Cyber Home Lab

By: Keziah Rogers

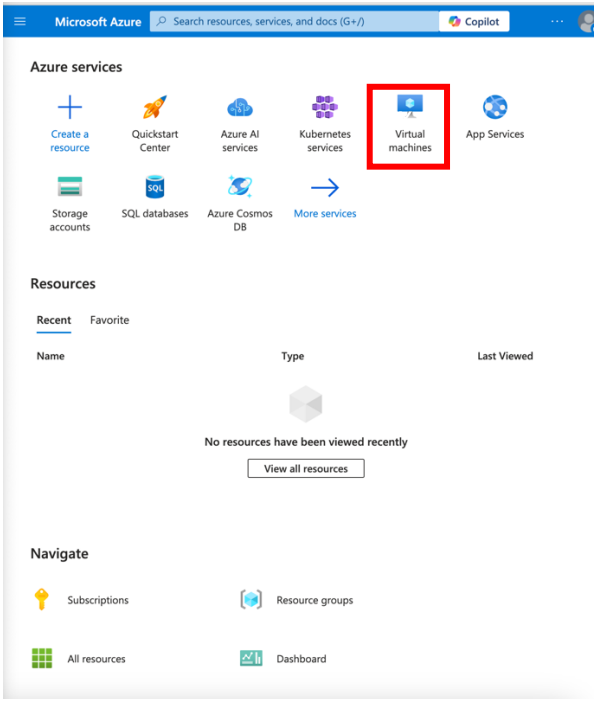
Part 1. Setup Azure Subscription

I created a Free Azure Subscription: https://azure.microsoft.com/en-us/pricing/purchase-options/azure-account

After my subscription was created, I logged in at: https://portal.azure.com

Part 2. Create the Honey Pot (Azure Virtual Machine)

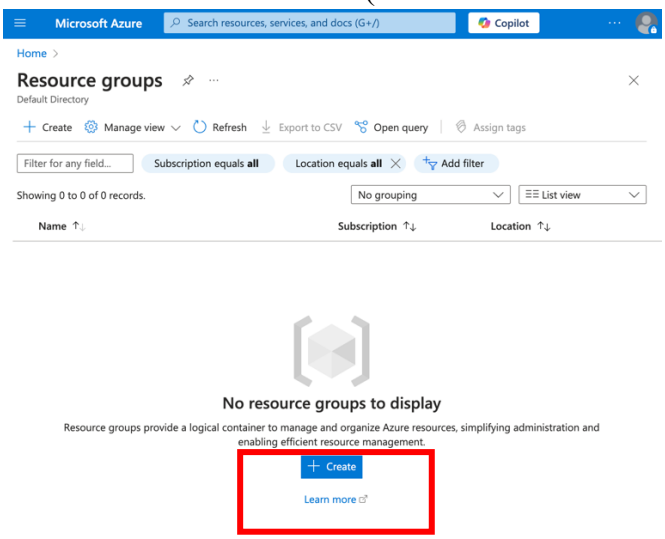
I went to: https://portal.azure.com and search for virtual machines



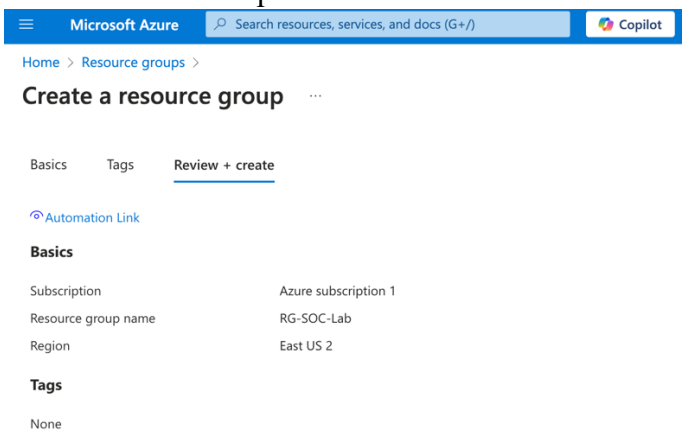
I created a new Windows 10 virtual machine (chose an appropriate size.

1) First, I created a resource group before creating a virtual machine (VM) by typing in the phrase in the top search bar.

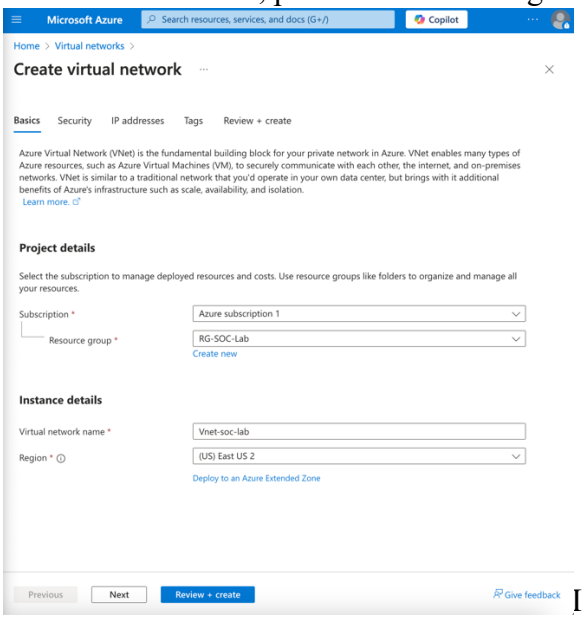
2) Next, I selected Create < Picked my subscription < Named my Resource Group: “RG-SOC-Lab < Chose the region as US East US 2 < Hit create (which creates a folder for all



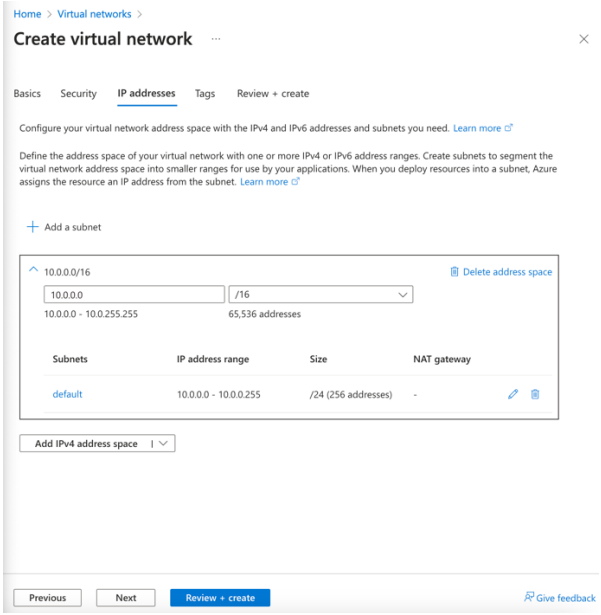
of the actions that I performed.



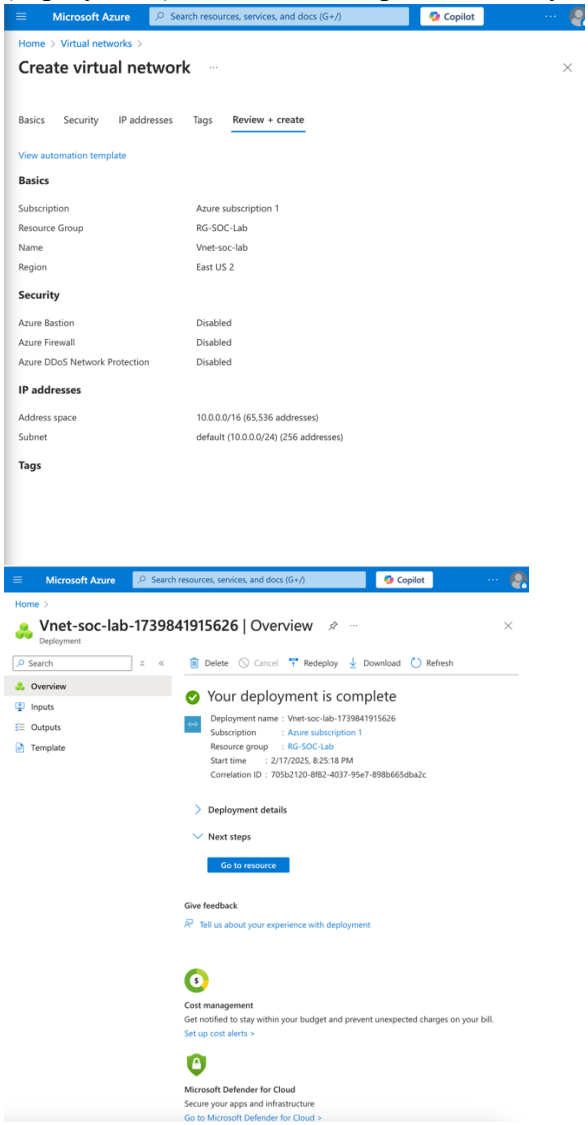
3) I then searched “Resource Group” at the top again, and confirmed that my particular group appears, and it does.

4) Next, I created a virtual network, put it in the same region as my RG-SOC-Lab folder, and hit next. 

I then hit next to keep the default IP addresses and tags, and then hit create.

