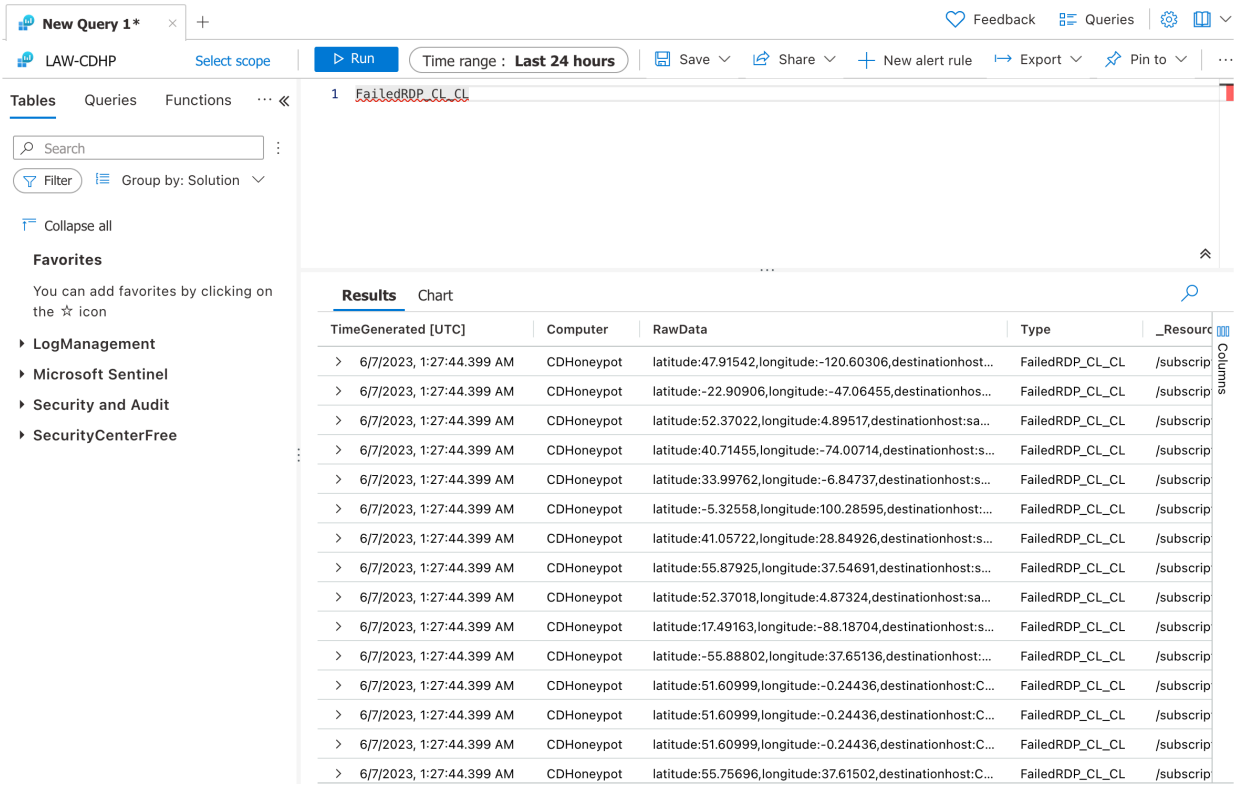
Details

Custom log name	FailedRDP_CL_CL
Description	

Step 10 - Query the Custom Log

Navigate to the Logs menu within the Log Analytics Workspace. This will open a window displaying a queries and their results. Once the custom log creation is complete, you can execute a query against this the data to observe the extracted data.

After successfully creating the custom log in Azure, execute a query to explore the available data. In this instance, the custom log is named "FailedRDP_CL”

