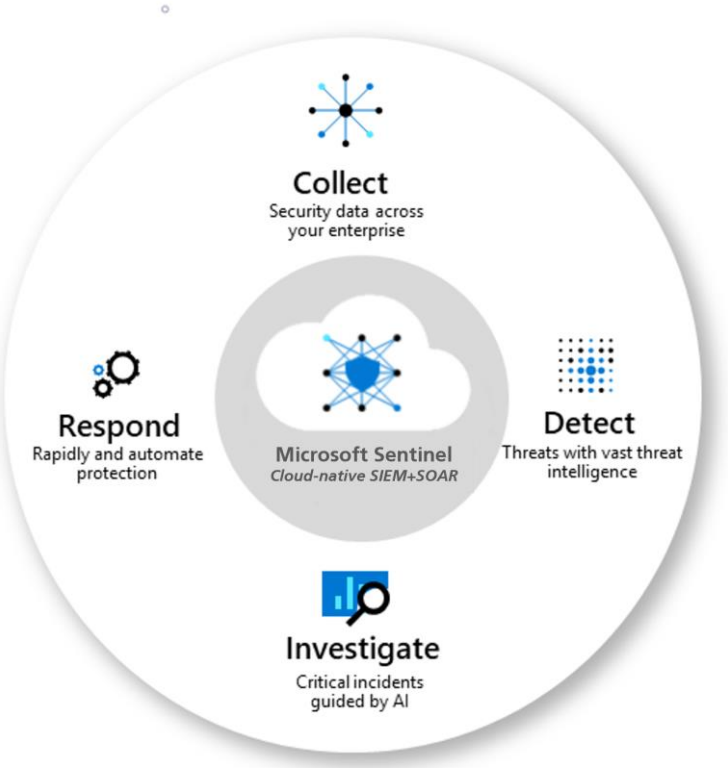
Microsoft Sentinel SIEM Lab

By Tomiwa Oladejo



Project Overview:

The focus of this lab was to leverage Microsoft Azure services to design and implement a virtual network environment, and simulate a basic Security Information and Event Management (SIEM) system utilising Microsoft Sentinel.

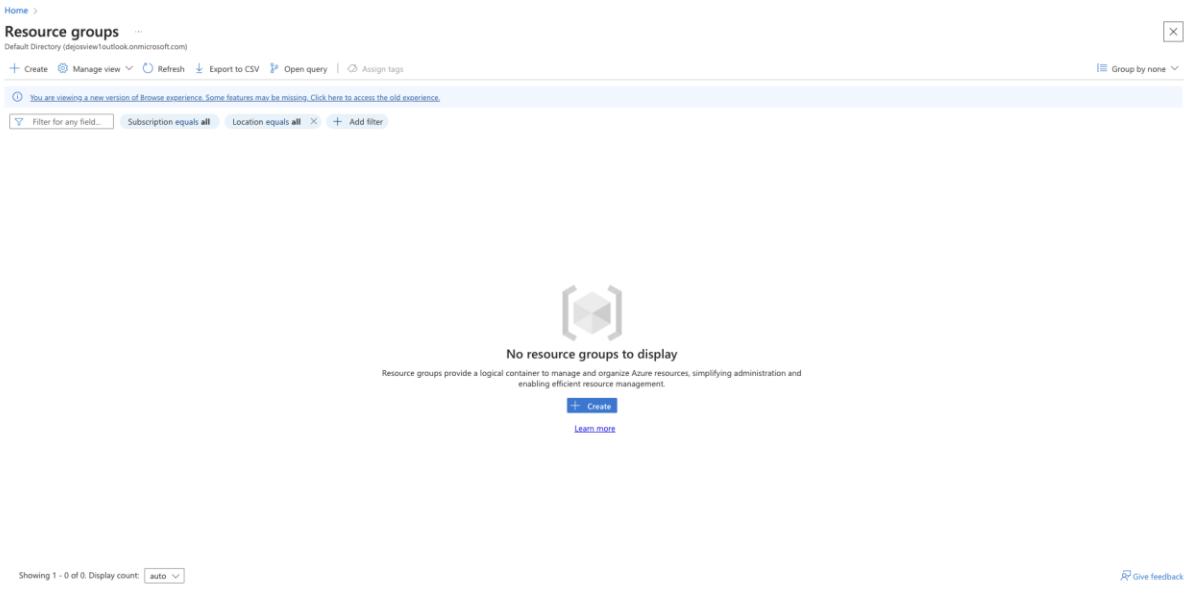
Key components:

- Creating the Honey Pot (Azure Virtual Machine)
- Reviewing Raw Logs on Virtual Machine
- Creating Log Repository
- Connecting Virtual Machine to Log Analytics Workspace
- Querying and inspecting Log Repository with KQL
- Uploading Geolocation Data to SIEM
- Attack Map Creation

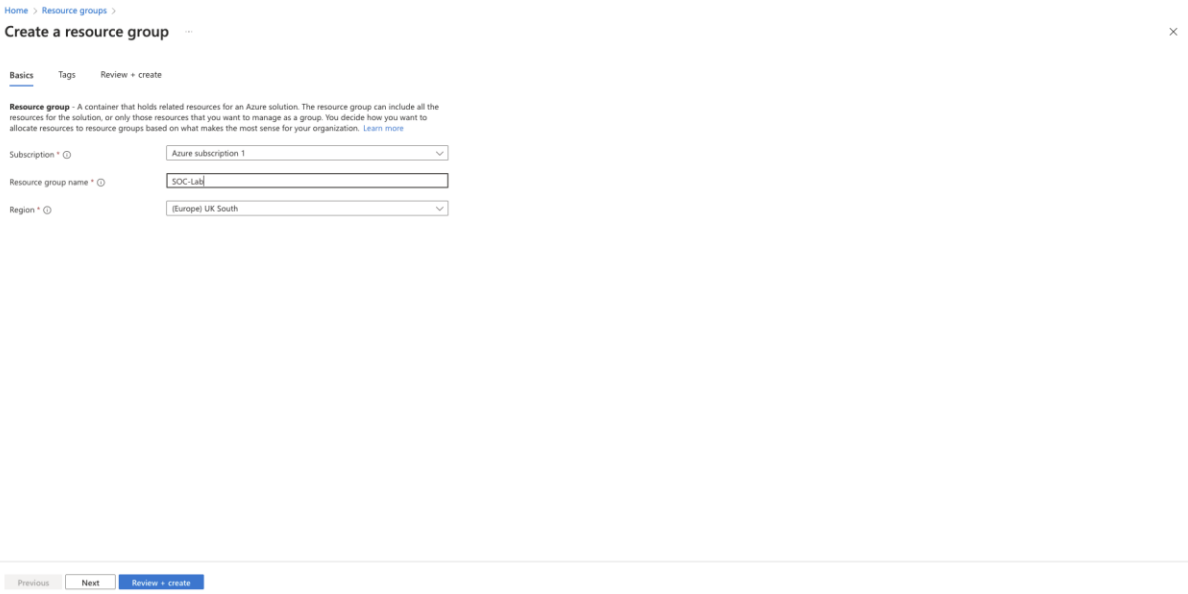
Create the Honey Pot (Azure Virtual Machine)

Although part of the objective in this lab is to create a honey pot, there are a few prerequisites that need to be set up. These include elements such as the resource group and network, which need to be put in place for the allocation and connectivity purposes.

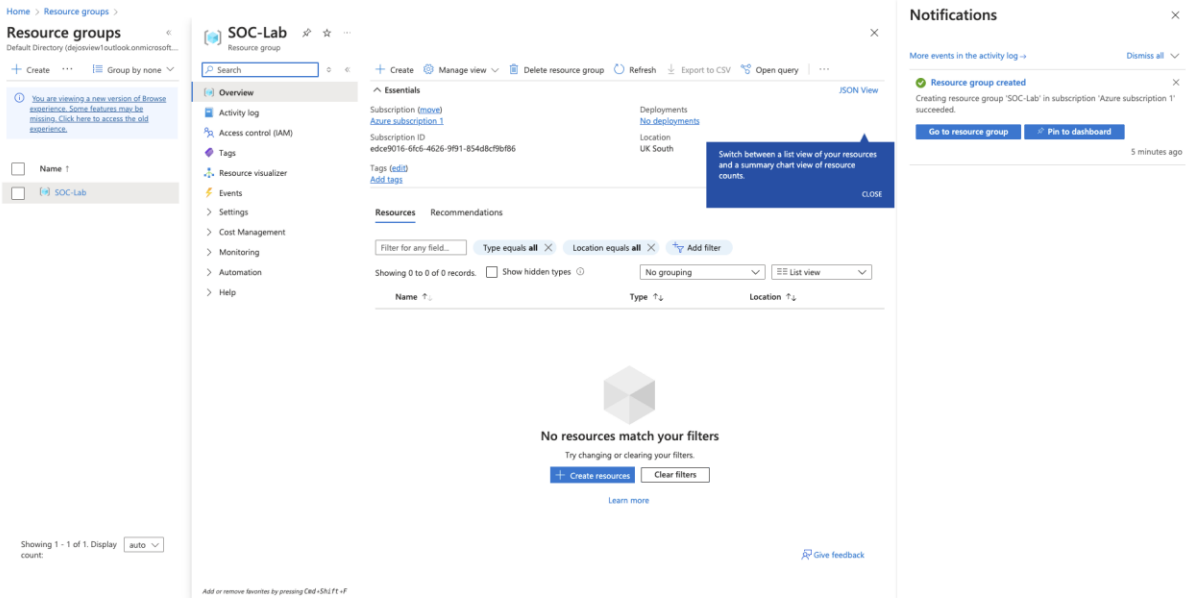
1) To start off the lab, I created a resource group. Resource groups act as folders in the cloud, aiding the management and organisation of resources, in turn streamlining administration and enabling efficient resource management. The resource group service can be located using the navigation bar, which will be useful as this lab unfolds, helping finding other services easier.



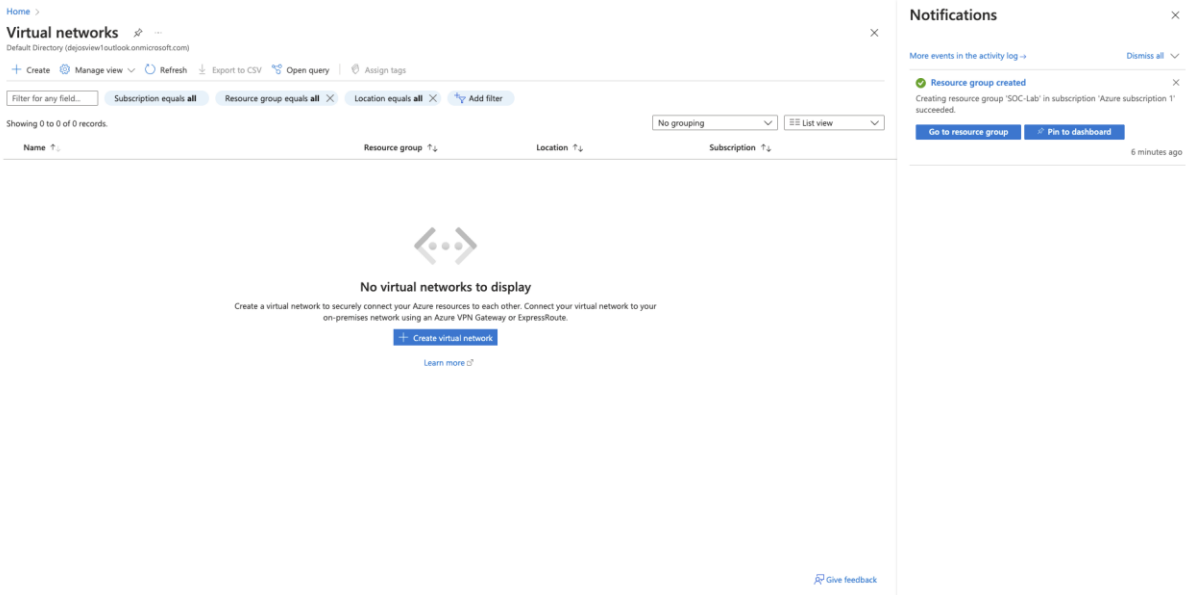
2) After selecting create, fill in the resource group name and choose your preferred region. Then simply click review and create.



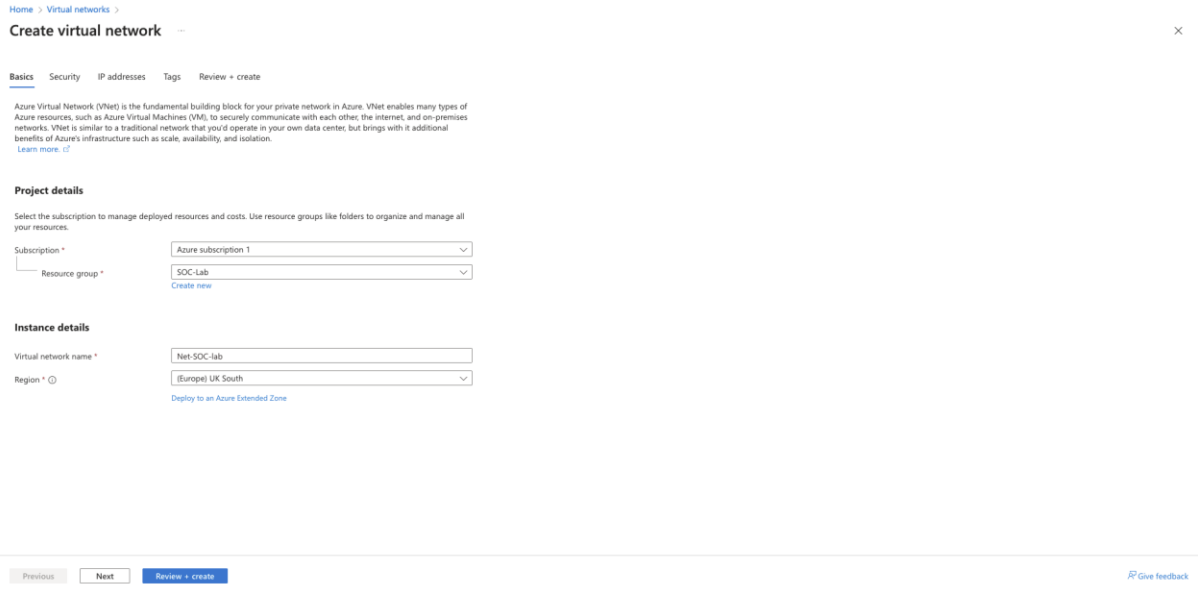
3) You can then return back to the resource group page to confirm it has been created.