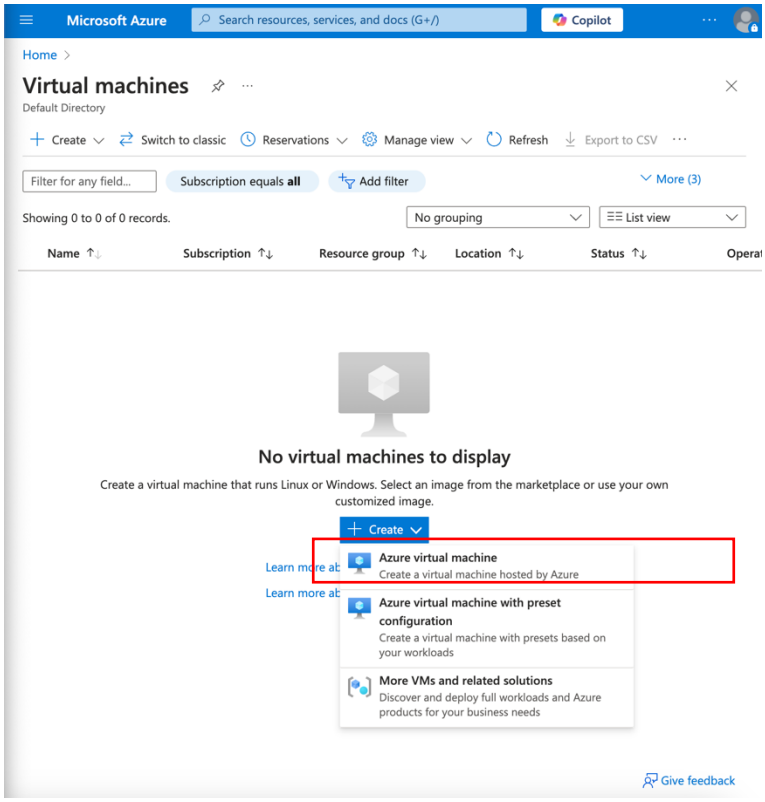


5) My VN (Virtual Network) formed, then I hit create to let everything complete (deployment), which shows up inside of my resource group I created already.

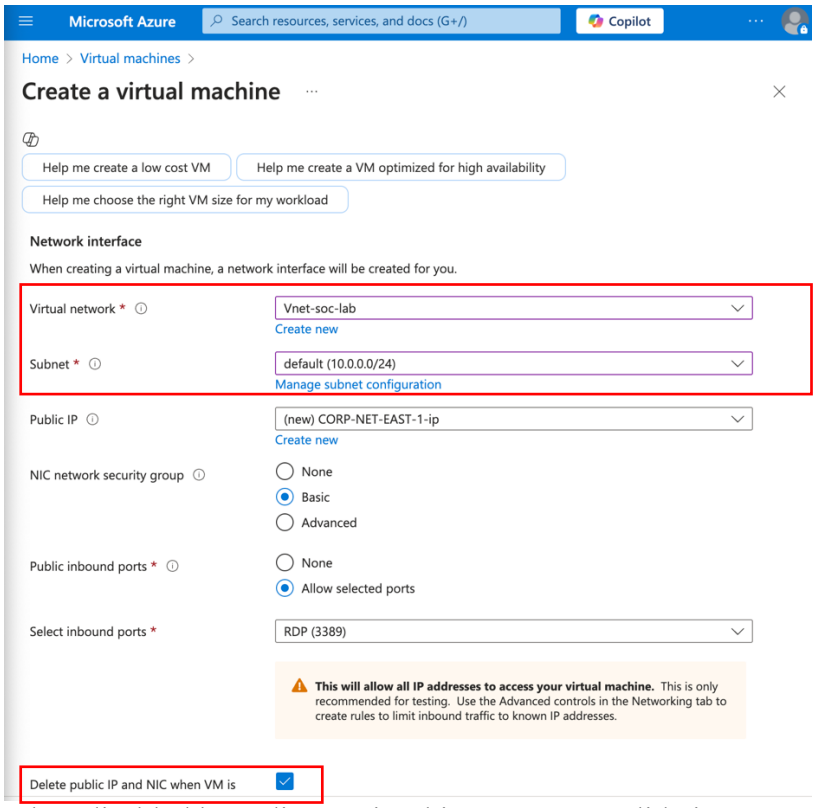


6)

7) Next, I created the Virtual Machine.

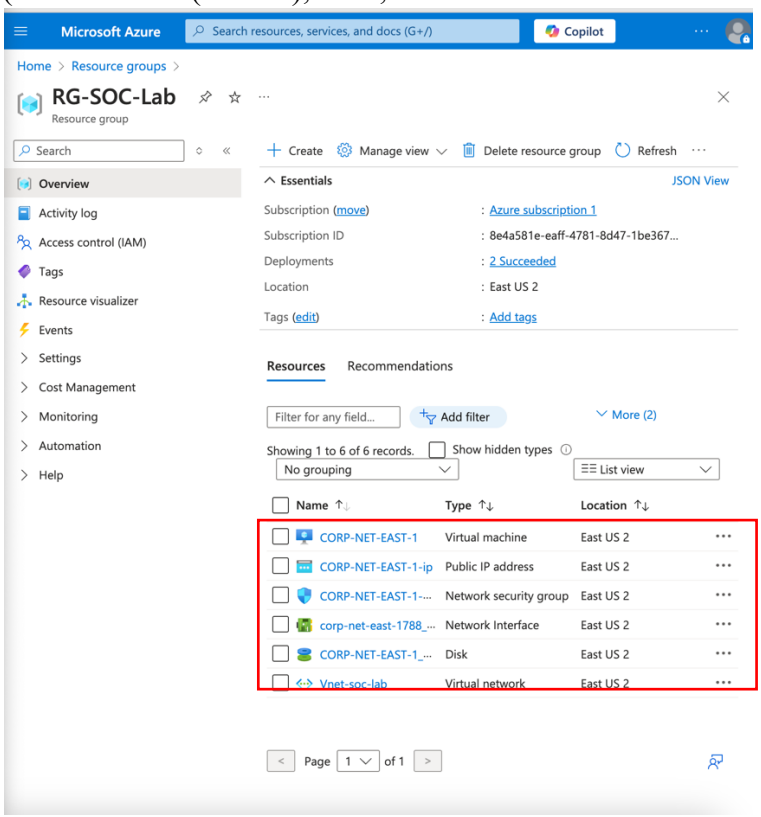


8) I then added the VM name: **CORP-Net-East-1**, the image: **Windows 10**, the username/password: **labuser | Cyberlab23!,** I confirmed the license agreement, then hit next, next, and selected “Delete public IP and NIC when VM is deleted, and hit next.



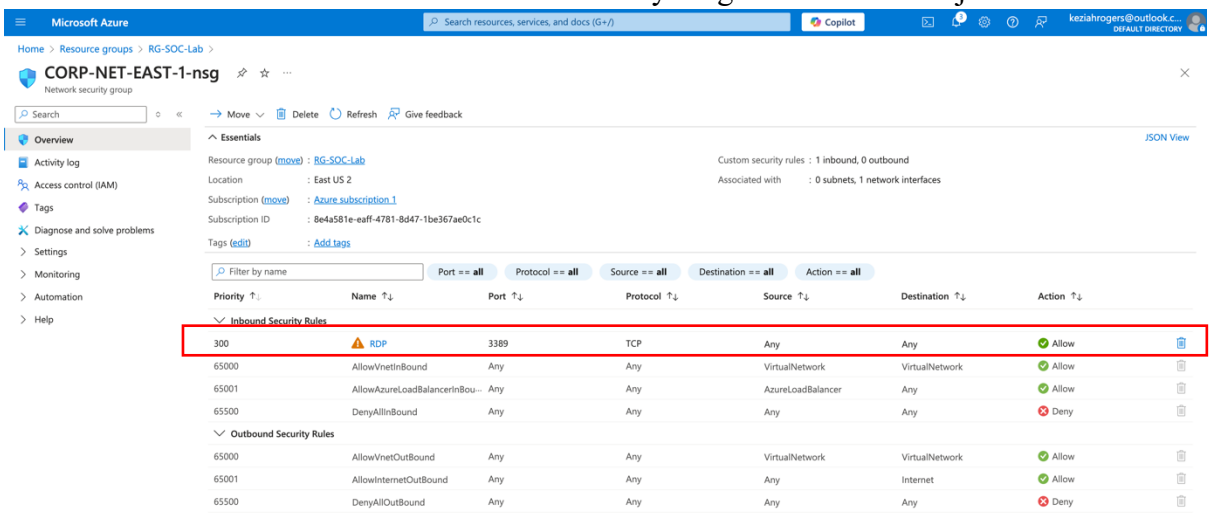
9)
10) I then disabled boot diagnostics, hit next, once validation passed, I hit create, and waited for the VM to finish deploying.
11) I then went to resource groups and viewed my computer components like: virtual machine, public IP address, network security group (Cloud Firewall), network interface

(Ethernet Port (Virtual), Disk, and Virtual Network.