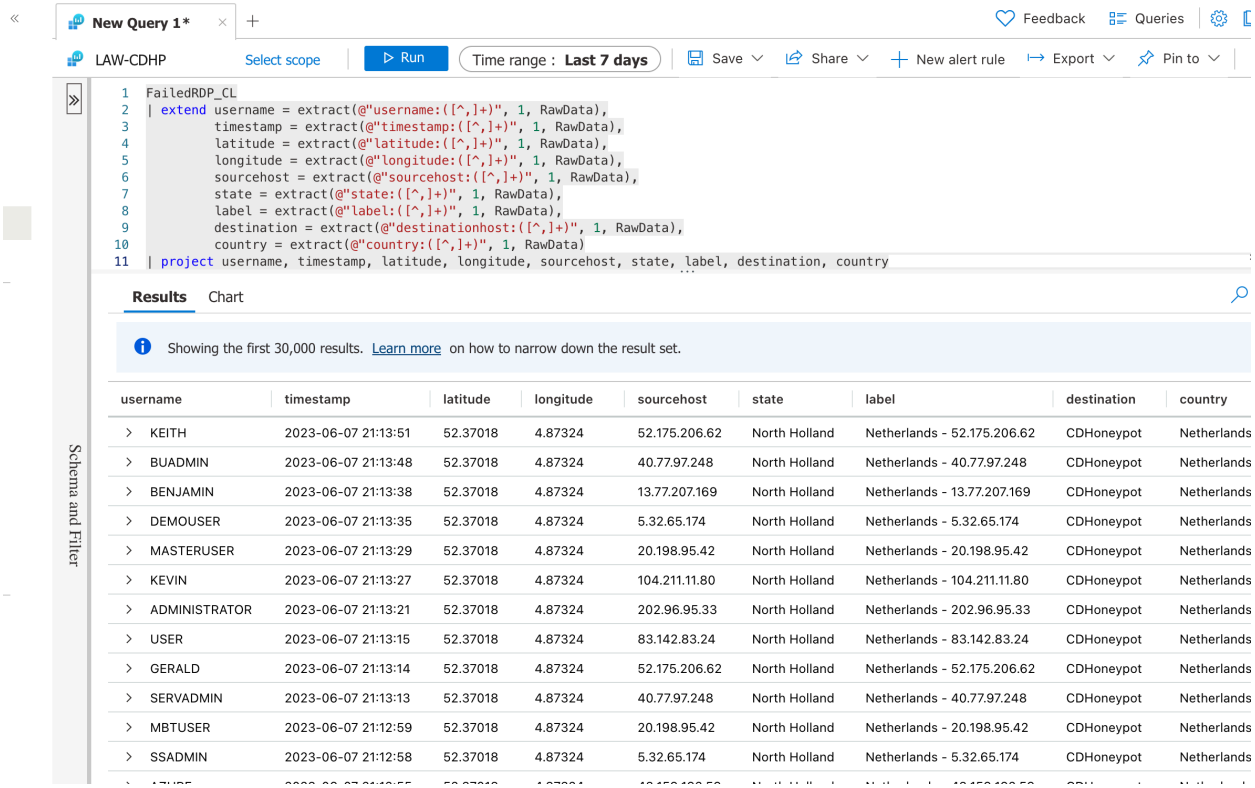


TimeGenerated [UTC]	Computer	RawData	Type	_Resourc
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:47.91542,longitude:-120.60306,destinationhost...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:-22.90906,longitude:-47.06455,destinationhos...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:52.37022,longitude:4.89517,destinationhost:sa...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:40.71455,longitude:-74.00714,destinationhost:s...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:33.99762,longitude:-6.84737,destinationhost:s...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:-5.32558,longitude:100.28595,destinationhost:...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:41.05722,longitude:28.84926,destinationhost:s...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:55.87925,longitude:37.54691,destinationhost:s...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:52.37018,longitude:4.87324,destinationhost:sa...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:17.49163,longitude:-88.18704,destinationhost:s...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:-55.88802,longitude:37.65136,destinationhost:...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:51.60999,longitude:-0.24436,destinationhost:C...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:51.60999,longitude:-0.24436,destinationhost:C...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:51.60999,longitude:-0.24436,destinationhost:C...	FailedRDP_CL_CL	/subscrip
6/7/2023, 1:27:44.399 AM	CDHoneypot	latitude:55.75696,longitude:37.61502,destinationhost:C...	FailedRDP_CL_CL	/subscrip