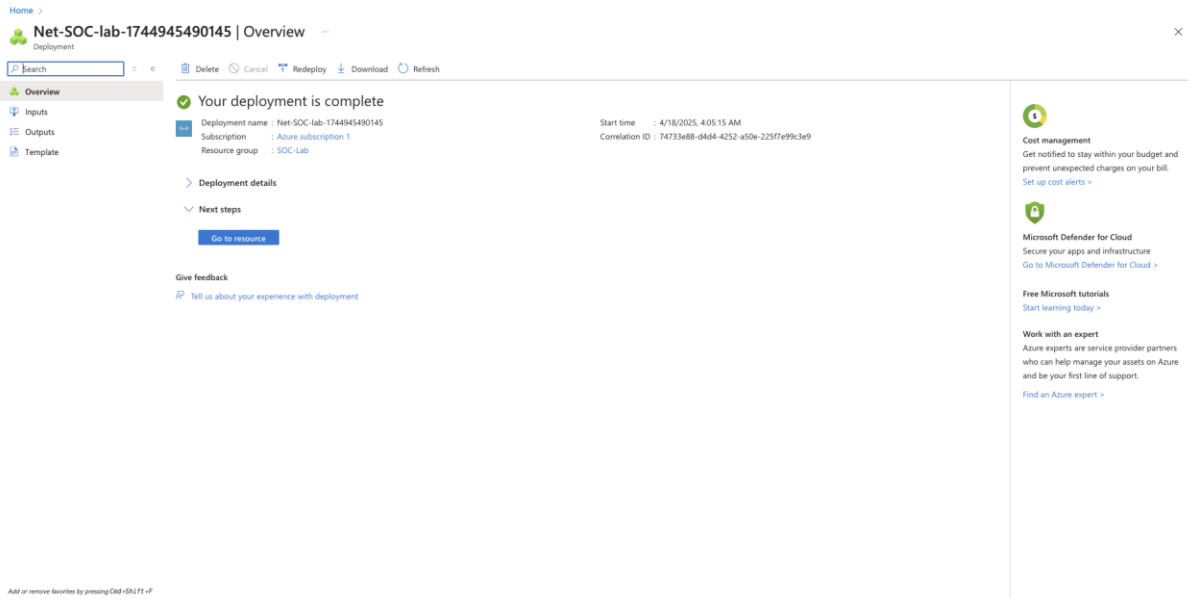
4) Search for the virtual networks service in using the navigation bar and click create.



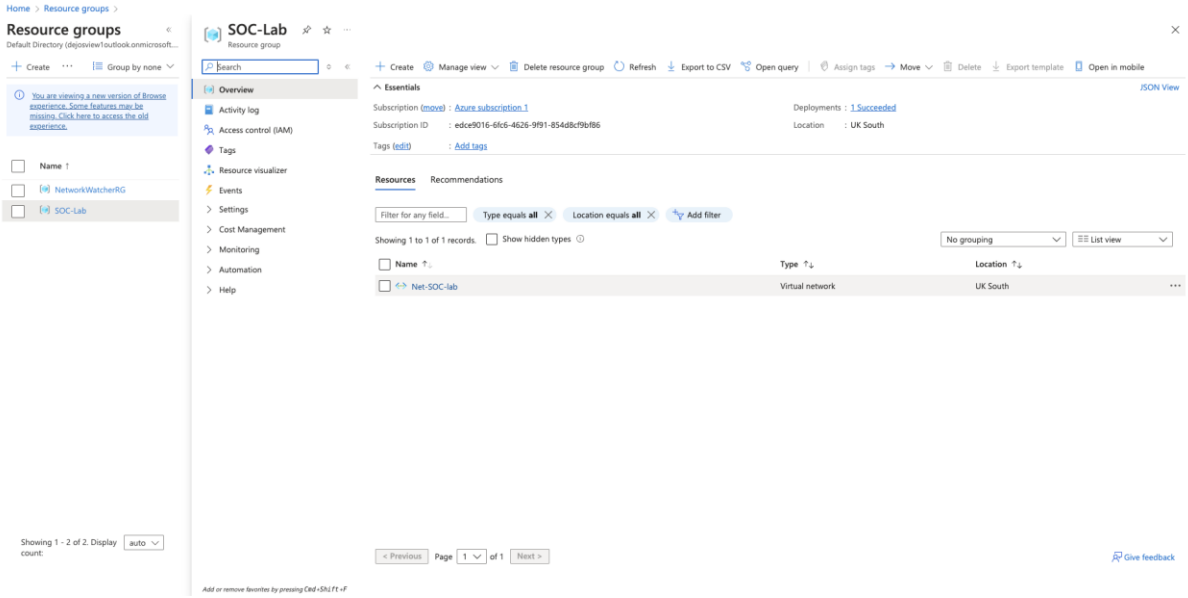
5) On this page, select the resource group that has been previously created. Additionally, input a name for the virtual network and select the region. The other tabs presented to you can remain untouched, as there is not anything required to be changed, and an IP address is created by default.
Proceed to click review + create and then do not forget to click create afterwards to confirm the creation.



6) It may take a minute for the creation to complete. As you can see in the image below, a virtual network has been generated with a subnet inside:

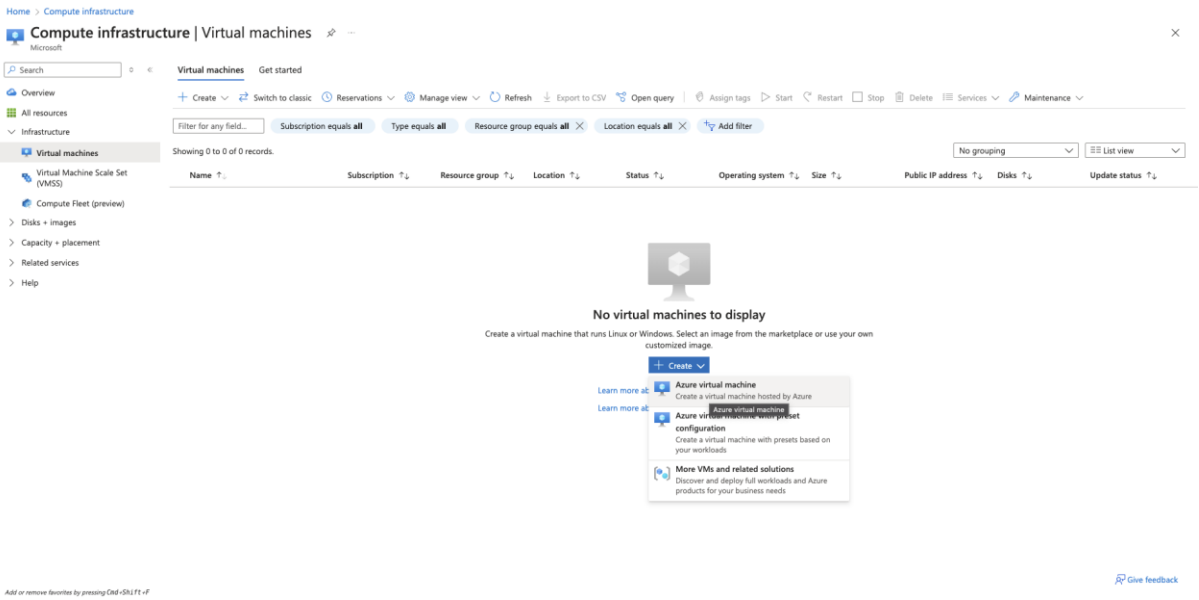


7) If you navigate back to resource groups, you should see a group named “NetworkWatcherRG” has been automatically created. The original resource group you created should also contain the network that has just been created.



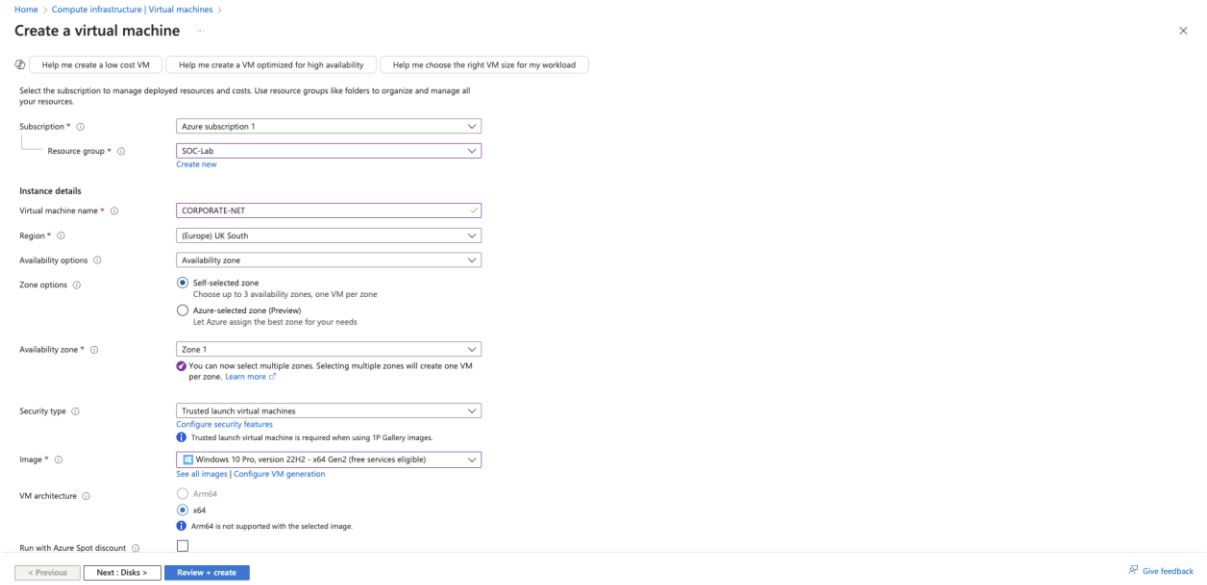
8) Next is the creation of the virtual machine, which will be acting as the honey pot. The purpose of a honey pot is to lure in attackers, through the use of deliberate security vulnerabilities. It aids the collection of information that can be used to understand existing threats to businesses.

After clicking “Create”, you will be presented with 3 options to choose from.



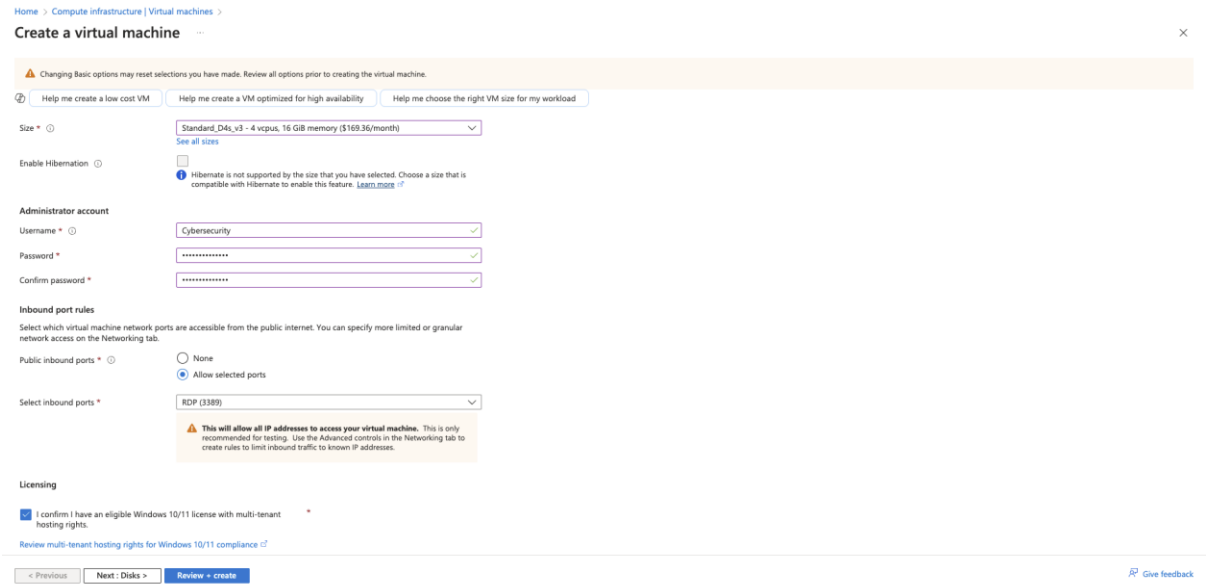
For this lab, I will be using the first option on the list - “Azure virtual machine”.

9) Select the correct subscription, resource group, virtual machine name and region. For the image, I will be using Windows 10 Pro.

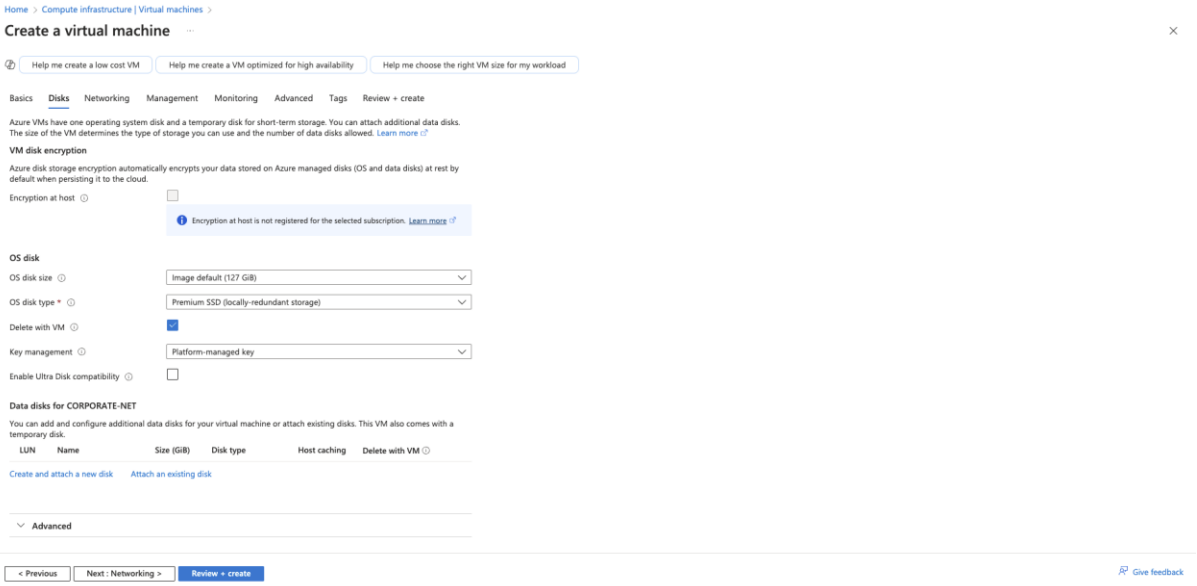


10) The selected size utilised for this lab is Standard_D4s_v3 - 4 vcpus. When inputting the username and password for the administrator account, ensure you take note of the details. Although there is a forgotten password option in settings, it would be more convenient to remember. The password does not have to necessarily be too complicated.