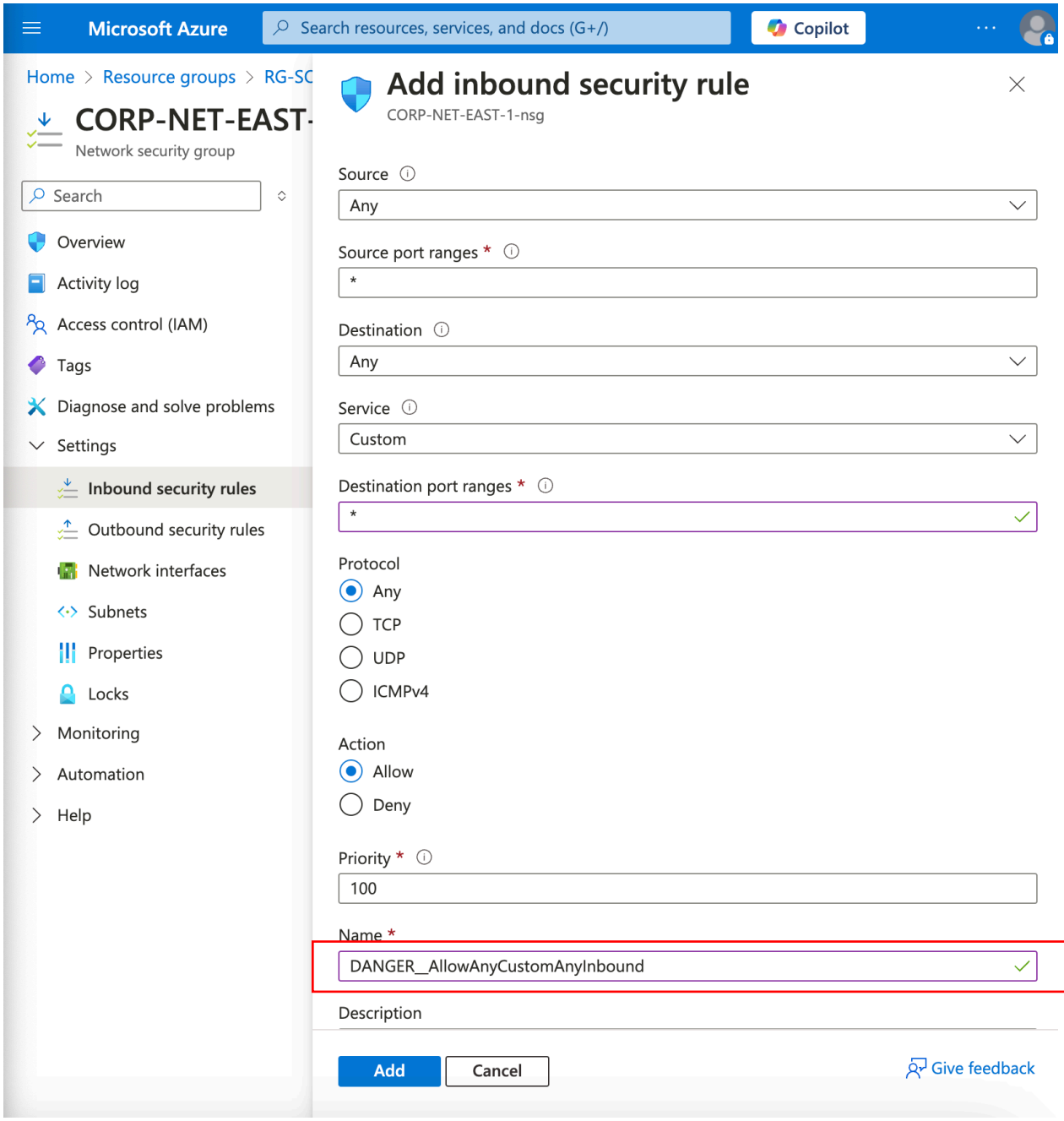
Go to the Network Security Group for your virtual machine and create a rule that allows all traffic inbound

- I edited this firewall so that anyone can access this so we can allow all traffic inbound.
- **RDP (Remote Desktop Protocol - 3389)** was already allowed inbound, but I deleted this default rule and created a new one that allows everything inbound and not just RDP.

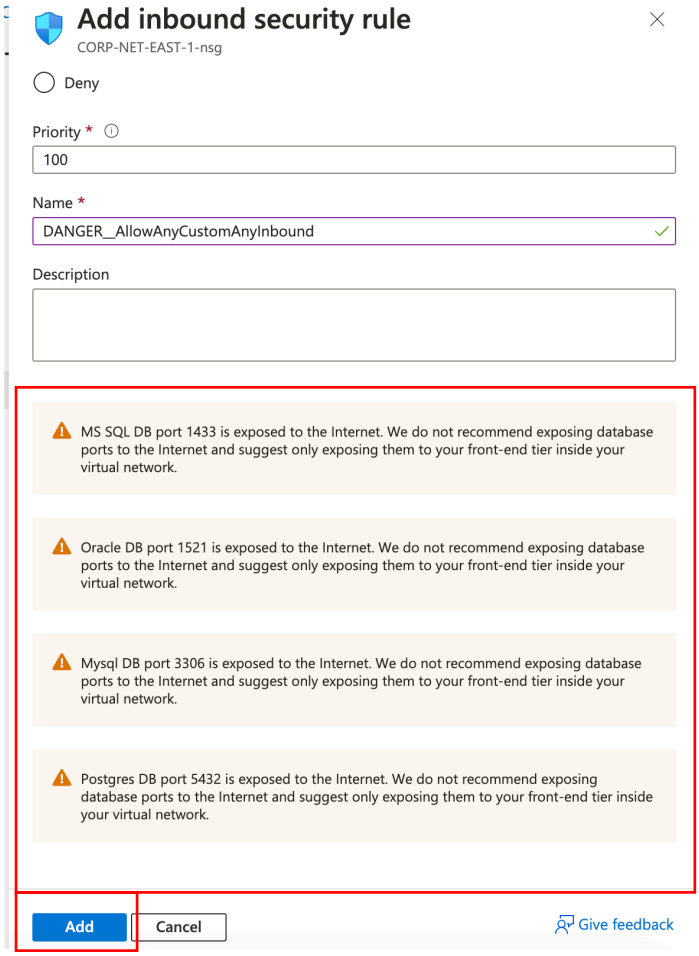


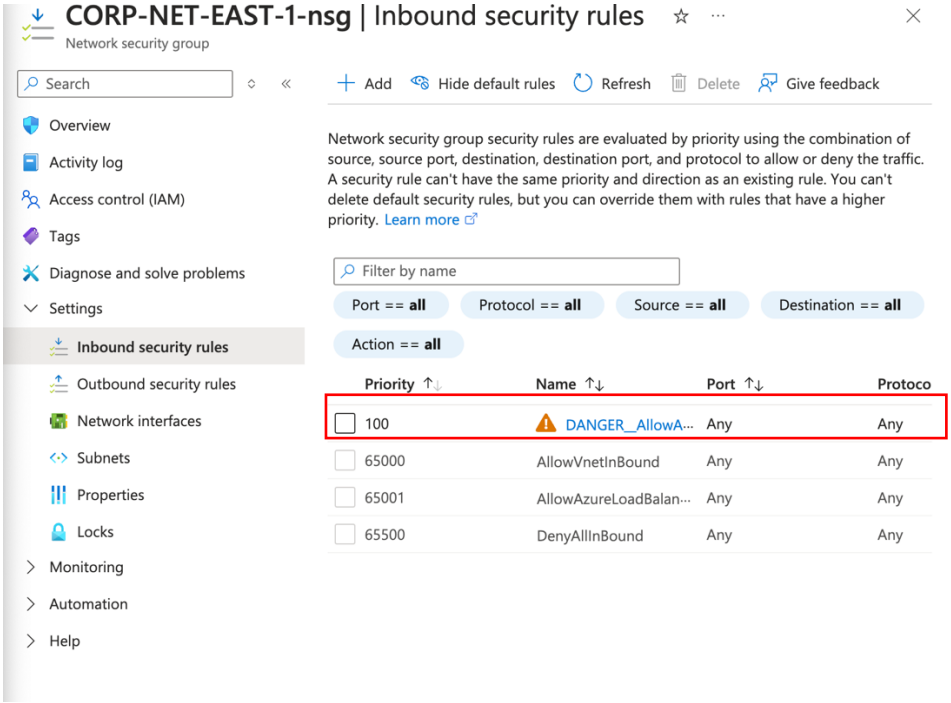
-
- Next, I went to Settings<Inbound Security Rules<Add to create a new inbound security rule.

- I kept the default rules to ANY or *. Then I added DANGER__ in front of the default name for this rule and hit add.



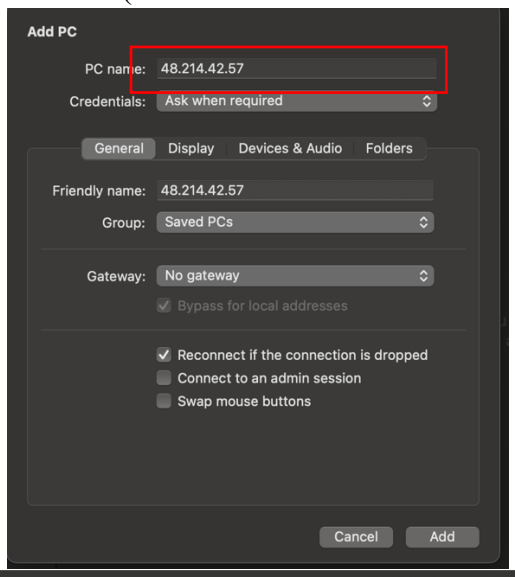
- I also noticed the warning messages also before submitting this new rule since they warned me that RDP is exposed to the internet.