Step 11 - Parse the data from the custom log

To parse the data, we're going to use KQL,

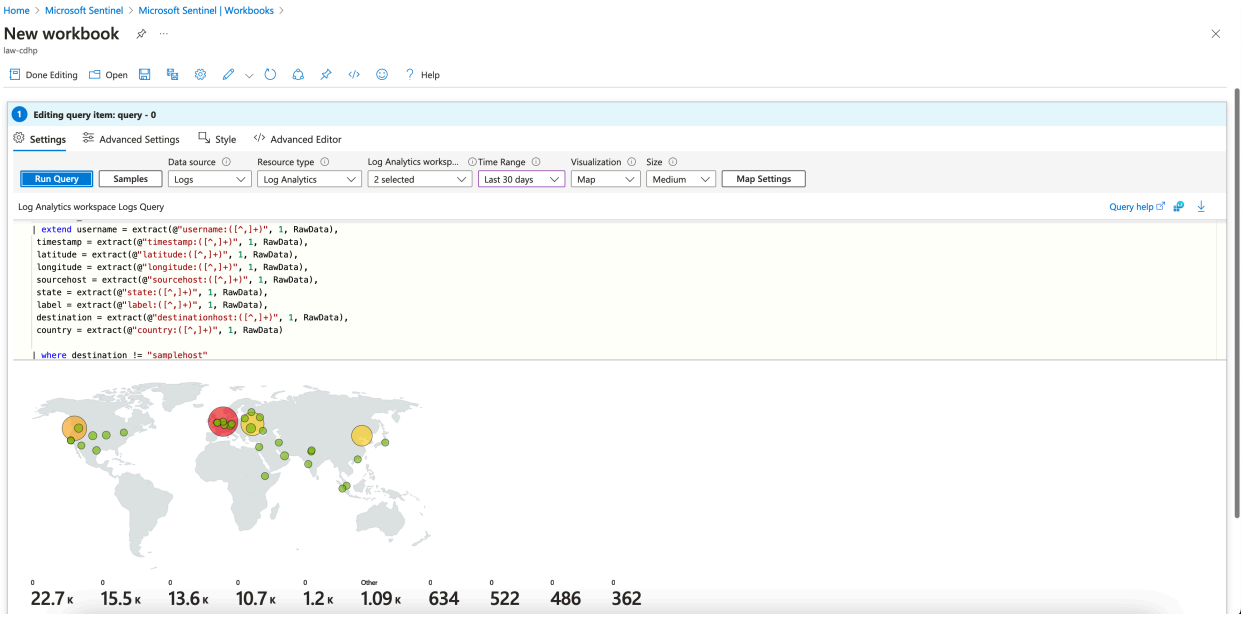
```
| extend username = extract(@"username:([^,]+)", 1, rawData),
        timestamp = extract(@"timestamp:([^,]+)", 1, rawData),
        latitude = extract(@"latitude:([^,]+)", 1, rawData),
        longitude = extract(@"longitude:([^,]+)", 1, rawData),
        sourcehost = extract(@"sourcehost:([^,]+)", 1, rawData),
        state = extract(@"state:([^,]+)", 1, rawData),
        label = extract(@"label:([^,]+)", 1, rawData),
        destination = extract(@"destinationhost:([^,]+)", 1, rawData),
        country = extract(@"country:([^,]+)", 1, rawData)
| project username, timestamp, latitude, longitude, sourcehost, state, label,
destination, country
```



username	timestamp	latitude	longitude	sourcehost	state	label	destination	country
KEITH	2023-06-07 21:13:51	52.37018	4.87324	52.175.206.62	North Holland	Netherlands - 52.175.206.62	CDHoneypot	Netherlands
BUADMIN	2023-06-07 21:13:48	52.37018	4.87324	40.77.97.248	North Holland	Netherlands - 40.77.97.248	CDHoneypot	Netherlands
BENJAMIN	2023-06-07 21:13:38	52.37018	4.87324	13.77.207.169	North Holland	Netherlands - 13.77.207.169	CDHoneypot	Netherlands
DEMOUSER	2023-06-07 21:13:35	52.37018	4.87324	5.32.65.174	North Holland	Netherlands - 5.32.65.174	CDHoneypot	Netherlands
MASTERUSER	2023-06-07 21:13:29	52.37018	4.87324	20.198.95.42	North Holland	Netherlands - 20.198.95.42	CDHoneypot	Netherlands
KEVIN	2023-06-07 21:13:27	52.37018	4.87324	104.211.11.80	North Holland	Netherlands - 104.211.11.80	CDHoneypot	Netherlands
ADMINISTRATOR	2023-06-07 21:13:21	52.37018	4.87324	202.96.95.33	North Holland	Netherlands - 202.96.95.33	CDHoneypot	Netherlands
USER	2023-06-07 21:13:15	52.37018	4.87324	83.142.83.24	North Holland	Netherlands - 83.142.83.24	CDHoneypot	Netherlands
GERALD	2023-06-07 21:13:14	52.37018	4.87324	52.175.206.62	North Holland	Netherlands - 52.175.206.62	CDHoneypot	Netherlands
SERVADMIN	2023-06-07 21:13:13	52.37018	4.87324	40.77.97.248	North Holland	Netherlands - 40.77.97.248	CDHoneypot	Netherlands
MBTUSER	2023-06-07 21:12:59	52.37018	4.87324	20.198.95.42	North Holland	Netherlands - 20.198.95.42	CDHoneypot	Netherlands
SSADMIN	2023-06-07 21:12:58	52.37018	4.87324	5.32.65.174	North Holland	Netherlands - 5.32.65.174	CDHoneypot	Netherlands

Step 12 - Mapping the Data in Azure Sentinel

On the top search bar, search for Sentinel.
Proceed to the Overview page to observe the available events.
In the left menu, select Workbooks and click on Add workbook.
Then, click on Edit.
The newly created workbook will contain default widgets.
Edit these widgets to remove them from the workbook, as we will be creating our own.
Add a query to display the query and results window.
Copy and paste the provided query into the query window, and then execute the query by clicking on Run Query.
After the results are displayed, navigate to the Visualization dropdown and choose the Map option to visualize the data on a World Map.



And there you have it! we've set a honeypot to attract and deceive potential attackers, as well as visualization of the origin of the attacks. This can help us in many ways including gathering information about attacker techniques, studying attack patterns, analyzing malware, and improving cybersecurity defenses. If you have any questions feel free to reach out via linked in.