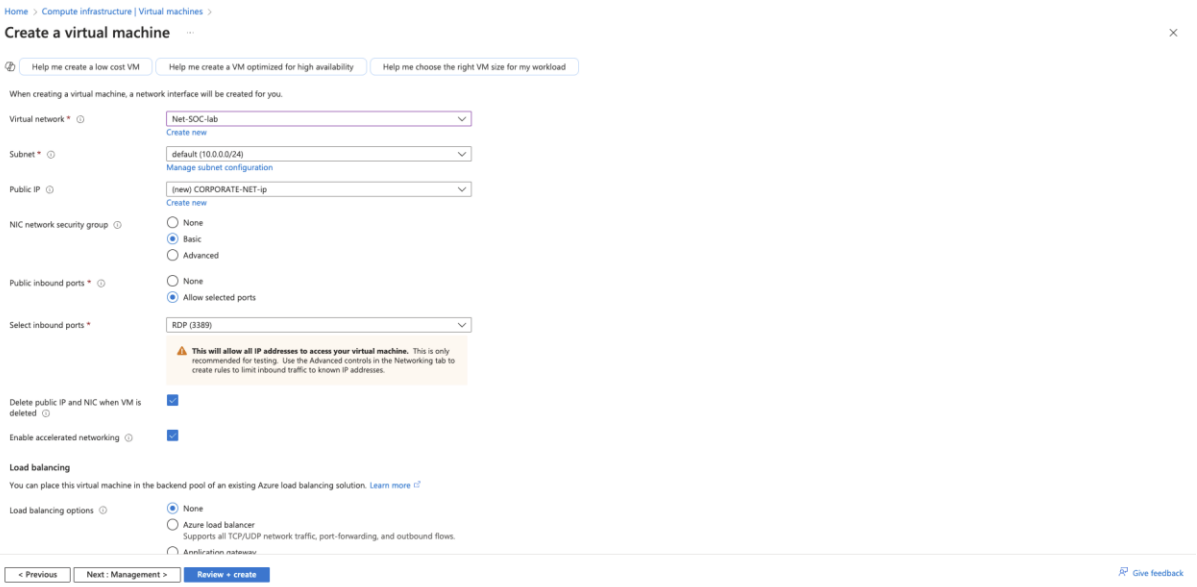
Make sure to confirm your license before proceeding to Disks.



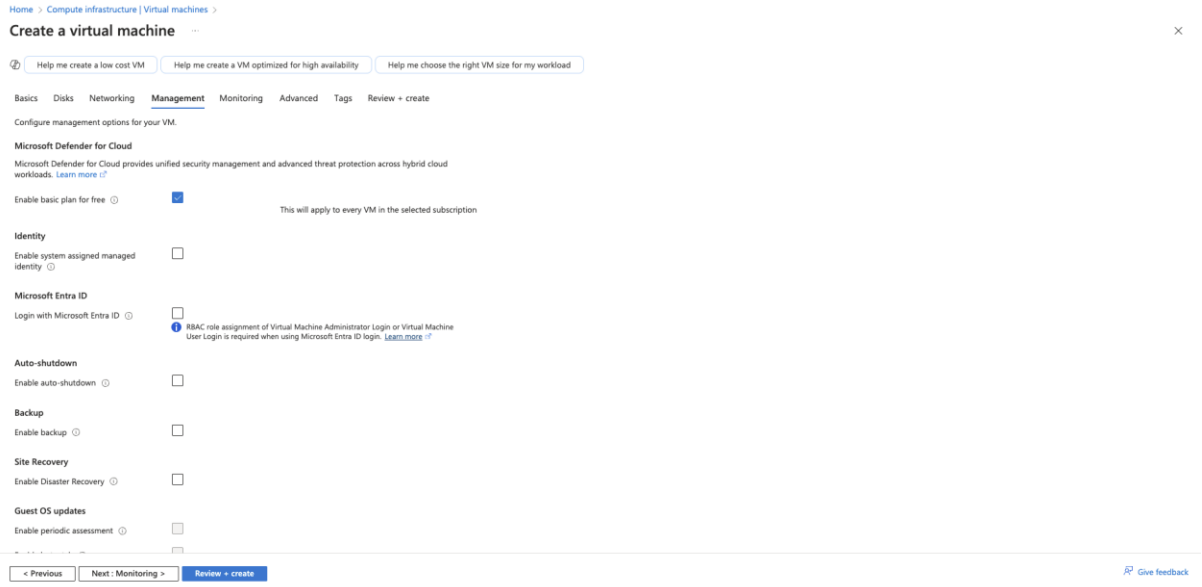
11) I left everything on the disk page as default.



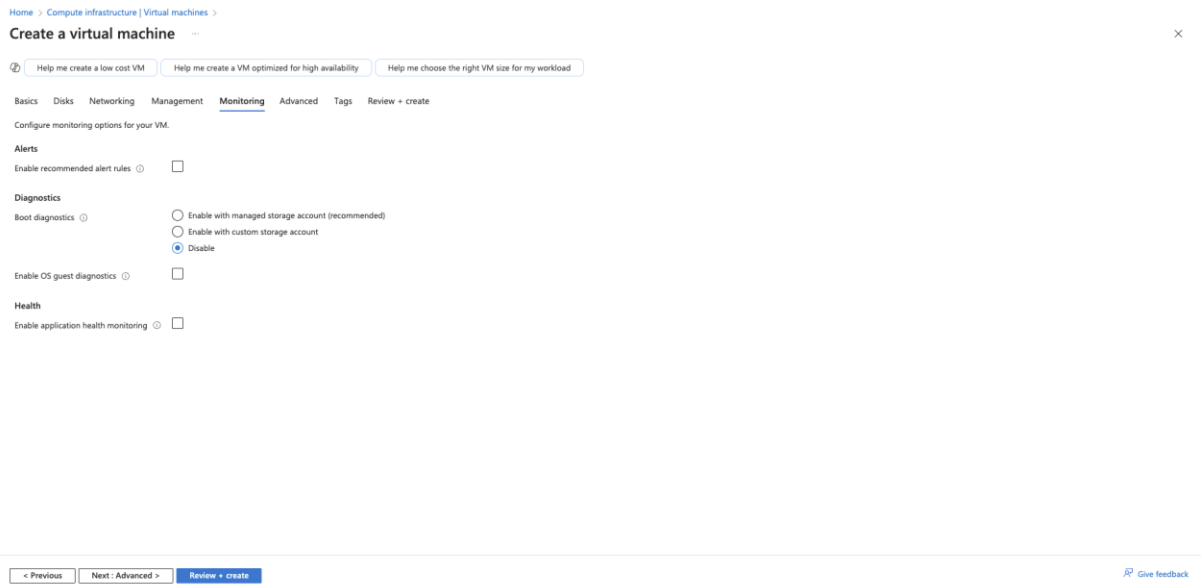
12) Select the virtual network you created, and you can also tick the “Delete public IP and NIC when VM is deleted” box.



13) The management page does not require any changes.

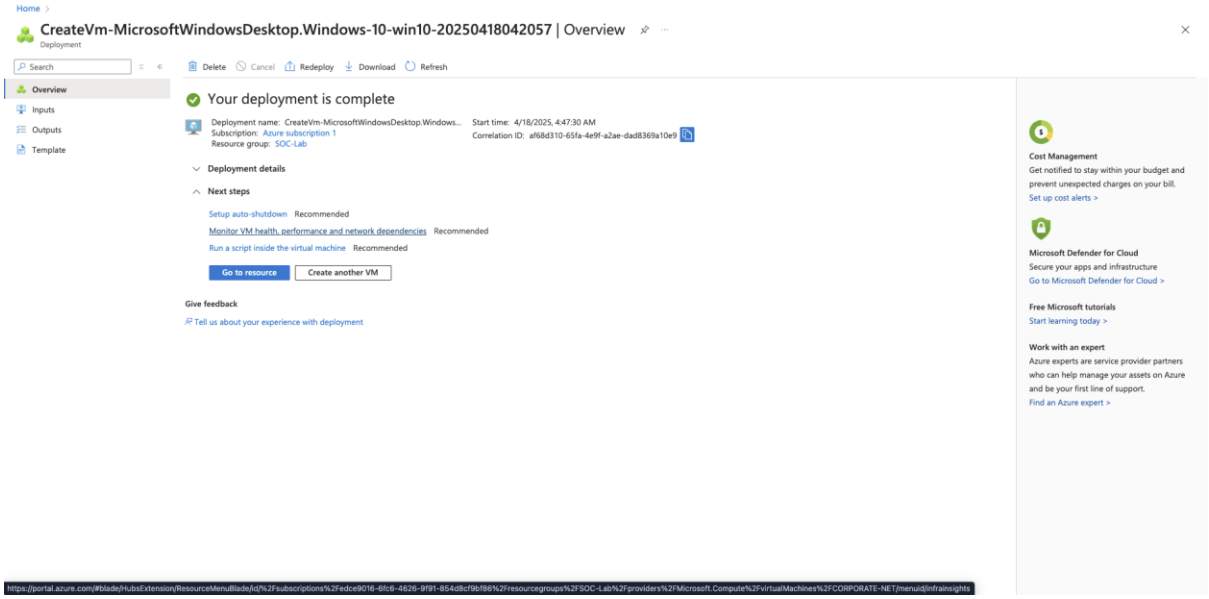


14) I chose to disable boot diagnostics.

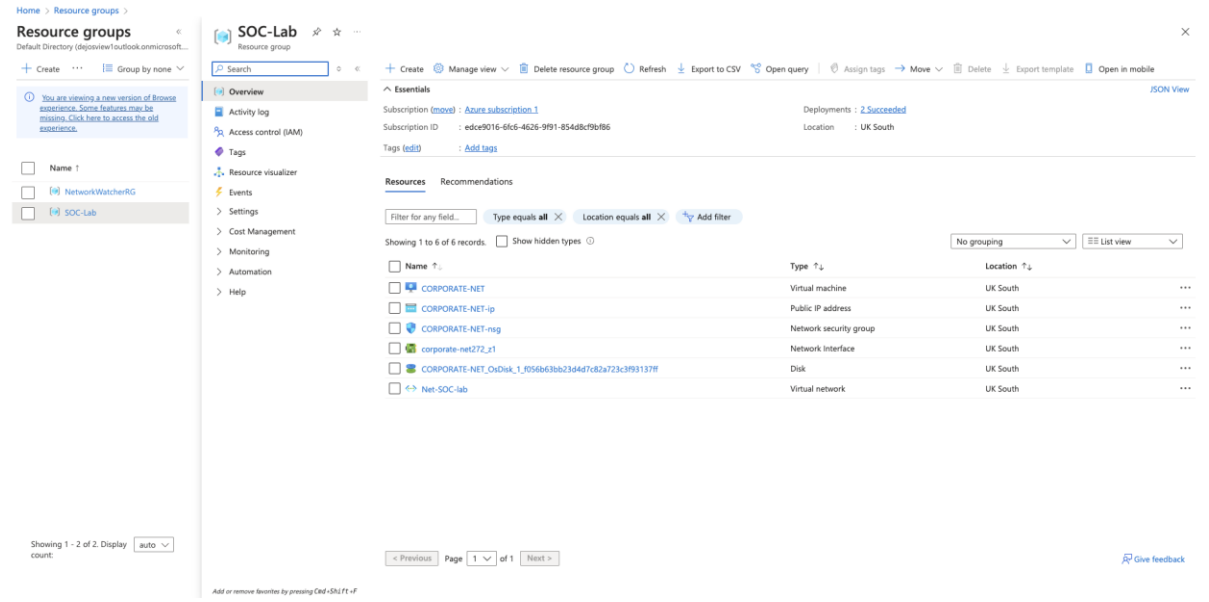


15) From there I progressed through advanced and tags as nothing I saw required changes. Once you click review and create, you need to once again click create to confirm the creation after the virtual machine has passed the review.

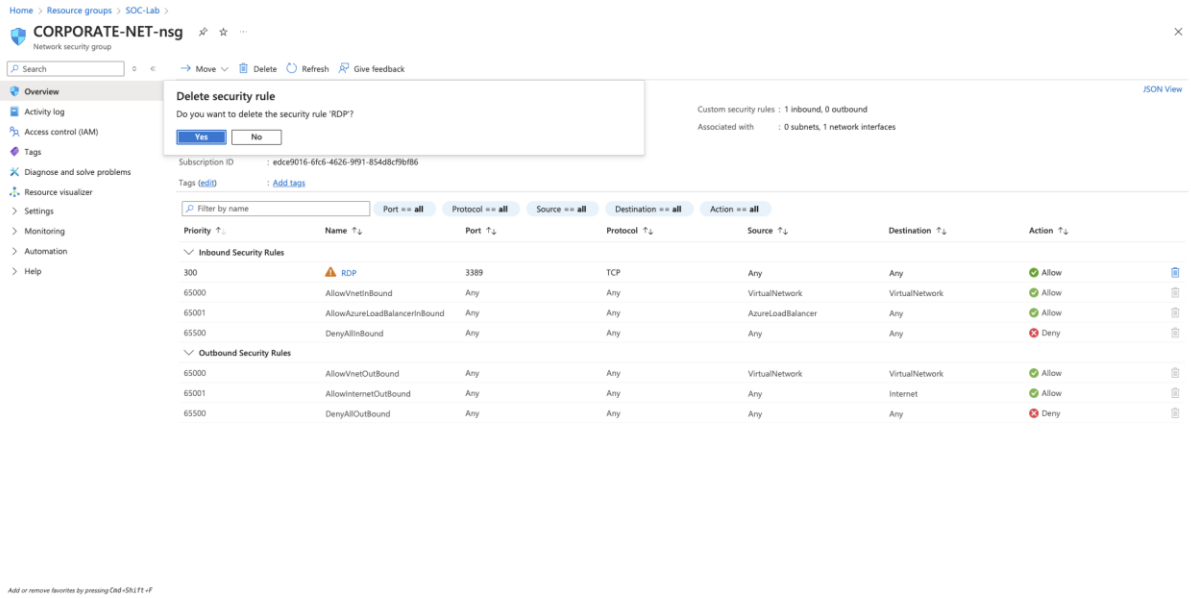
Once the deployment is complete a confirmation screen should be shown:



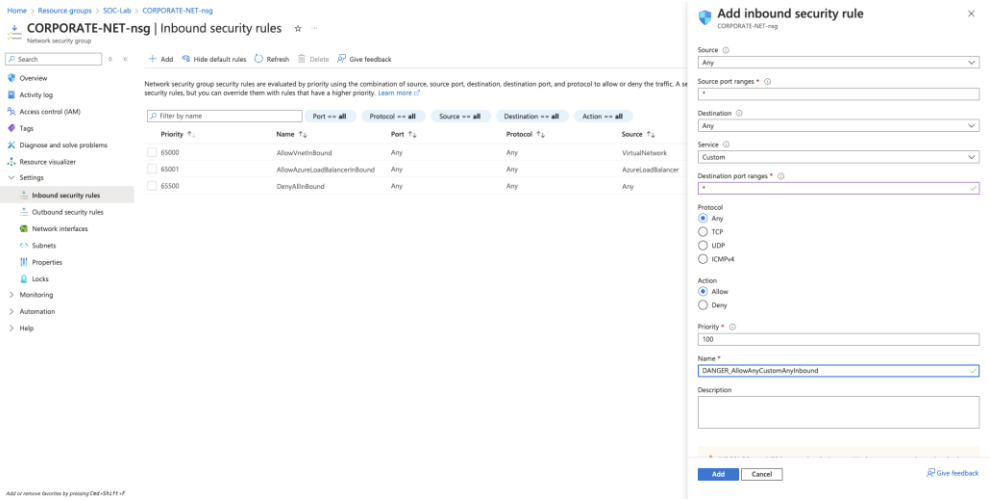
16) If you navigate to the resource groups, you should find the virtual machine has been added amongst the other materials. Observing the screenshot below, you can see the public IP address has been created alongside the virtual machine. Additionally, a network security group, network interface and disk have all been added into the resource group.