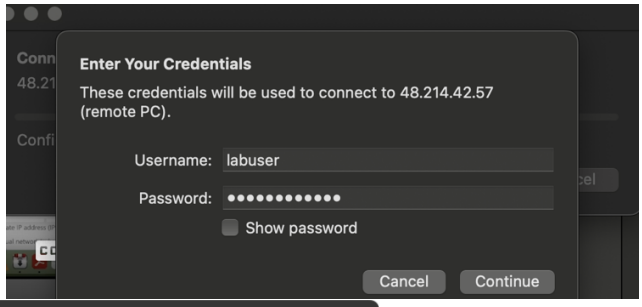

Add inbound security rule
CORP-NET-EAST-1-nsg
Deny
Priority *
100
Name *
DANGER__AllowAnyCustomAnyInbound
Description
MS SQL DB port 1433 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.
Oracle DB port 1521 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.
Mysql DB port 3306 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.
Postgres DB port 5432 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.
Add
Cancel
Give feedback

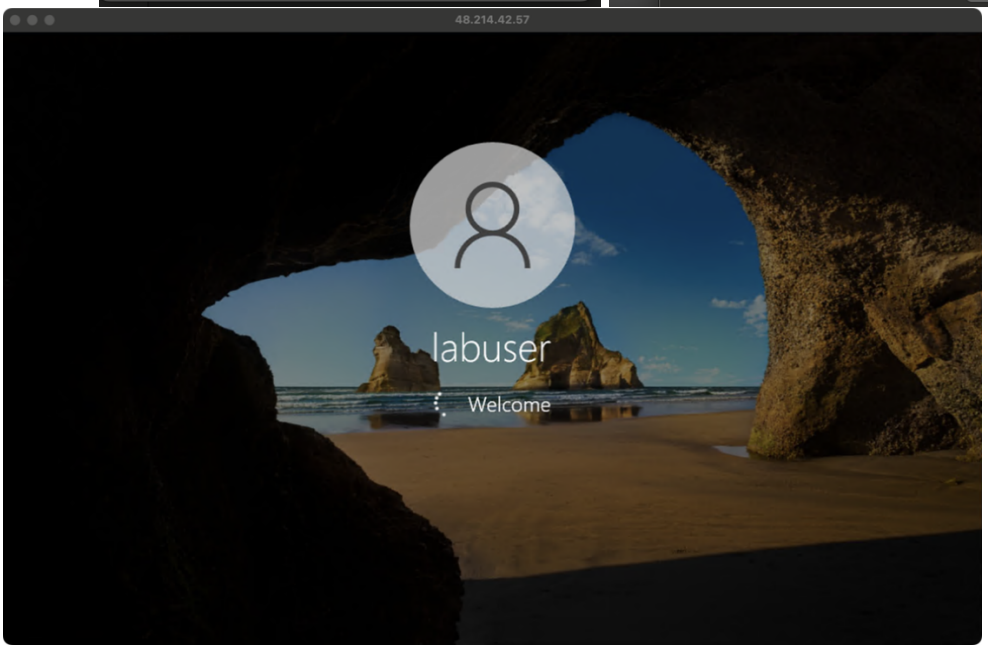

CORP-NET-EAST-1-nsg | Inbound security rules
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Add
Hide default rules
Refresh
Delete
Give feedback
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protoco
100
DANGER__AllowA...
Any
Any
65000
AllowVnetInBound
Any
Any
65001
AllowAzureLoadBalan...
Any
Any
65500
DenyAllInBound
Any
Any

Log into your virtual machine and turn off the windows firewall (start -> wf.msc -> properties -> all off)

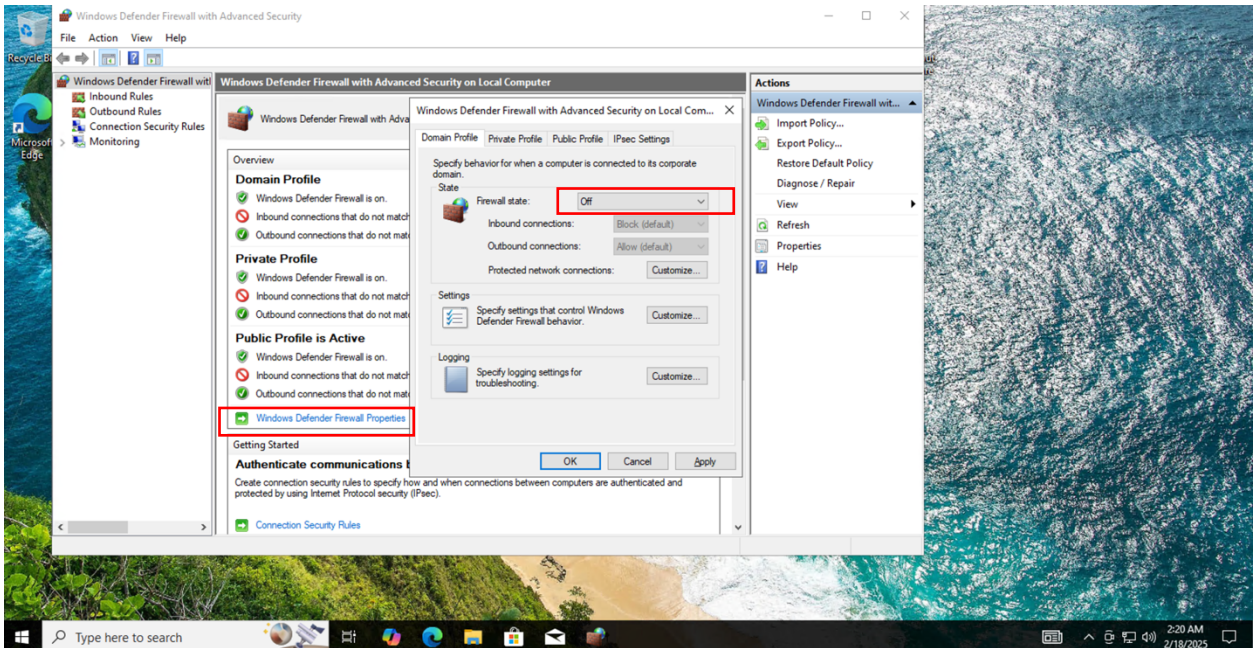
- I had to download Windows Mac to use RDP since I was using a MacBook for this whole process.
- I copied my machine's **Public IP address**, I opened the Windows Mac, clicked add a pc, input the VM's public IP address into the name fields, clicked add, and accessed the machine (I waited sometime for this to fully log me in).



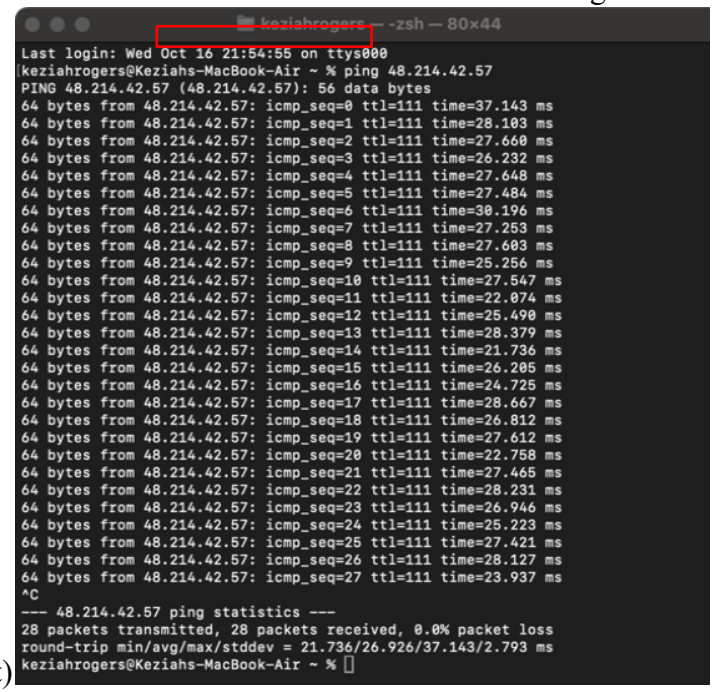




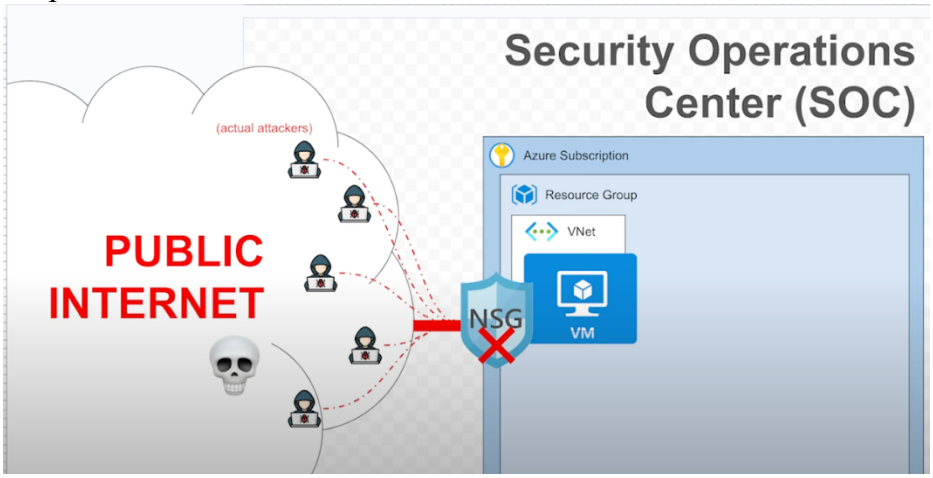
- I then put "No" for my privacy settings and fully accessed my VM.
- I then turned off my firewall by going to: Start<typed in wf.msc< opened the MS Common Console Document to view my Firewall, clicked Windows Defender Firewall Properties, and turned the firewall tab off for each tab (Domain Profile, Private Profile, Public Profile, IPsec Settings)



- I then pinged my virtual machine from my local computer by going to search<terminal<ping 48.214.42.57<and hit Ctrl+C to stop the run. (The bytes show that the device was able to be reached due to the firewall being turned off and connected to the internet)