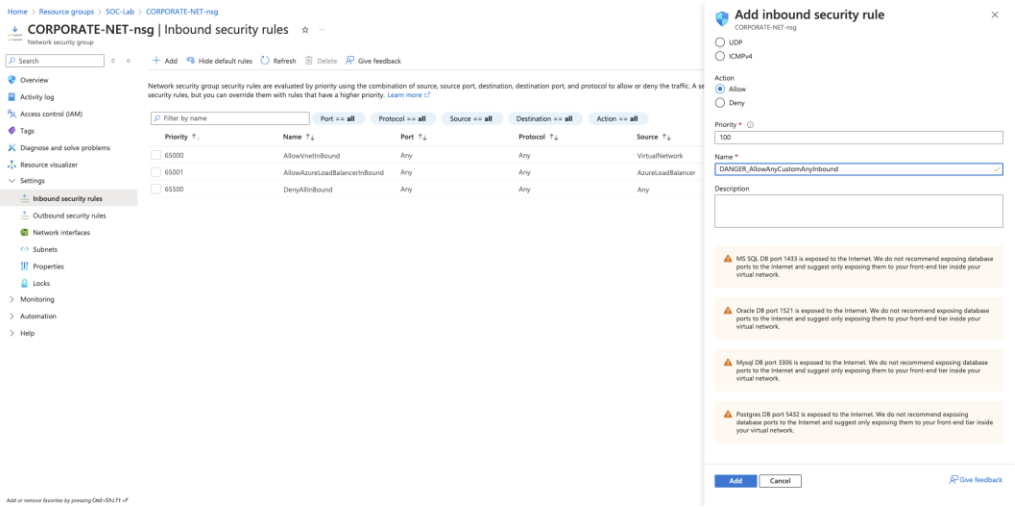


17) Now the network security group needs to be opened up to the internet. To achieve this, the firewall requires editing. The inbound rules control what can enter the virtual network from the public internet. Currently, the “RDP” rule is the only rule that allows traffic to attempt to login, but that can only be carried out through a remote desktop. Any other traffic sent to the network will get blocked as there are no rules that permit it. To alter this, the default RDP rule needs to be deleted.

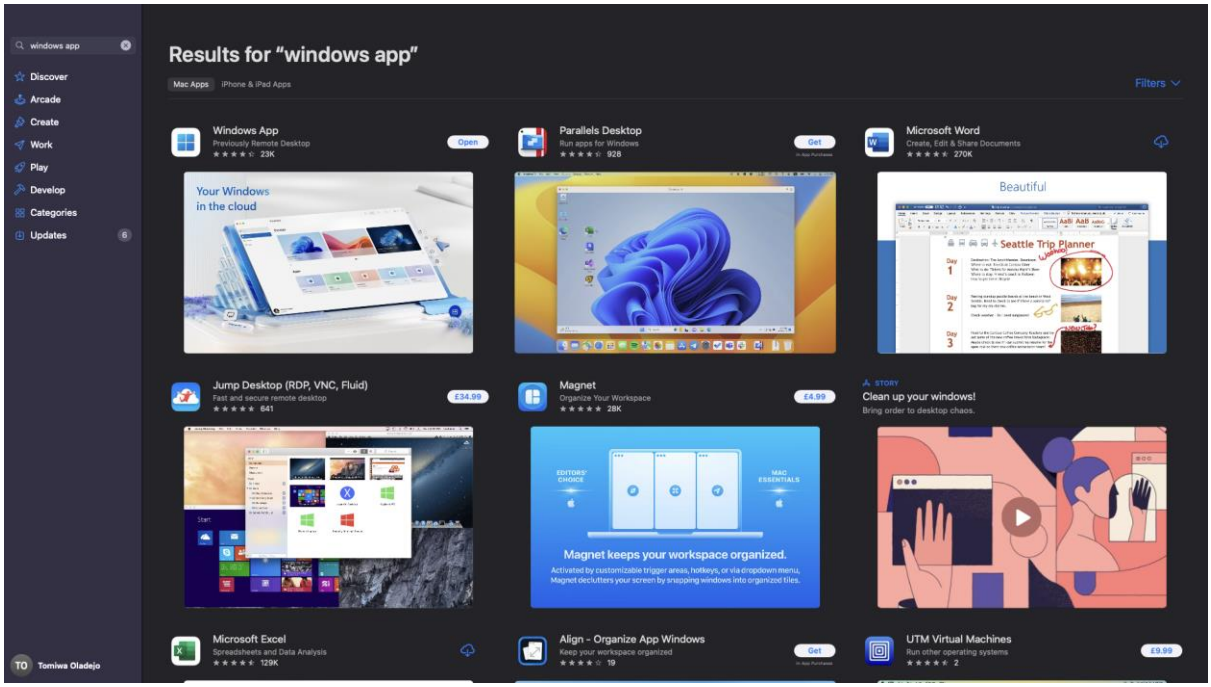


18) Subsequently, look to the left of the screen and navigate to settings > inbound security tools. Click add then proceed to input the settings shown in the images below.

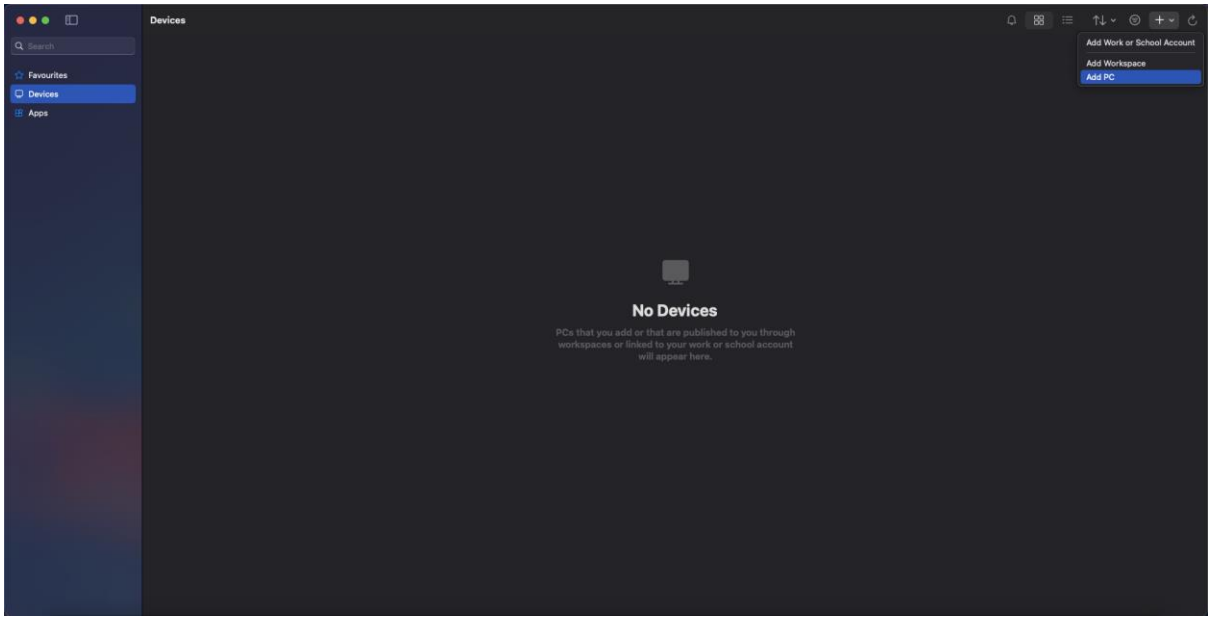




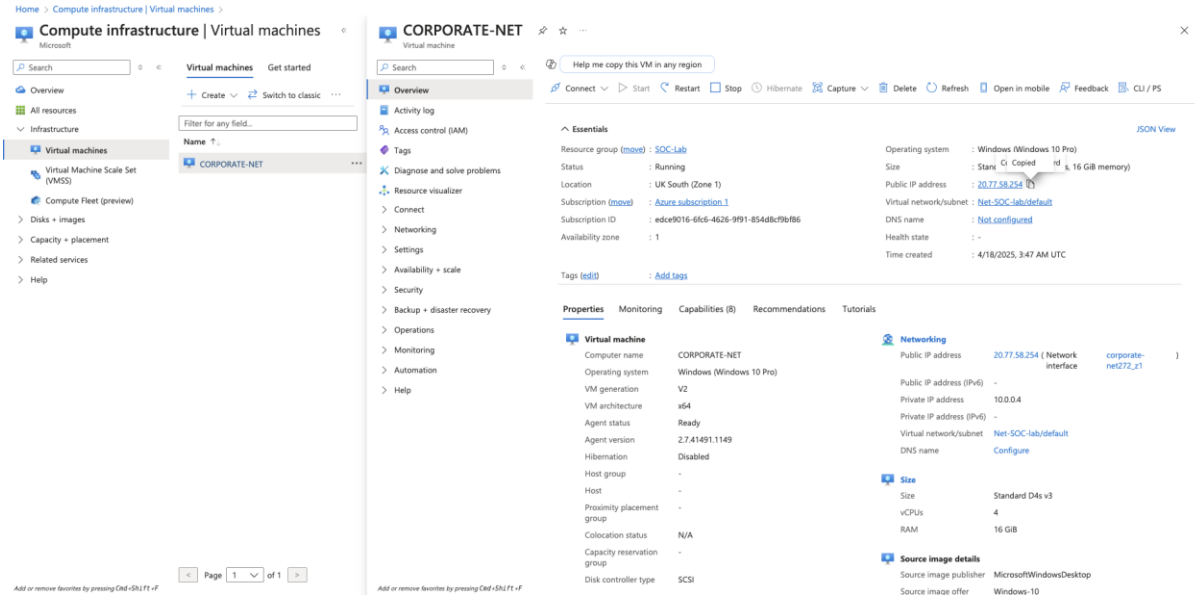
19) After configuring the security rule, we now want to disable the firewalls within the virtual machine. As I carried out this lab on Mac, I downloaded “Windows App” to access the virtual machine. However, if you are using windows you should be able to find a remote desktop through a quick search.

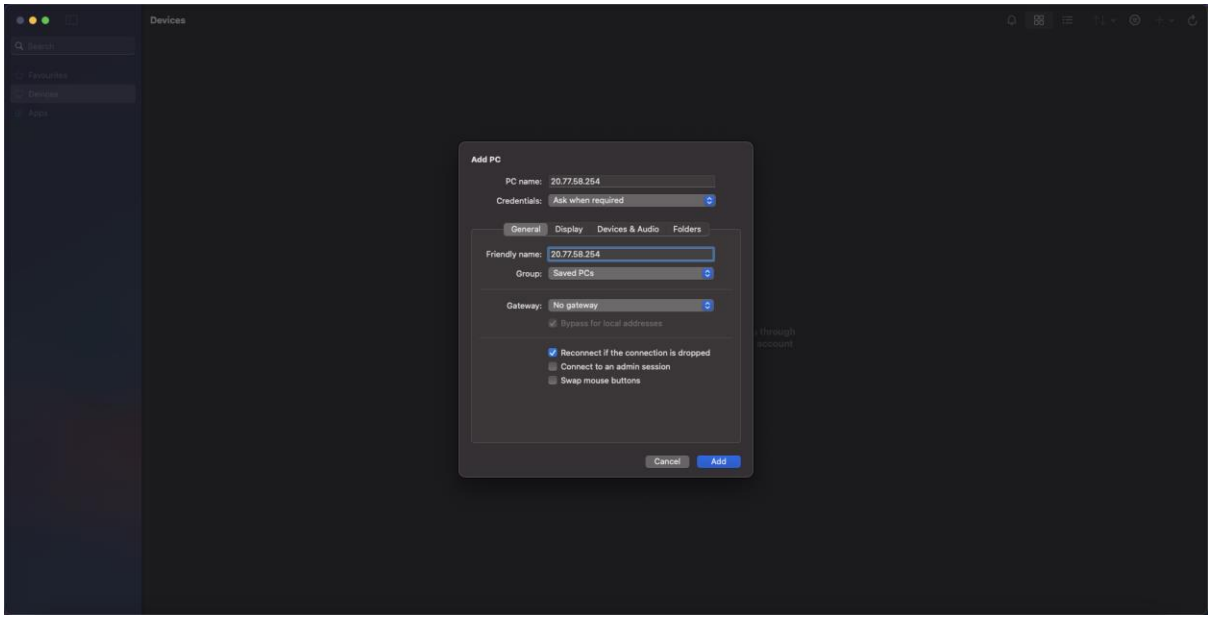


20) Open the windows app after it has installed and select add PC.

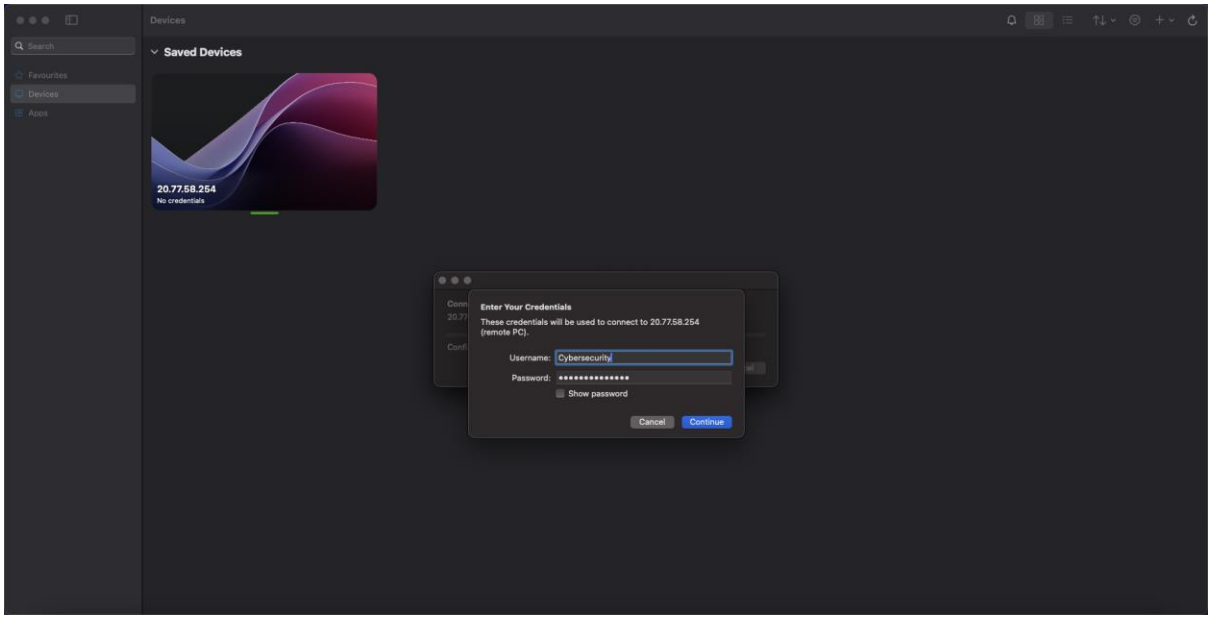


21) You will be prompted to enter the public IP address for the virtual machine. This can be found in the overview section of the virtual machine that you created. Once located, copy and paste the public IP address into the “PC name” section. Make sure the credentials are set to ask when required, and the friendly name can be whatever you want.

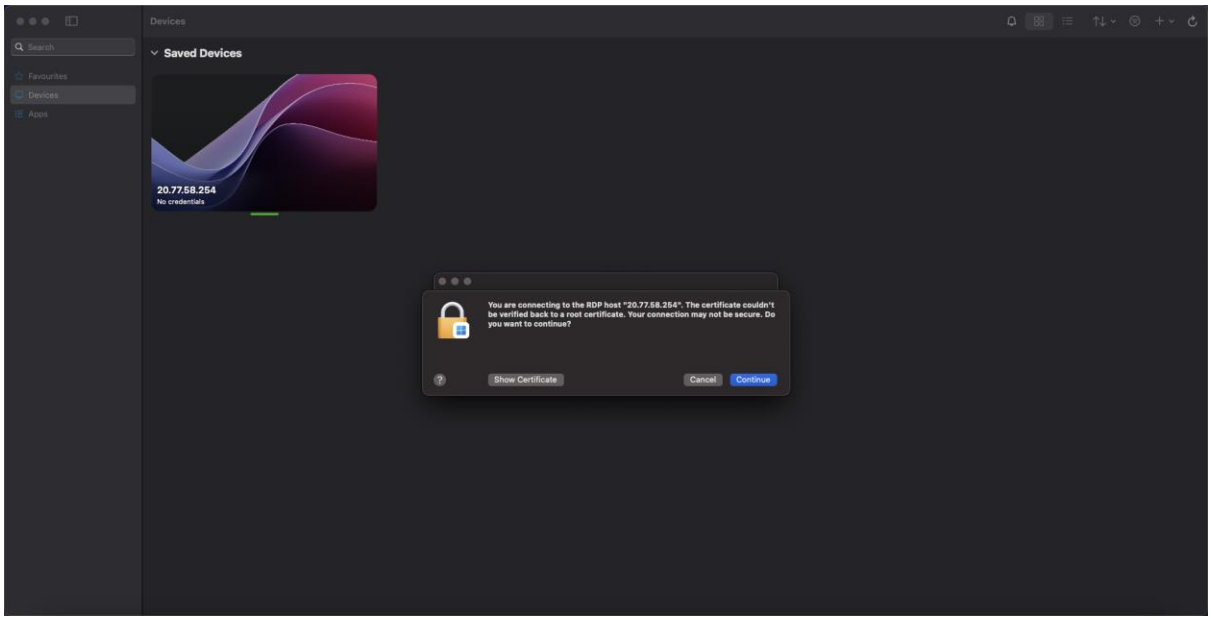




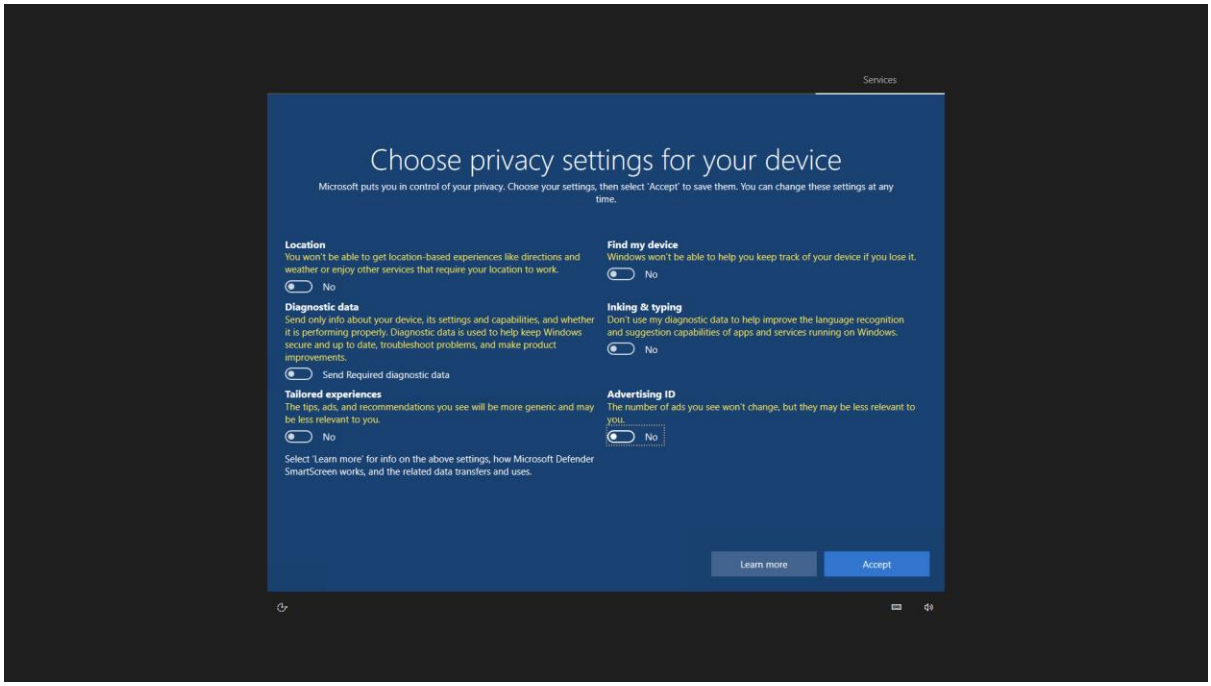
22) Enter the username and password that has been set for the virtual machine.



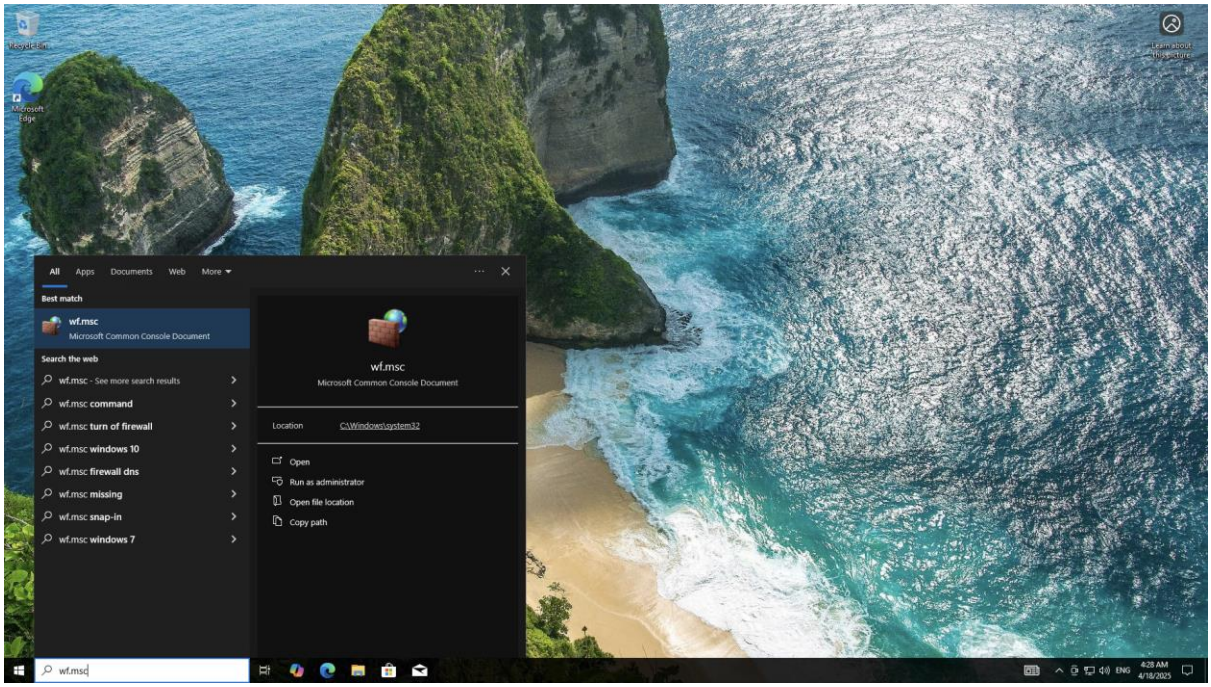
23) Click continue.



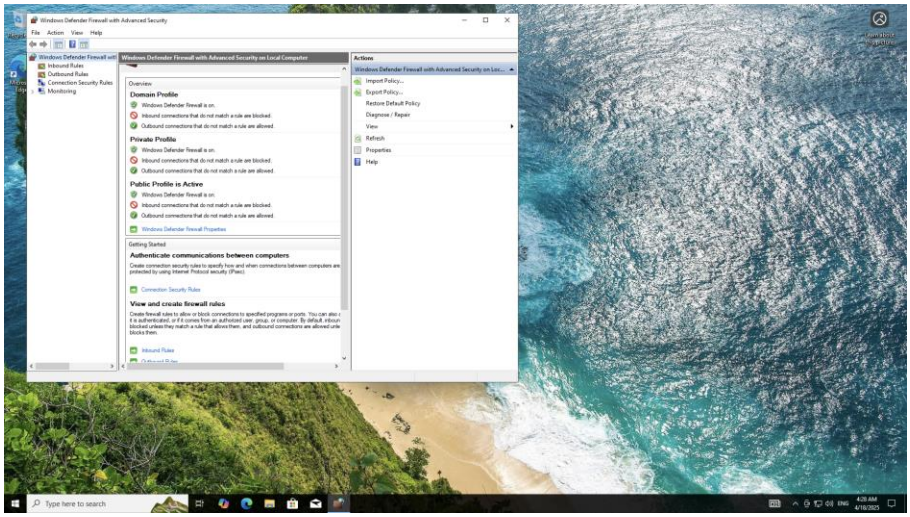
24) Select no for all options.



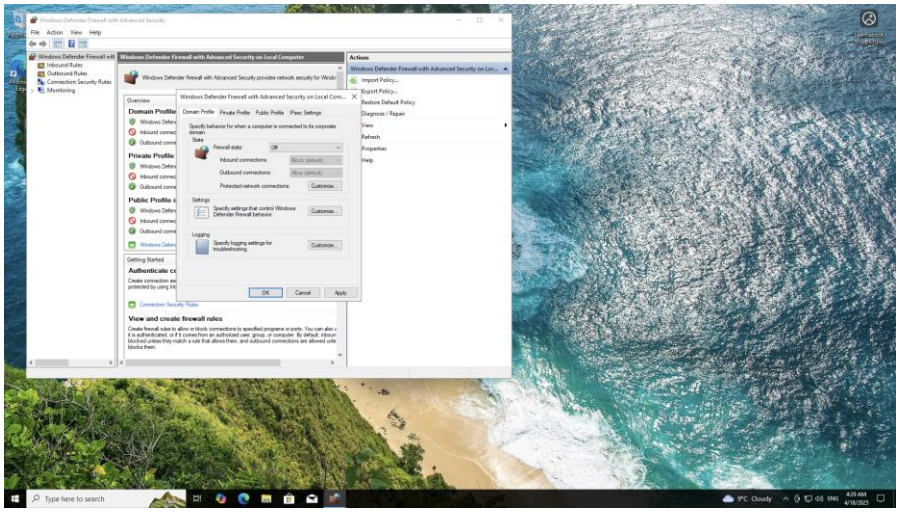
25) Now that we are logged into the virtual machine, the next step is to disable the firewall. So type wf.msc in the search bar below.

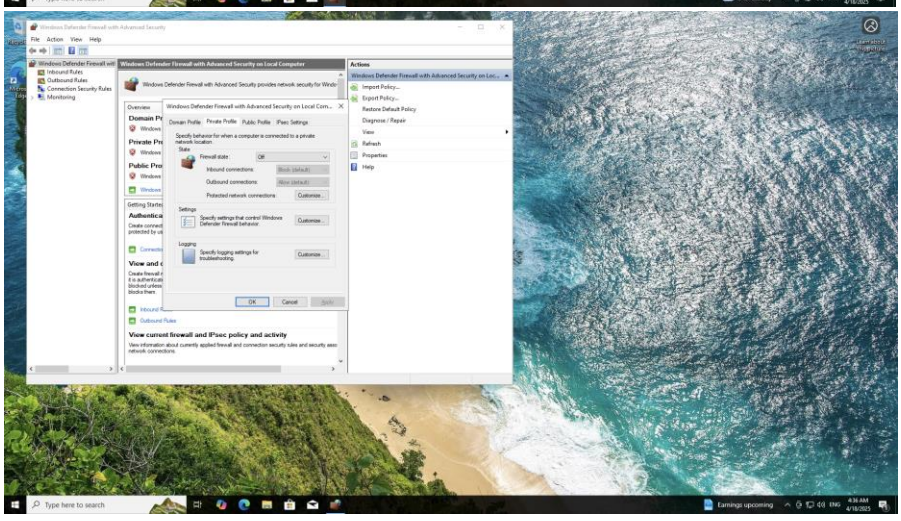


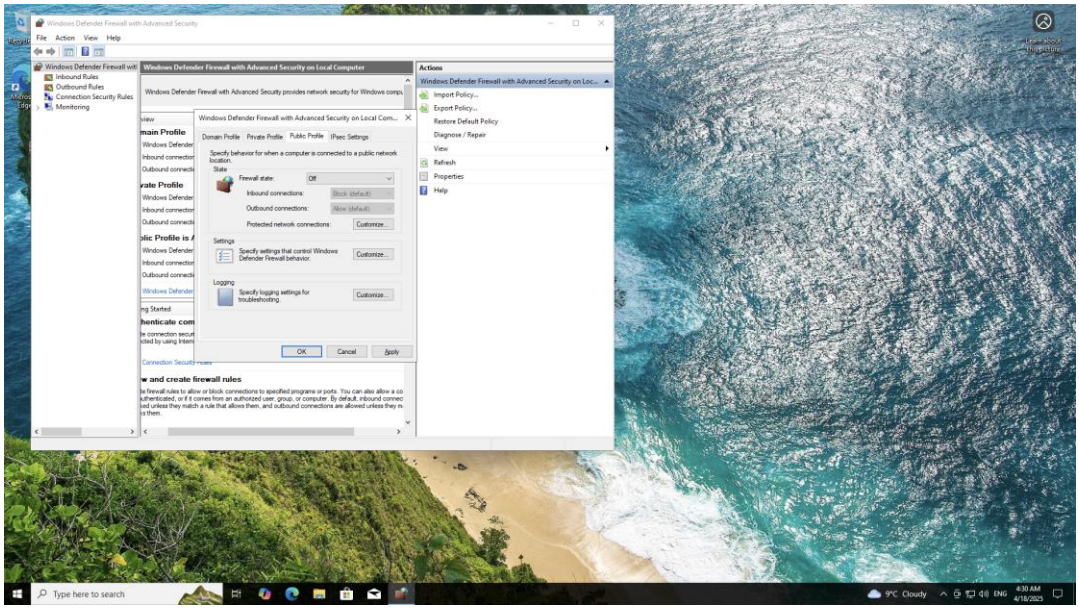
26) “Windows Defender Firewall with Advanced Security” should open.