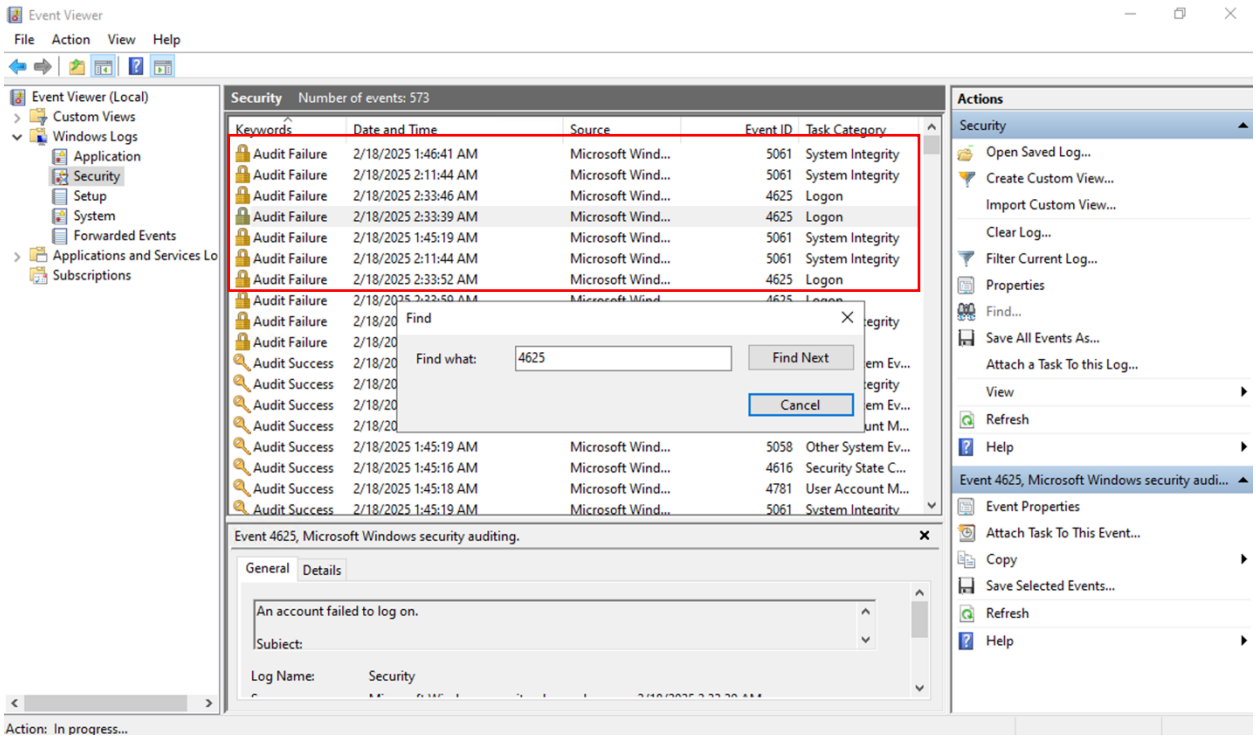


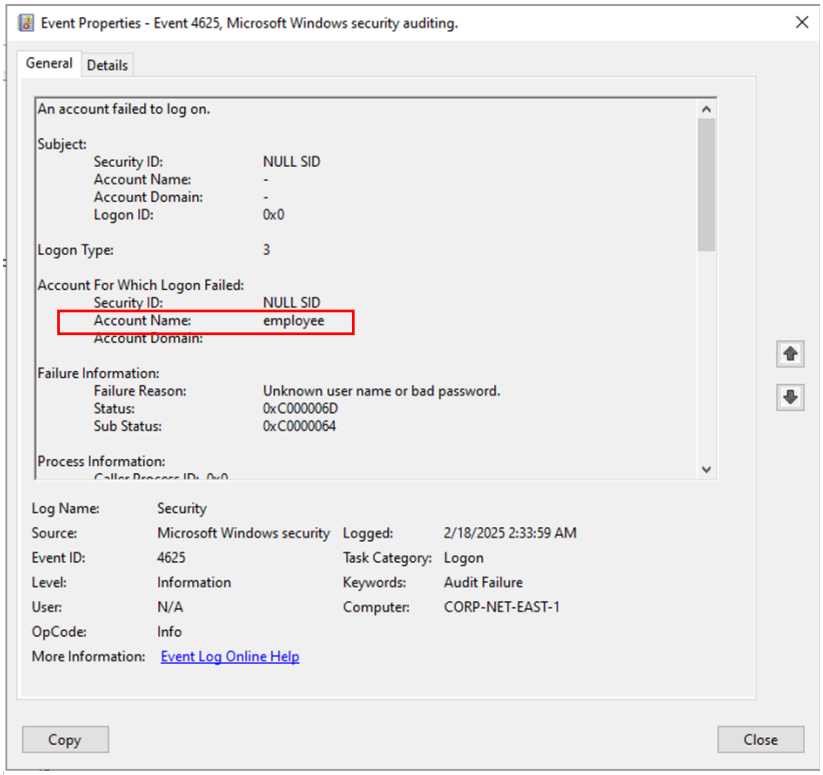
Snapshot of the blank architecture so far:

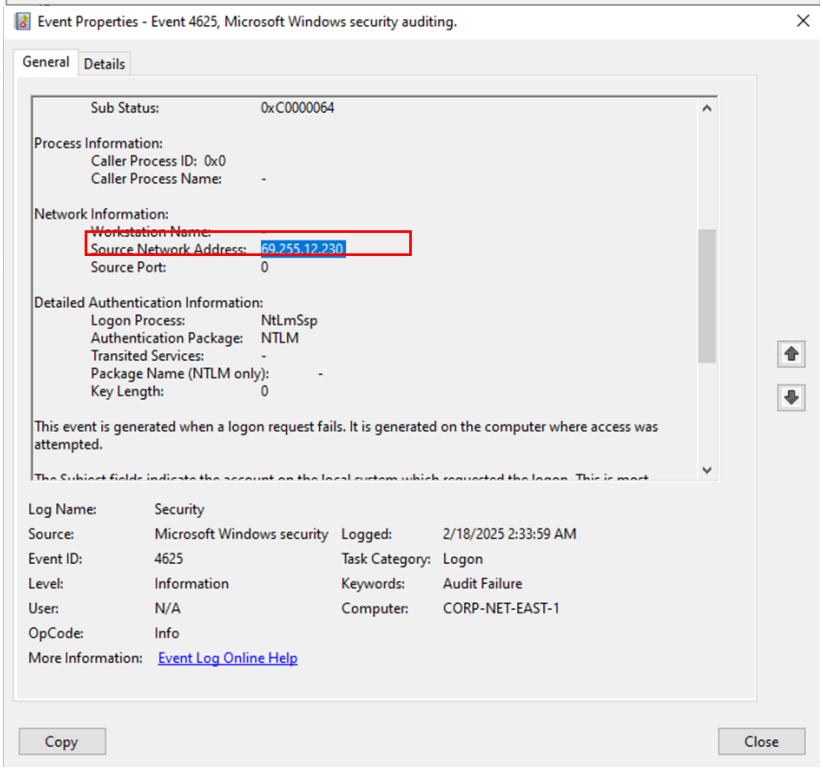


Part 3. Logging into the VM and inspecting logs

- I then logged out of the VM and attempted to reopen it by failing the login or trying to access it as someone else. Then I logged in with the correct credentials.
- I failed 3 logins as “employee” (or some other username)
- I logged into my virtual machine
- I opened up **Event Viewer** and inspected the security logs
- I saw the 3 failed logins as “employee”, event ID **4625 (I also noticed my IP address from where I attempted to log in from was also shown: 69.255.12.230)**



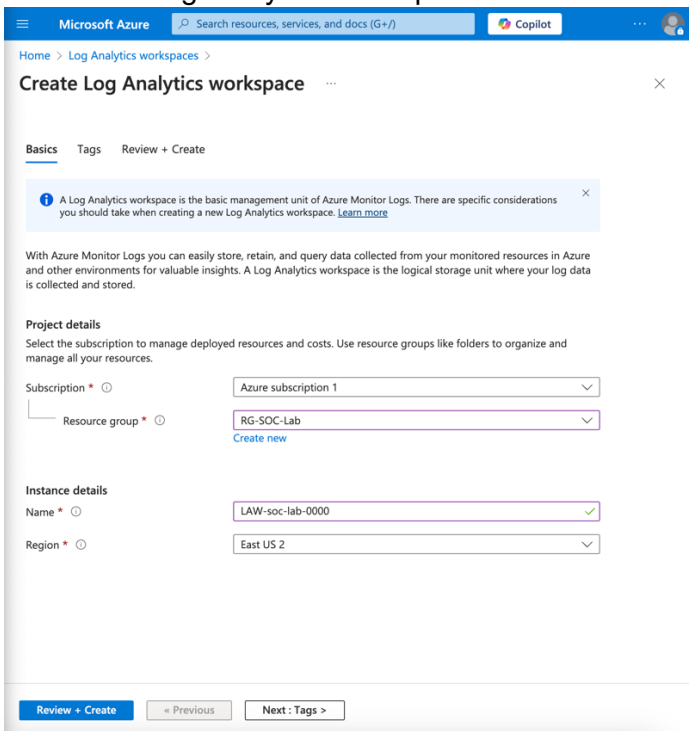




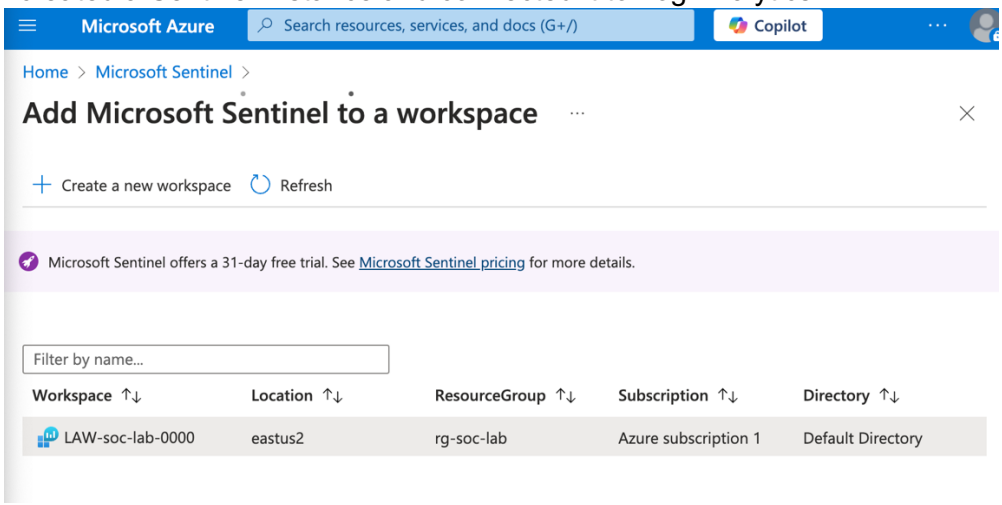
- Next, I created a central log repository called a LAW in Azure to forward the logs to.