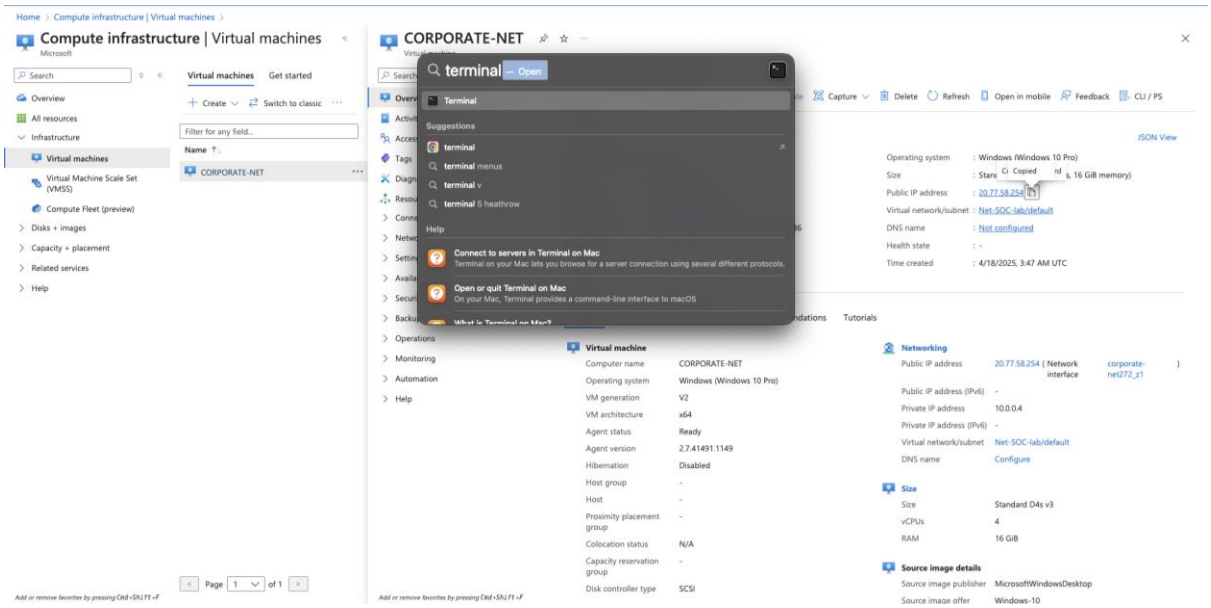
27) Select “off” in the firewall state option for domain, private and public profile, before clicking apply.





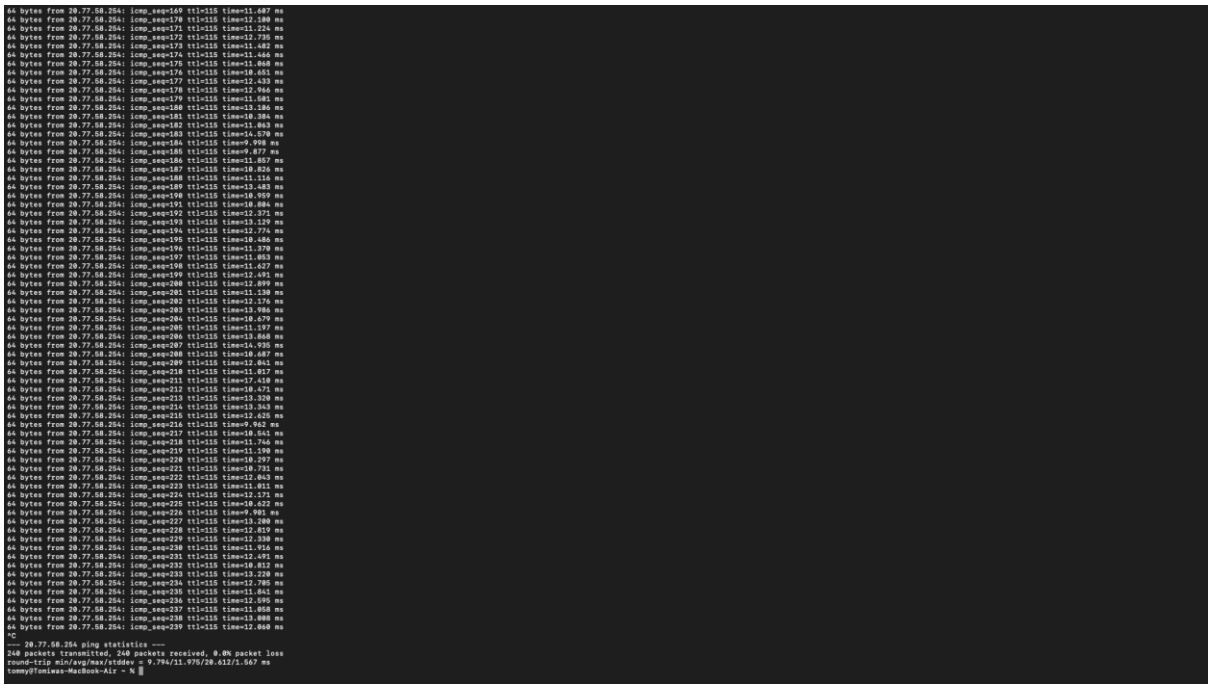


28) Subsequent to disabling the firewalls, open up the terminal. We need to ensure it is possible to ping the virtual machine over the internet. If it is not possible to ping the virtual machine, then the attackers are not able to ping it too.

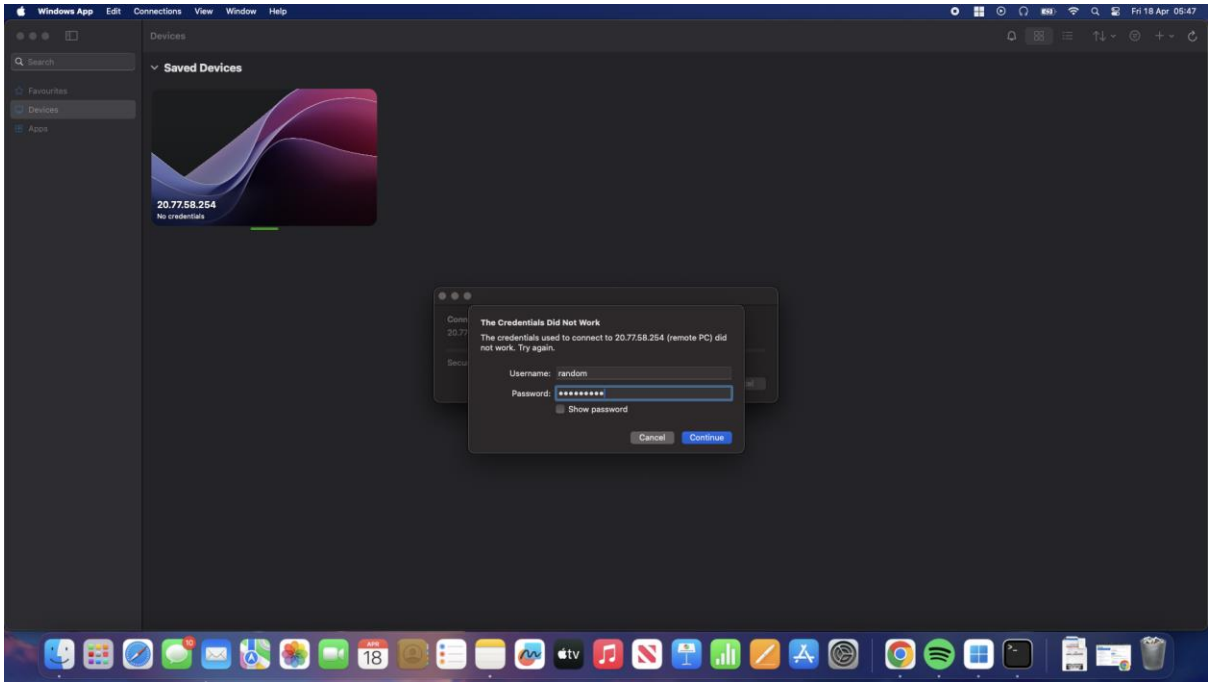


29) Once the terminal has opened, type “ping” press spacebar and then enter the public IP address for the virtual machine. Click enter and you should see bytes being returned from the IP address.

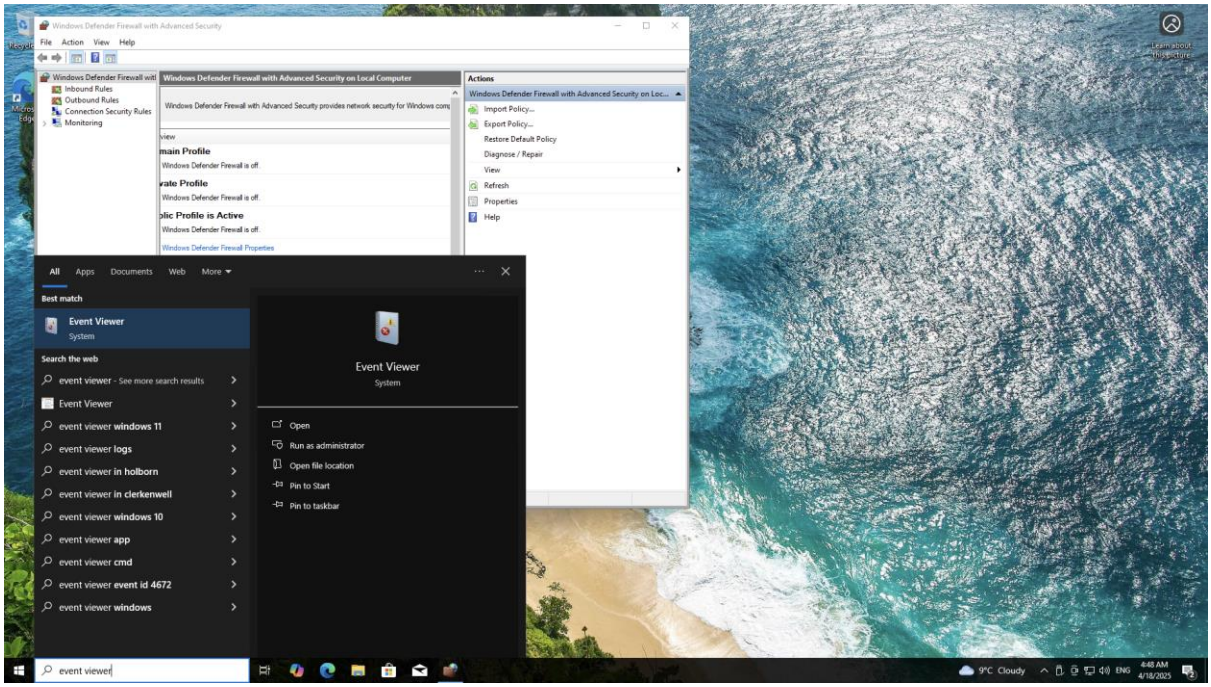
When the pinging has shown to be successful, it can be stopped with ctrl + c. In the scenario the ping has not been successful, the firewall may not be off.



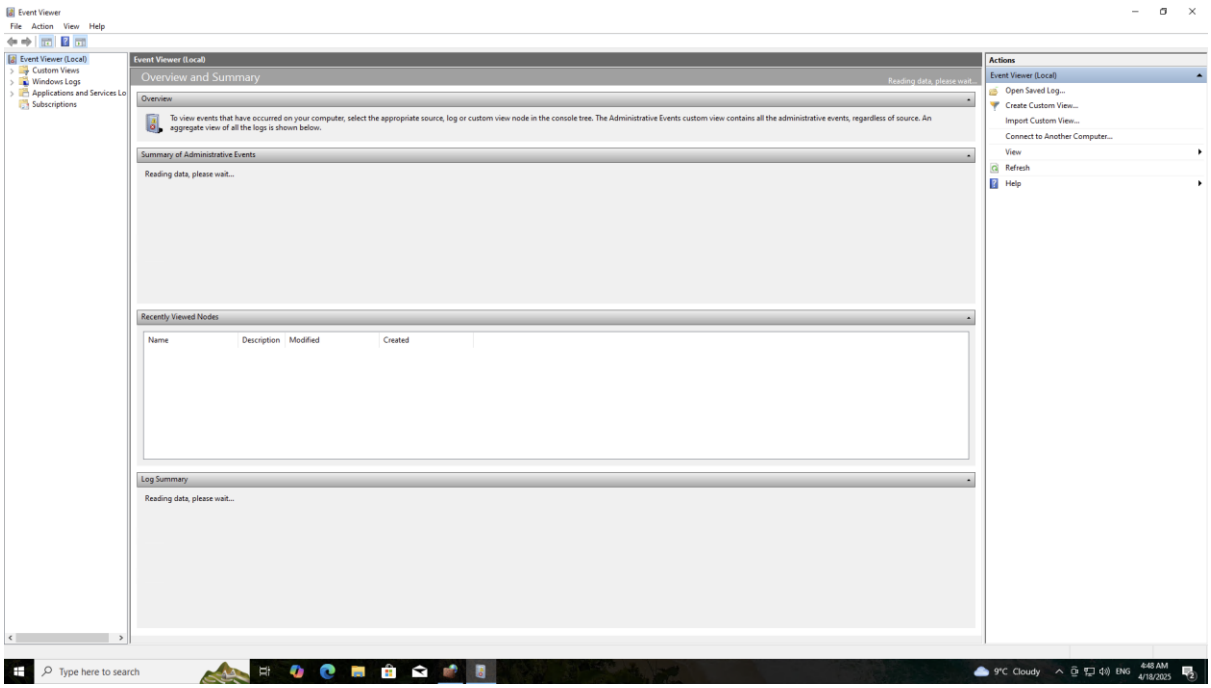
30) Next, log out of the virtual machine account, and intentionally enter incorrect credential a few times to fail the login attempt.



31) Log back into the virtual machine and search “event viewer”. We are going to look at the local logs.