Part 4. Log Forwarding and KQL

- I created a Log Analytics Workspace

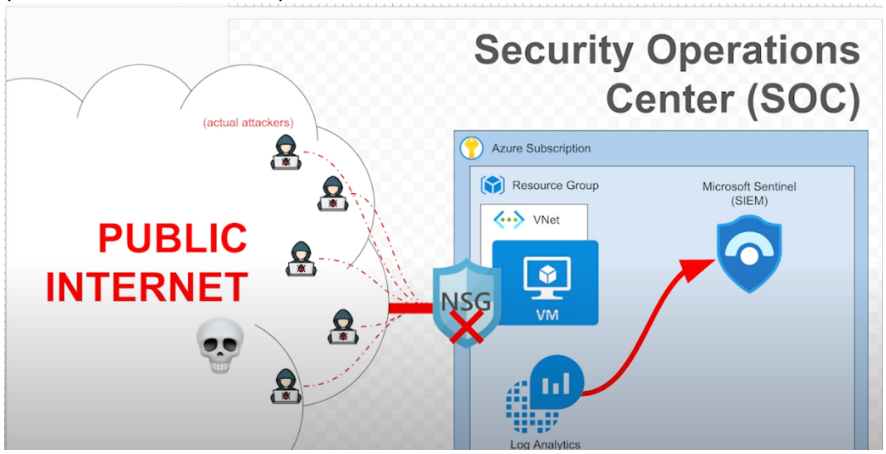


- I created a Sentinel Instance and connected it to Log Analytics

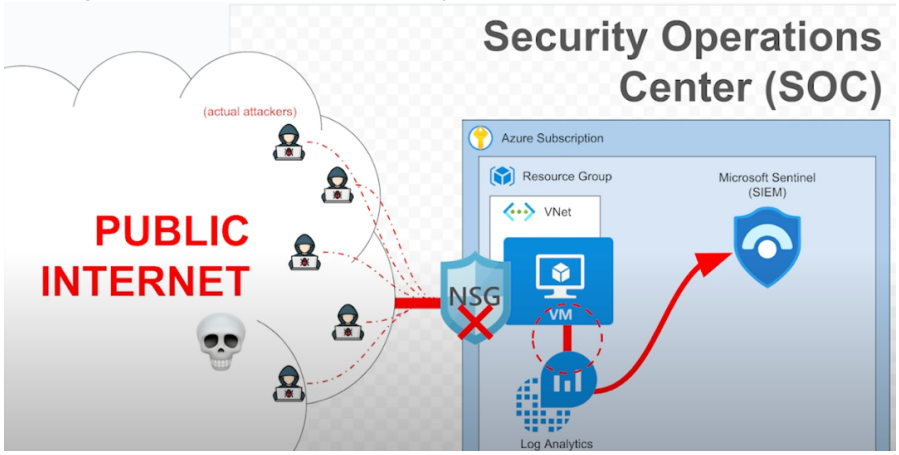


-

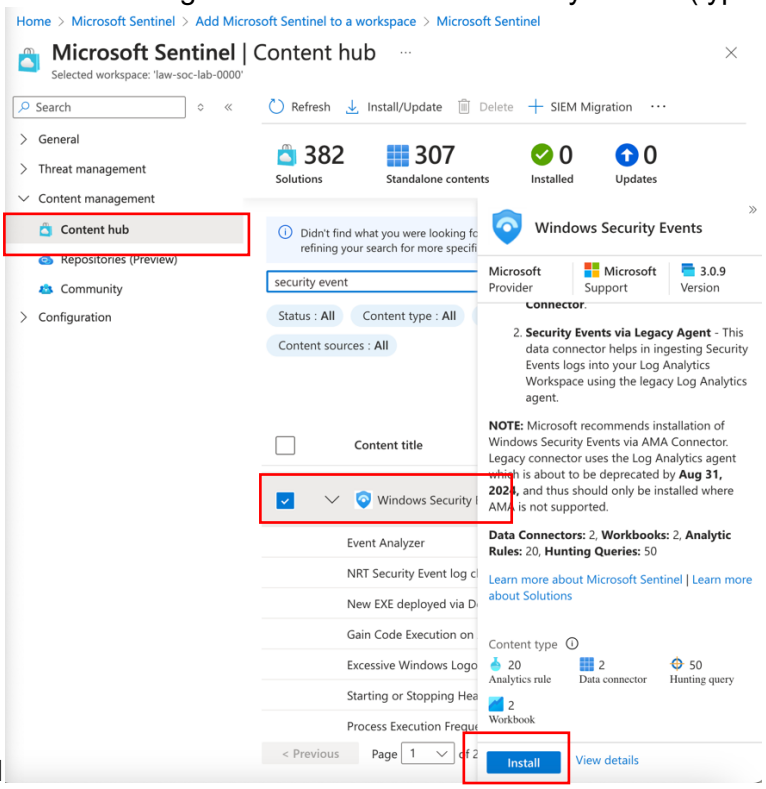
- (observe architecture)



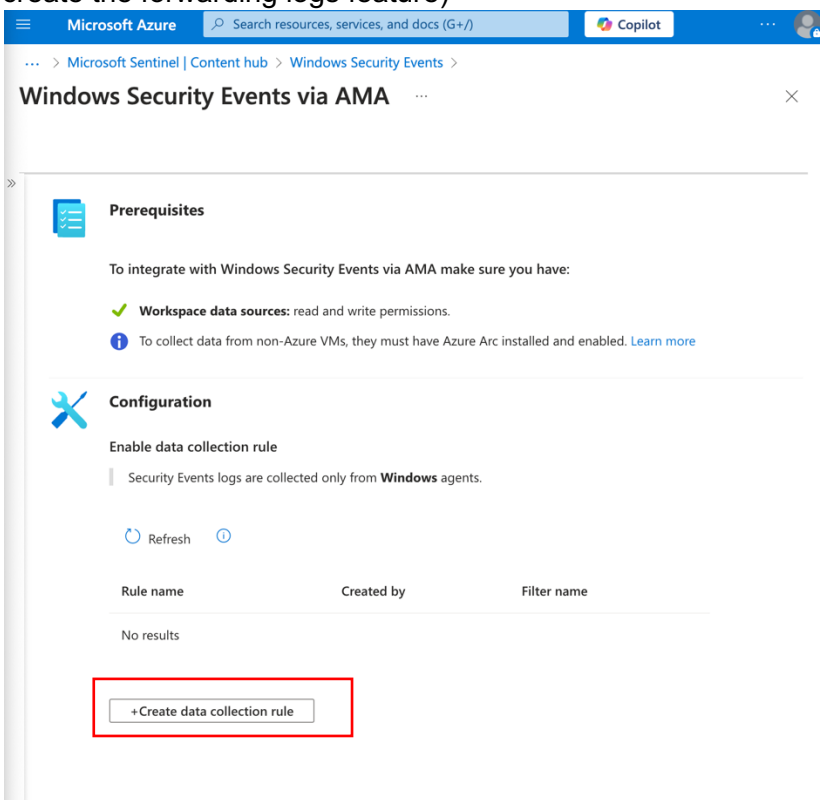
- I configured the “Windows Security Events via AMA” connector



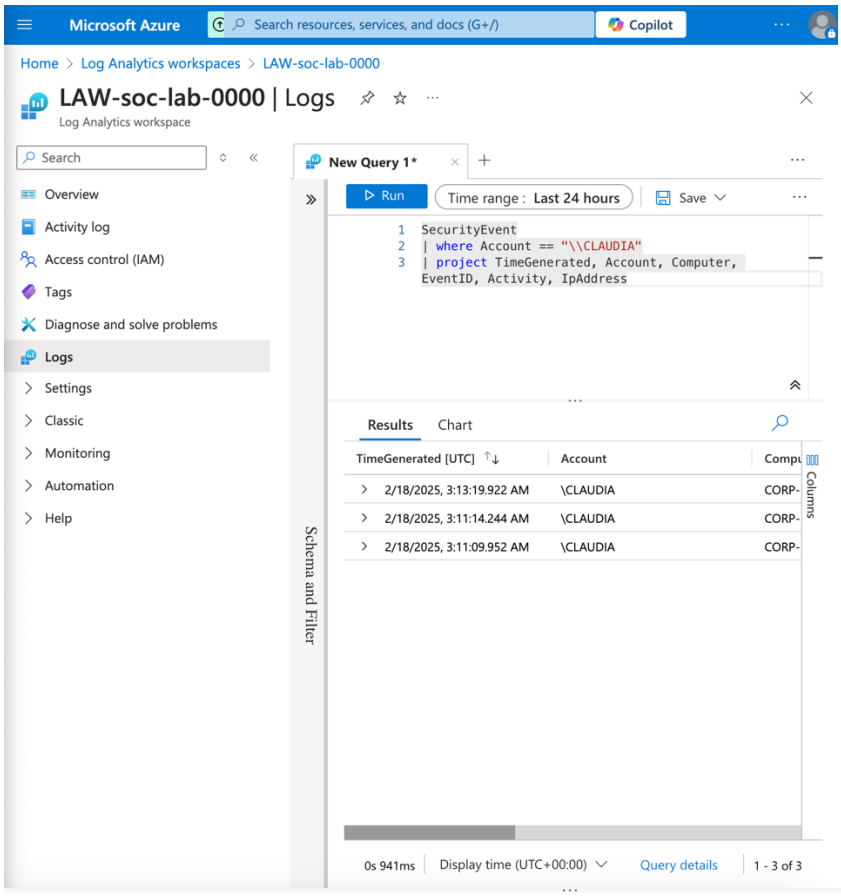
- Within Sentinel, I accessed: Content Management<Content Hub<Security Events (typed within search bar)< Hit install