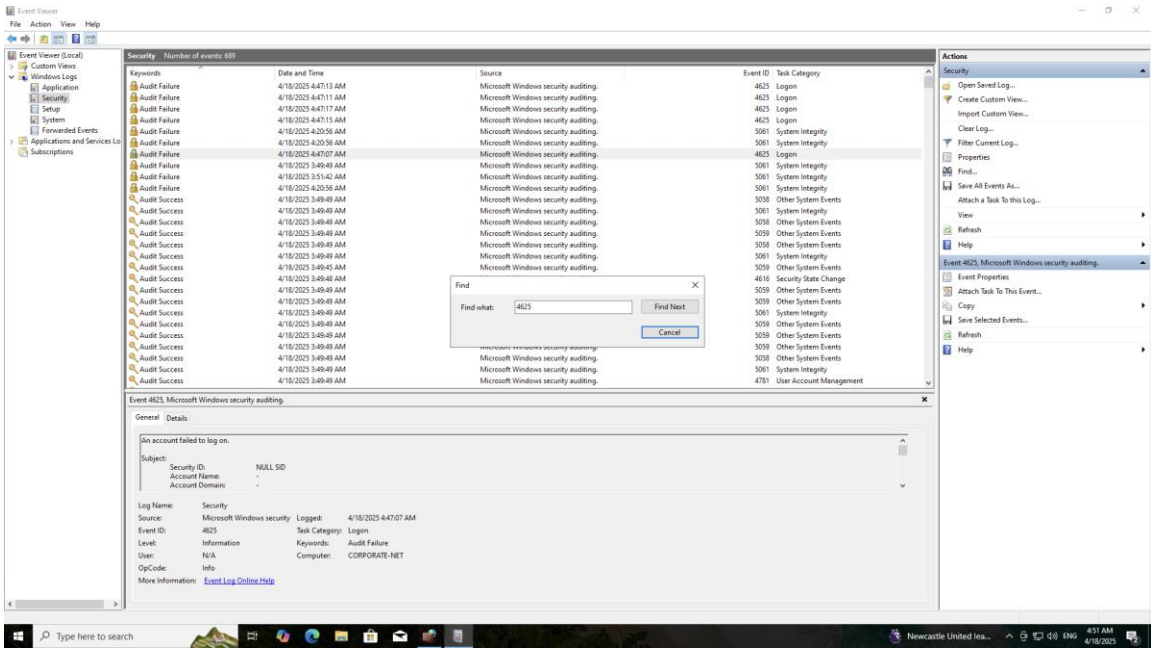


32) If anything happens on the computer, it gets logged. There are certain configurations that can be used to log specific activities, but there are already default settings in place that log activities, which is what we will be viewing.

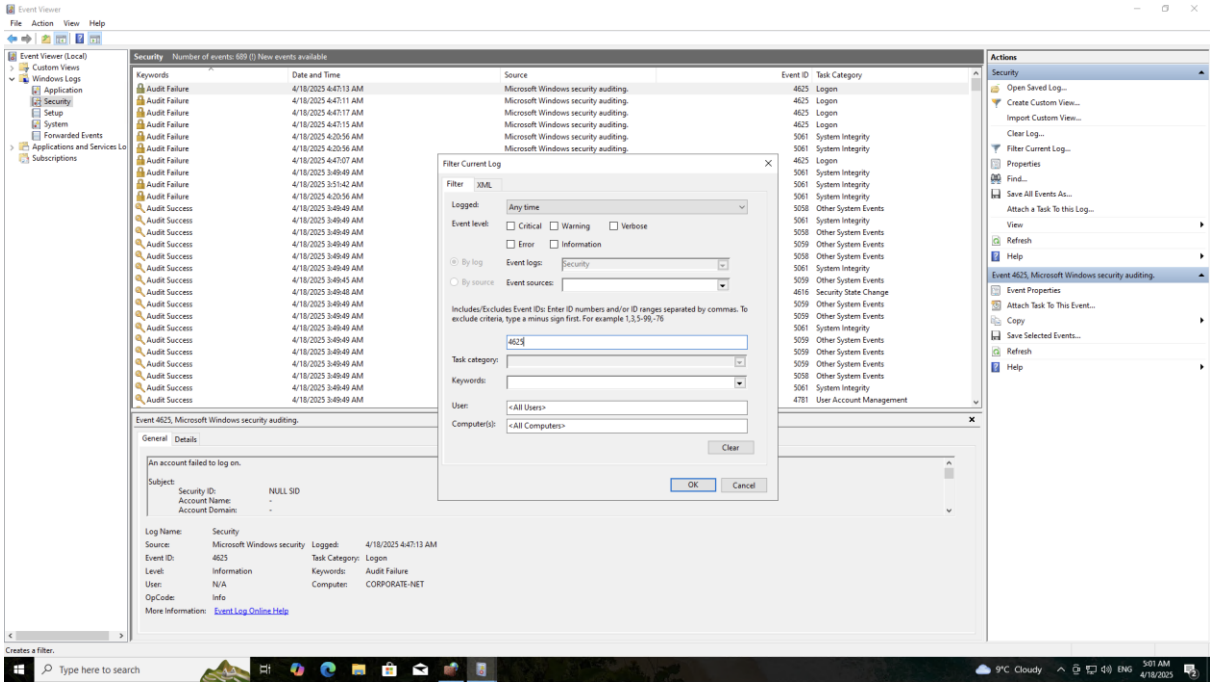


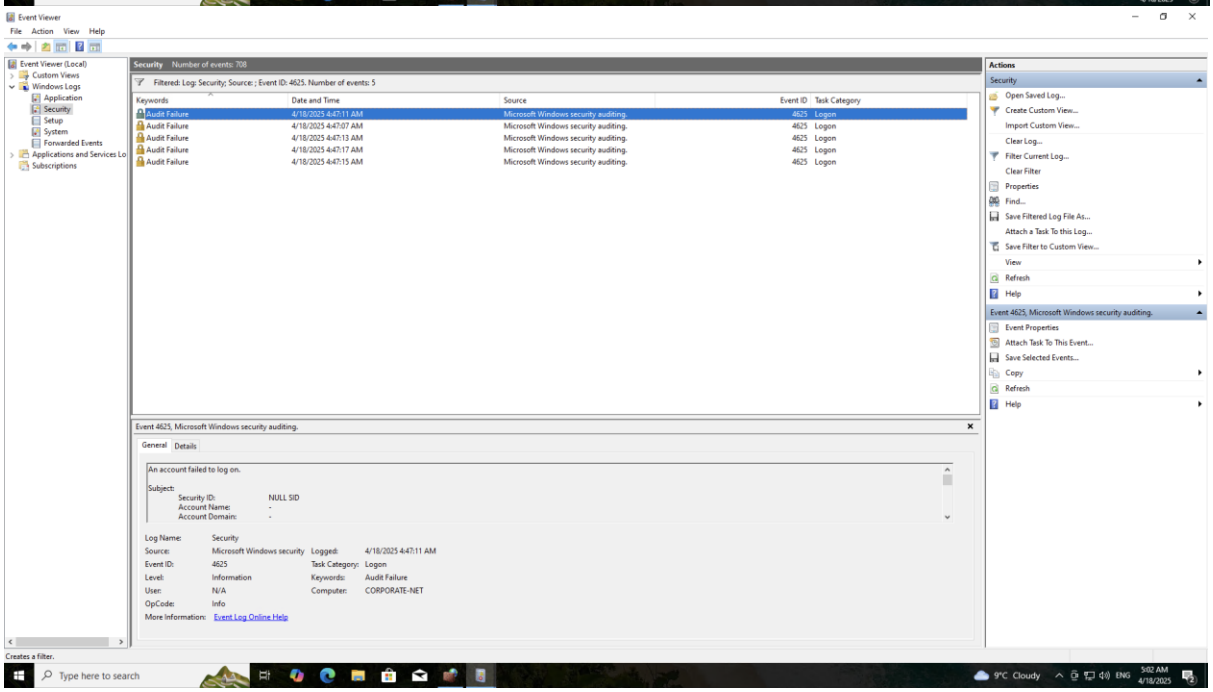
33) Look to the left of the screen and navigate to the security logs. Here you can see the different security events that took place. Each log is categorised into an event type, and is then labelled with a specific event ID.

In the screenshot below I searched for the events with the ID “4625” using ctrl + f. This event ID number is given to failed login attempts.

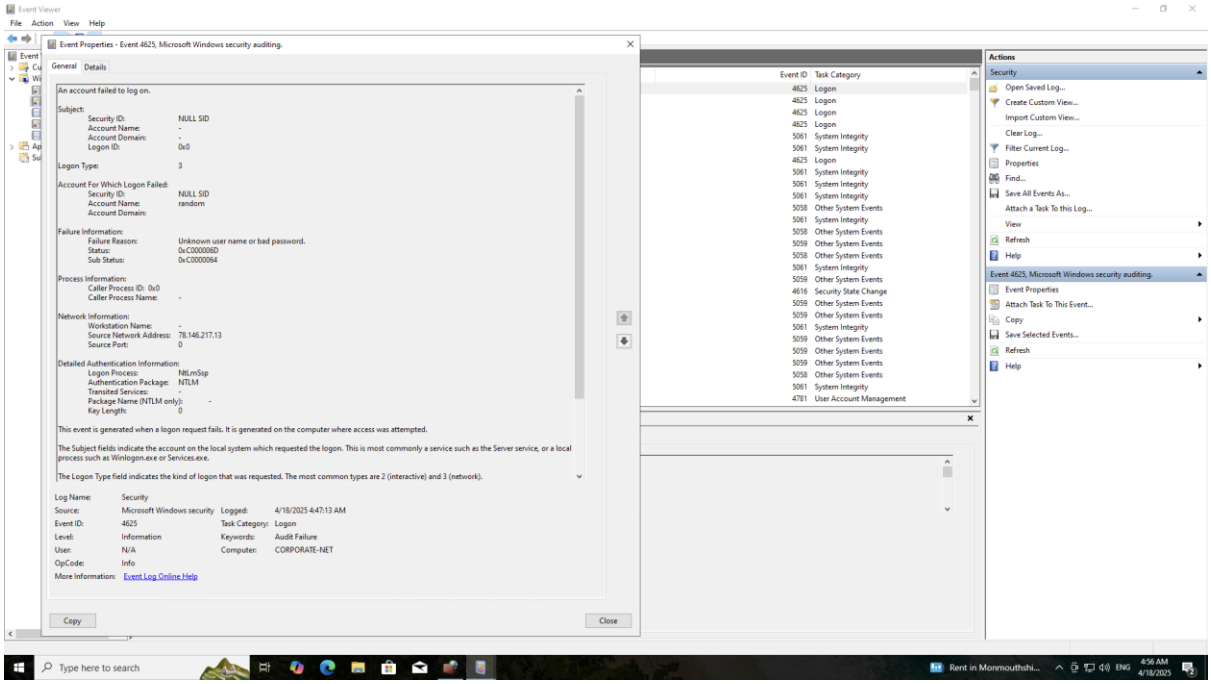


The logs can be filtered using the filter current log tool to the right of the screen.



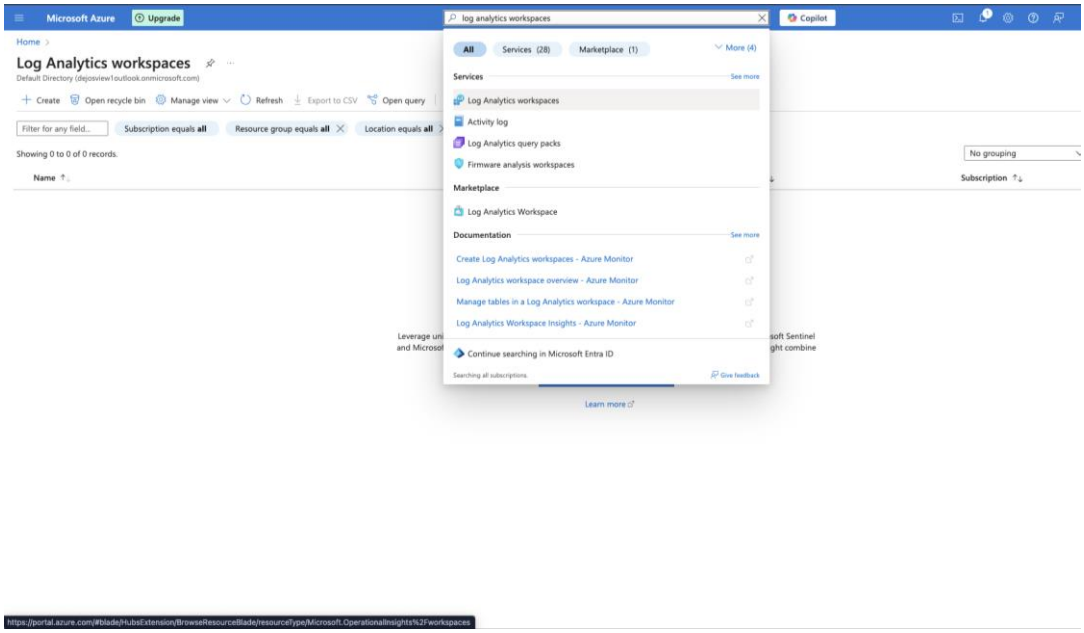


You can double click the event and then expand it to view more information regarding the event. The details include the account name that failed to login, the source network address (the IP address of the device that attempted to login, and more. As the lab progresses, we will forward this data to Azure where it can be queried and connected to the SIEM in order to view where the attacks originate from.

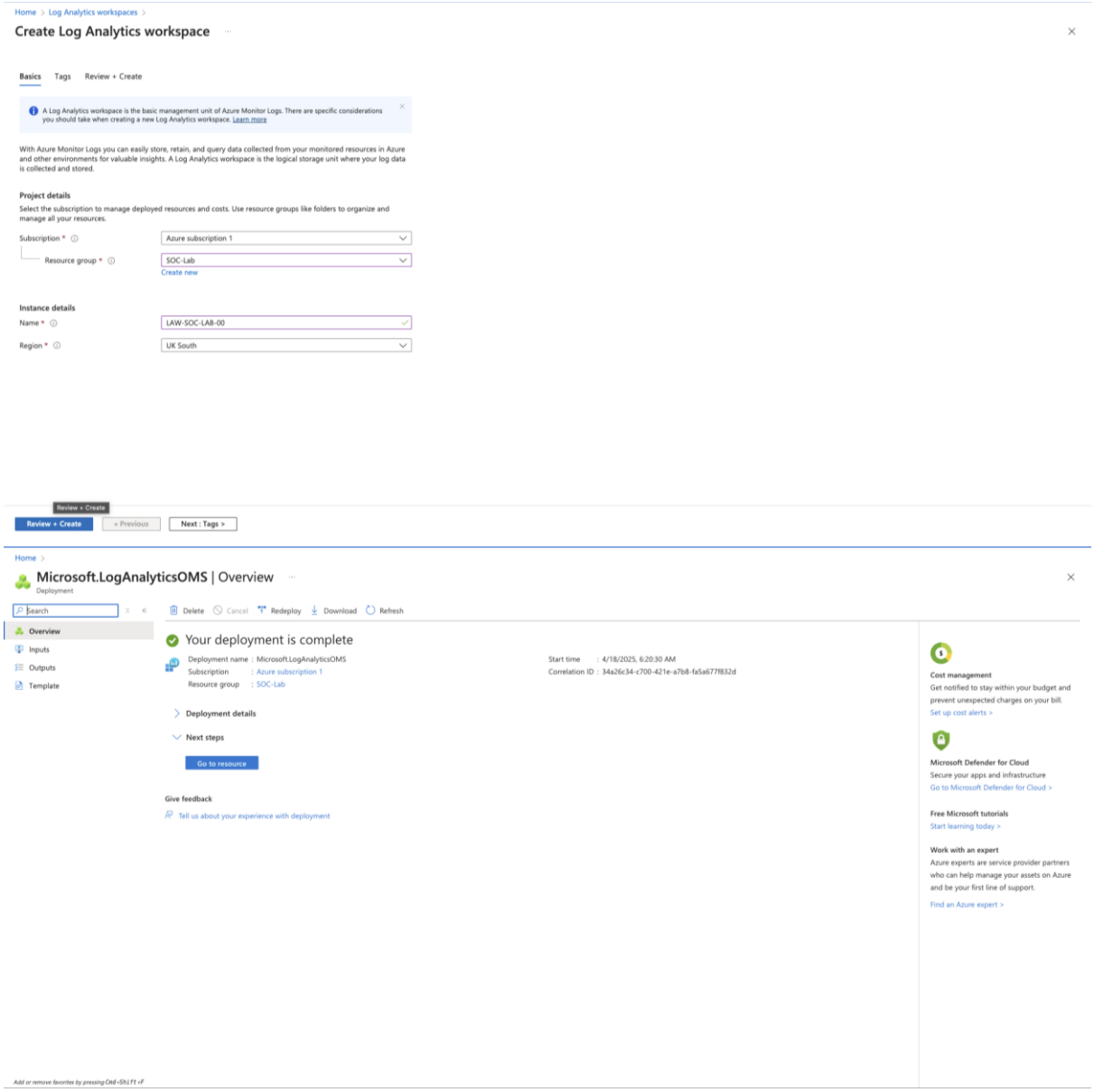


Creating Log Repository - Log Analytics Workspace

1) Navigate to Log Analytics Workspace.