- I created the DCR within Sentinel and watched for extension creation (I used this to create the forwarding logs feature)



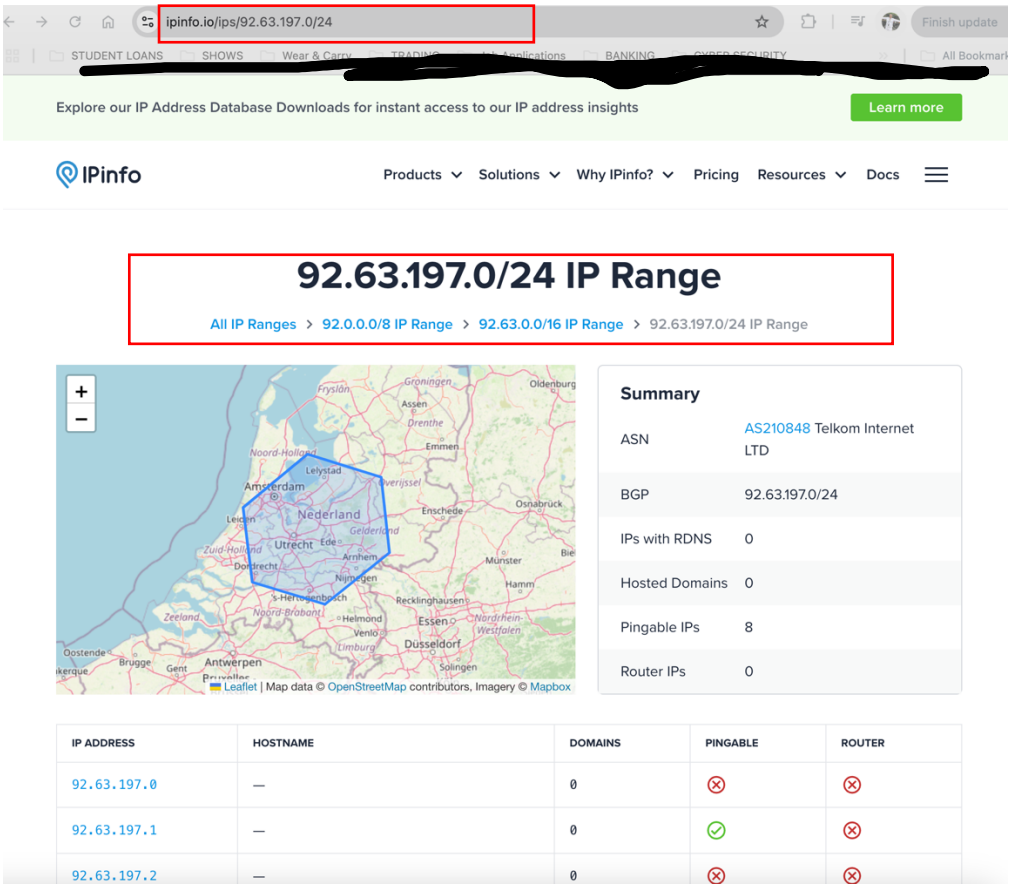
- I queried for logs within the LAW

- 

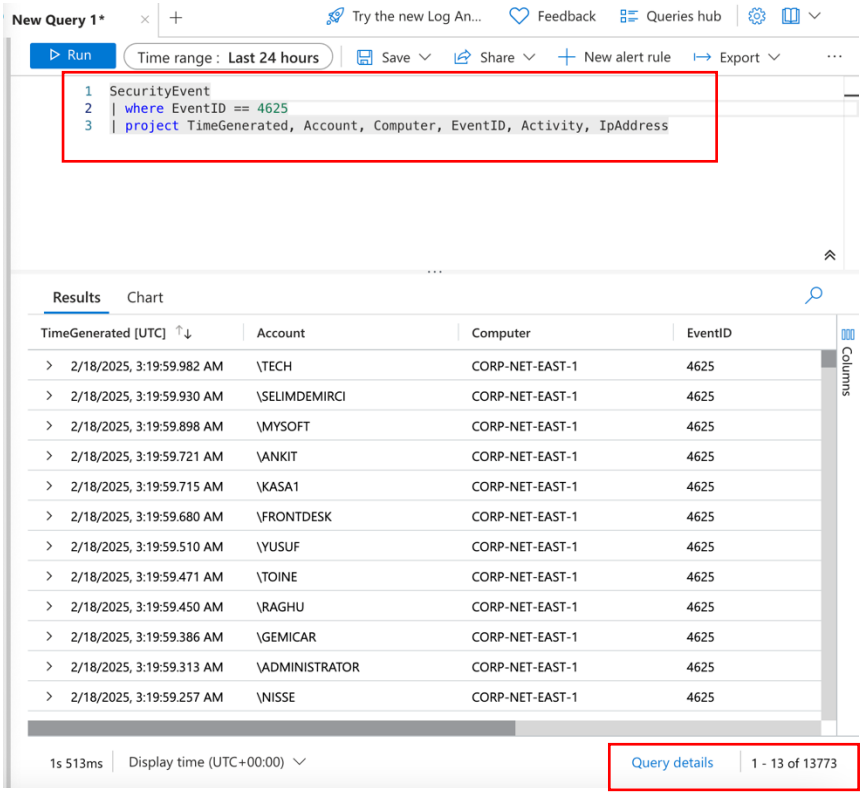
Results Chart

Account	Computer	EventID	Activity	IpAddress
\CLAUDIA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	92.63.197.9
\CLAUDIA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	94.102.52.73
\CLAUDIA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107

- I looked up the IP Address (92.63.197.9), and I found this was a person from the Netherlands trying to log in to my network.



- I also found that there are about 13,000 failed login attempts on my VM.



- I can now query the Log Analytics workspace as well as the SIEM sentinel directly, which I did soon.

Part 5. Log Enrichment and Finding Location Data

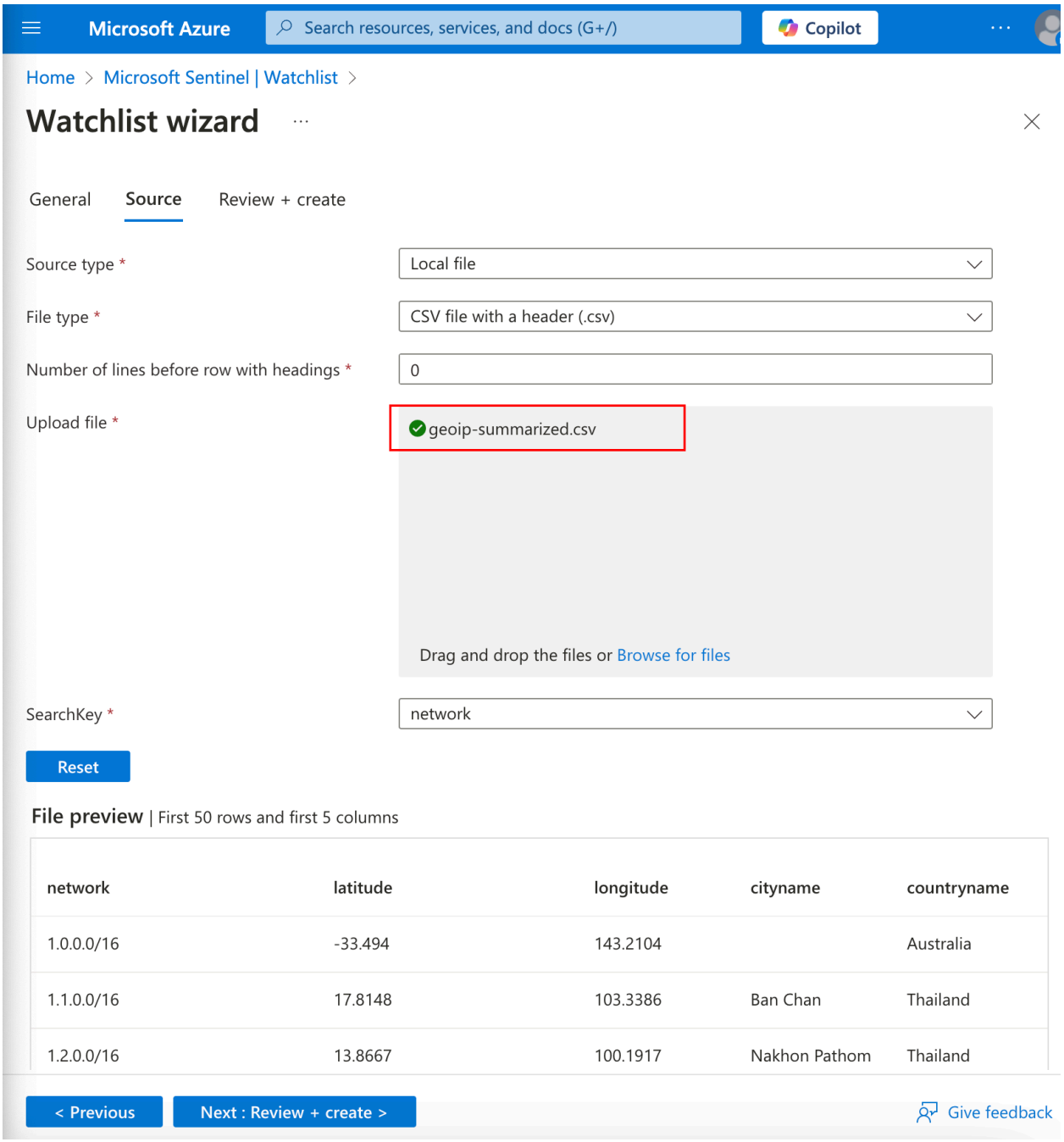
I observed the SecurityEvent logs in the Log Analytics Workspace; there is no location data, only IP address, which I can use to derive the location data.

I imported a spreadsheet (as a “Sentinel Watchlist”) which contains geographic information for each block of IP addresses.

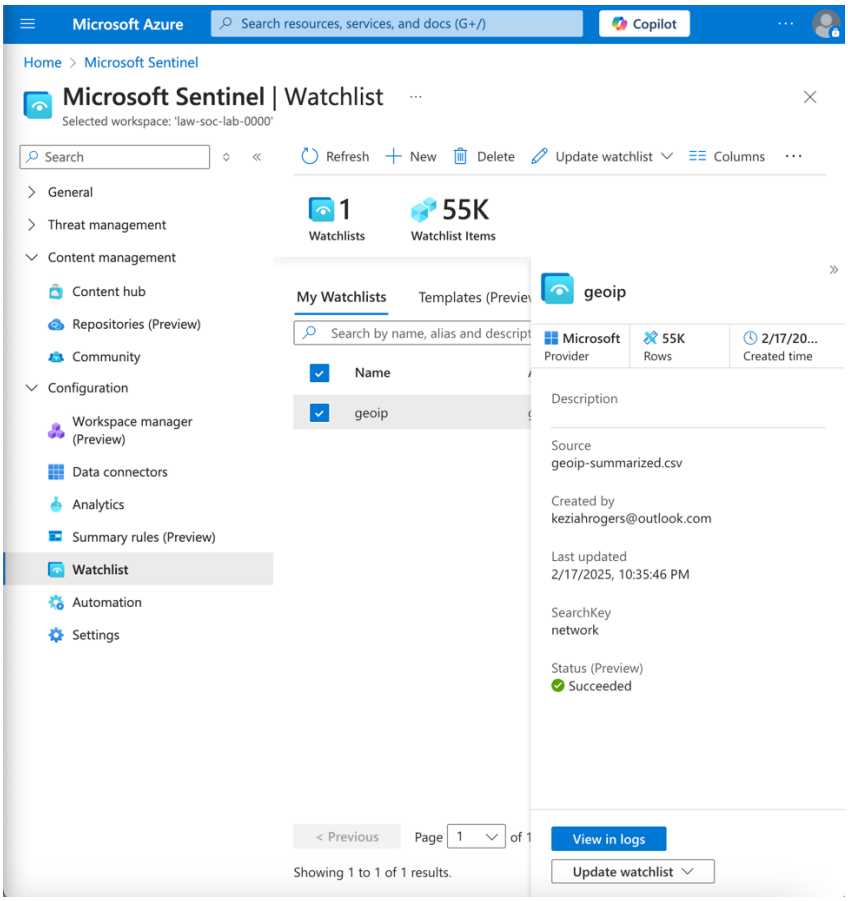
Downloaded from: geoip-summarized.csv

Within Sentinel, I create the watchlist:

Name/Alias: geoip
Source type: Local File
Number of lines before row: 0
Search Key: network



I allowed the watchlist to fully import, there was about 54,000 rows.



(observe architecture)

I observed that the logs now have geographic information, so I can see where the attacks are coming from

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent
    | where IpAddress == <attacker IP address>
    | where EventID == 4625
    | order by TimeGenerated desc
    | evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
WindowsEvents
```

- I put my geoip file into Sentinel, but mainly in my Log Analytics Workspace/log repository.

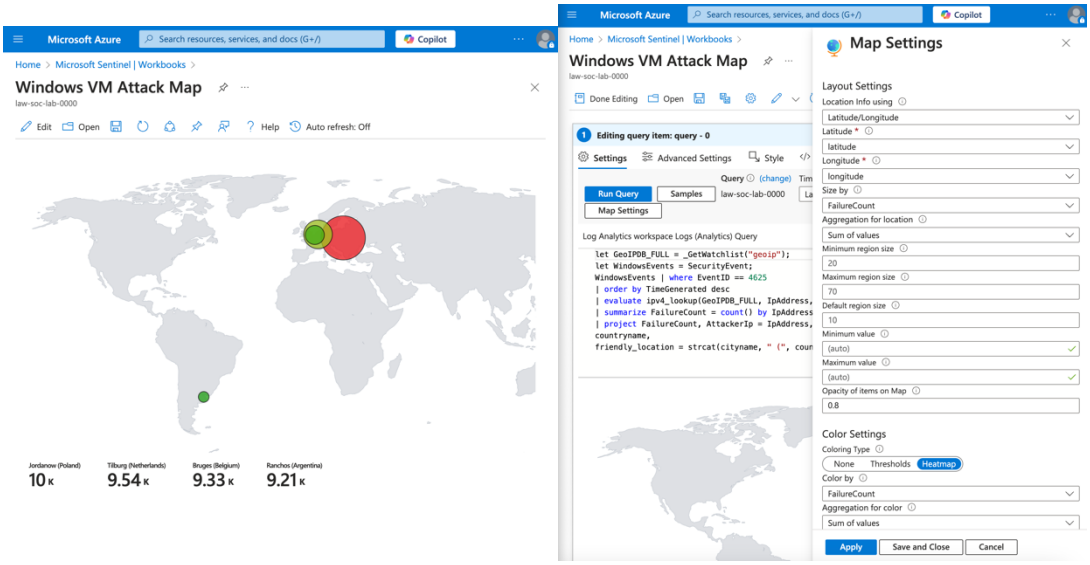
(observe architecture)

Part 6. Attack Map Creation

- Within Sentine, I created a new Workbook
- I deleted the prepopulated elements and added a “Query” element
- I went to the advanced editor tab, and pasted the JSON

Workbook (Attack map):
map.json

- I observed the query
- I observed the map settings
- I observed the map



Home > Microsoft Sentinel | Workbooks >

Windows VM Attack Map

law-soc-lab-0000

Done Editing | Open | Help

1 Editing query item: query - 0

Settings | Advanced Settings | Style | Advanced Editor

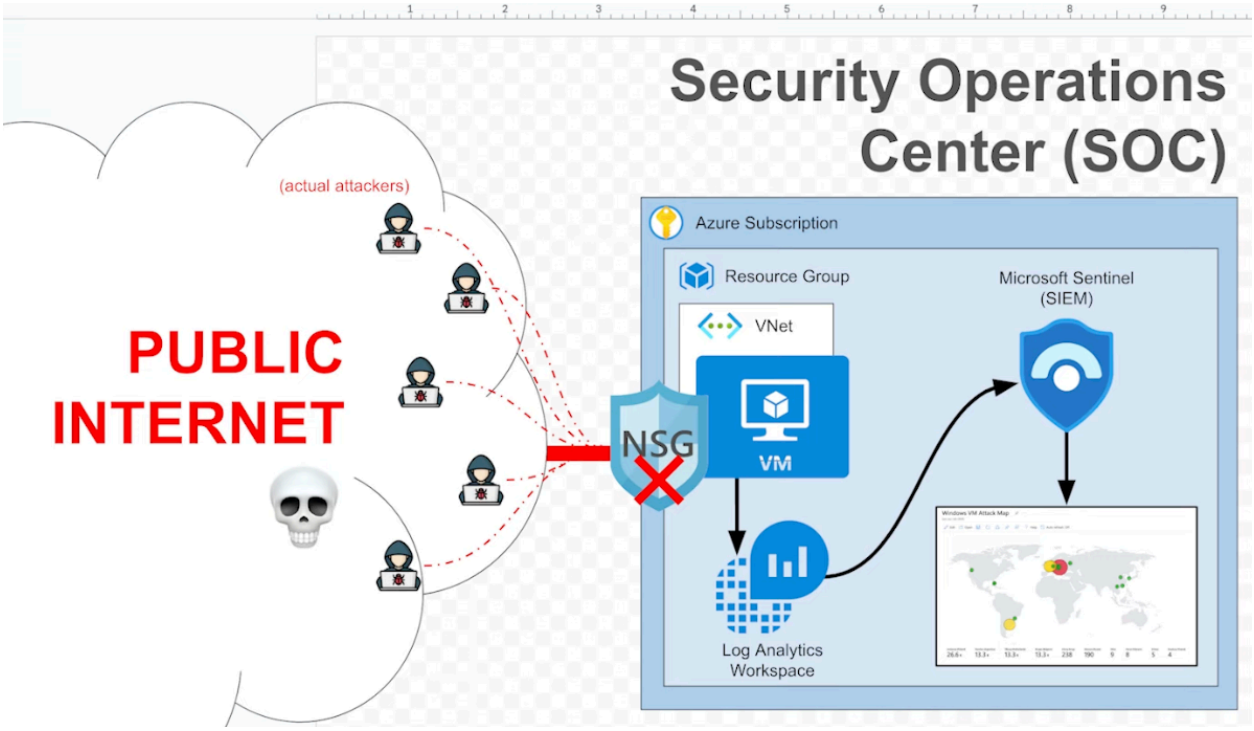
Query (change) | Time Range | Visualization | Size

Run Query | Samples | law-soc-lab-0000 | Last 30 days | Map | Full

Map Settings

Log Analytics workspace Logs (Analytics) Query — Query help

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent;
WindowsEvents | where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)
| summarize FailureCount = count() by IpAddress, latitude, longitude, cityname, countryname
| project FailureCount, AttackerIp = IpAddress, latitude, longitude, city = cityname, country =
countryname,
friendly_location = strcat(cityname, " (", countryname, ")");
```


Security Operations Center (SOC)
(actual attackers)
PUBLIC INTERNET
Azure Subscription
Resource Group
VNet
NSG
VM
Microsoft Sentinel (SIEM)
Log Analytics Workspace