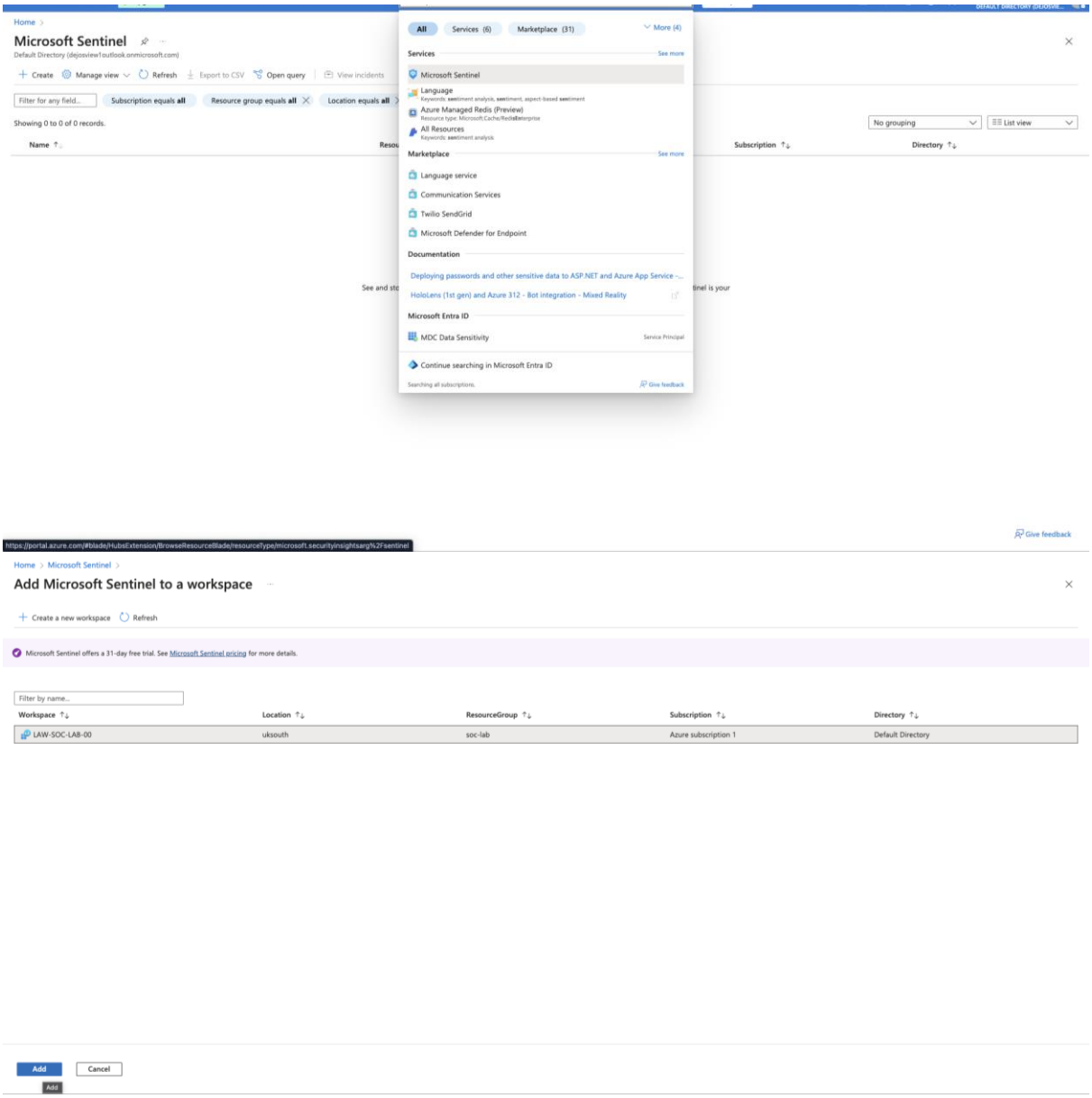


2) Assign it to the resource group that was created earlier. The chosen name in the instance details is not important. Then click “review + create” and click “create” again afterwards.

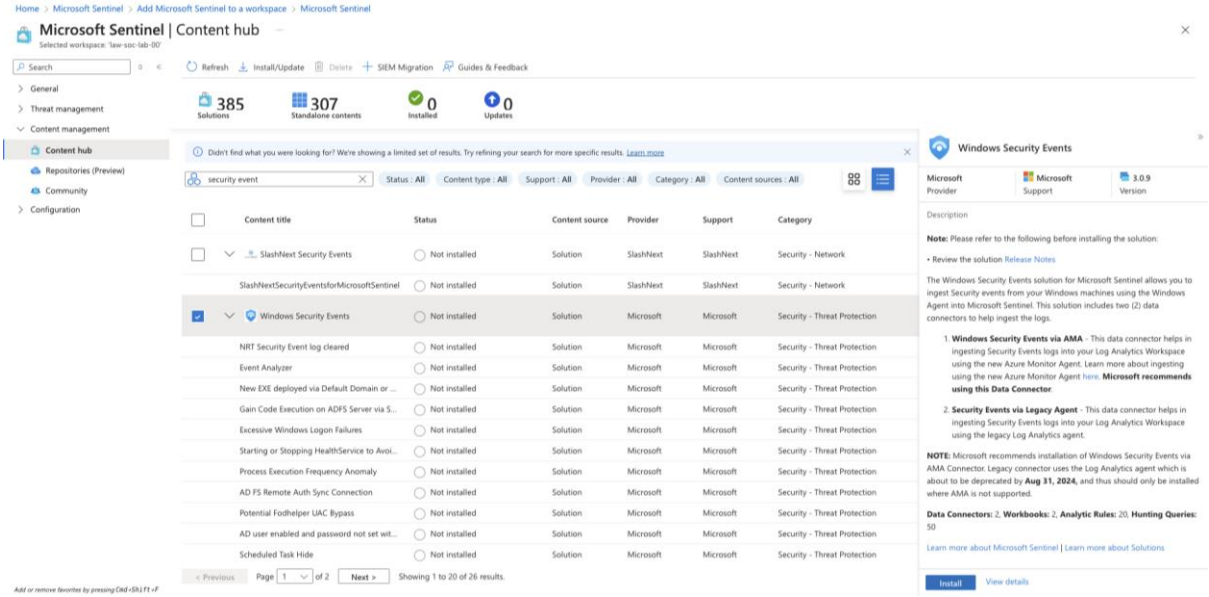


Creating Microsoft Sentinel

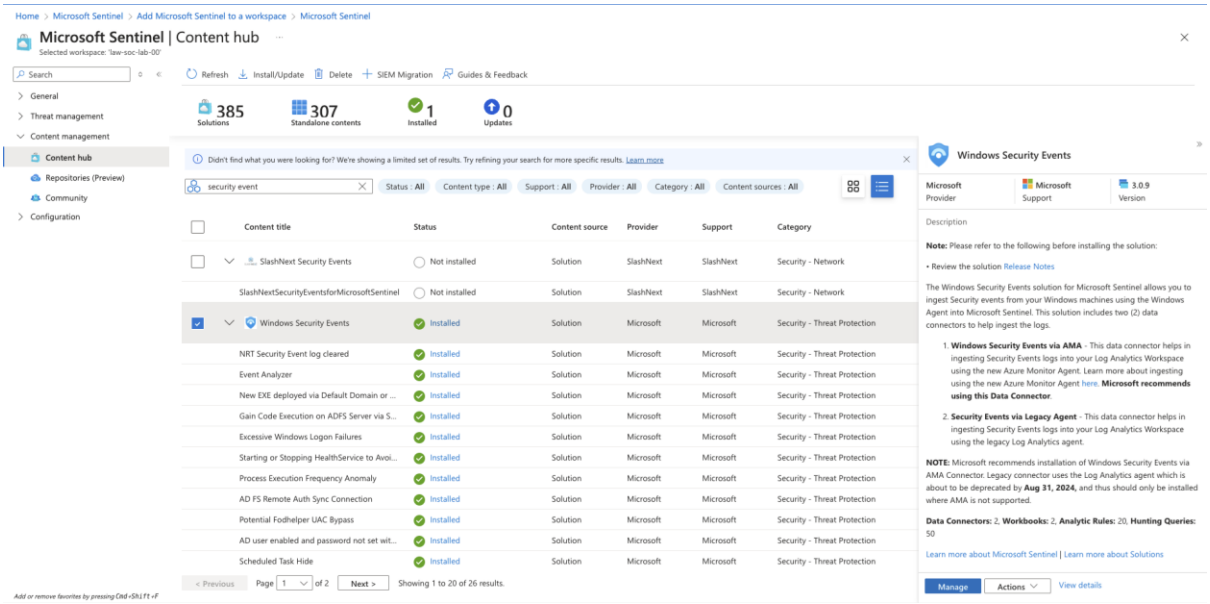
1) Navigate to Microsoft Sentinel, select the workspace you created, and click add in the bottom left corner.



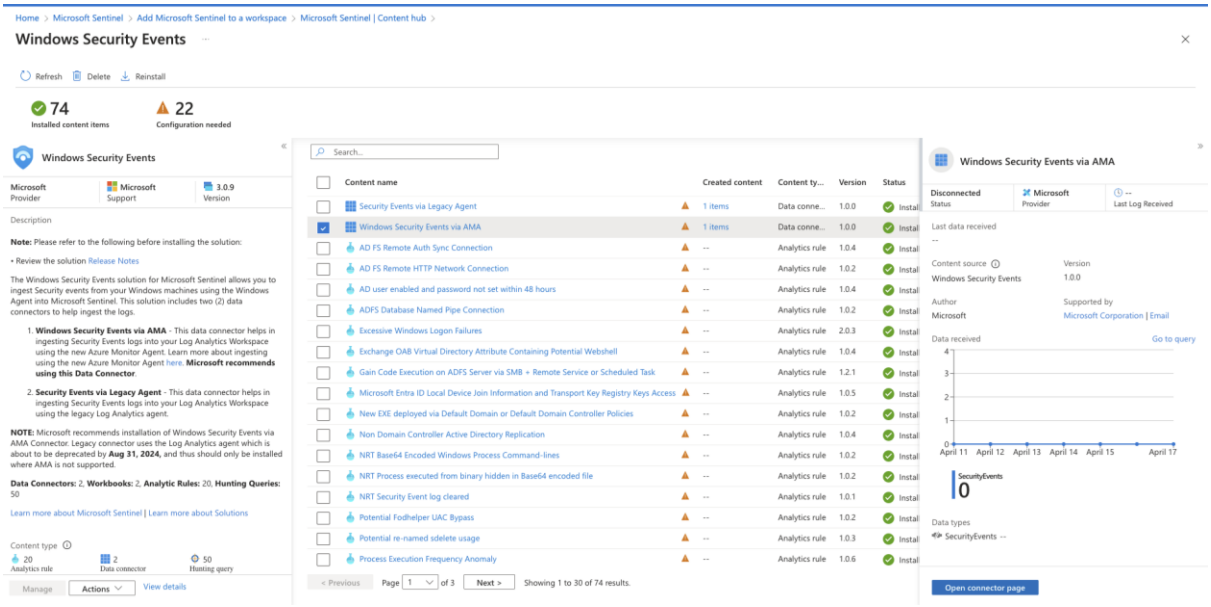
2) Go to Content Hub in the newly added workspace, and search “Windows Security Events”. Once you have found the content, select the box and then proceed to install.



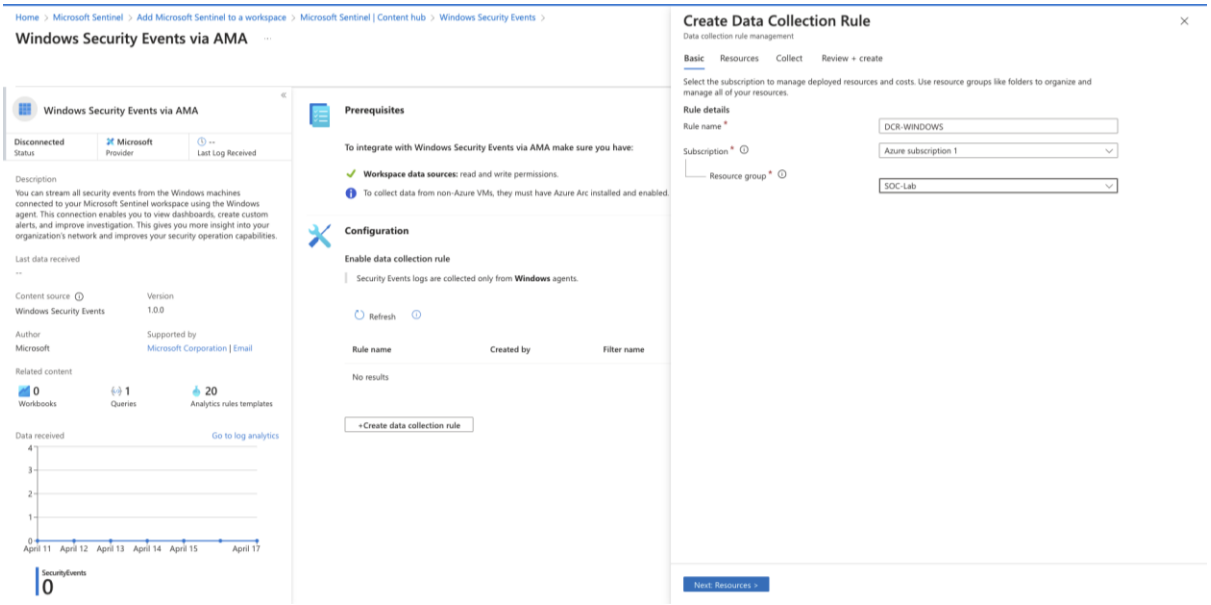
3) The status column will show you when the install is complete. Next, click manage in the Windows Security Events.



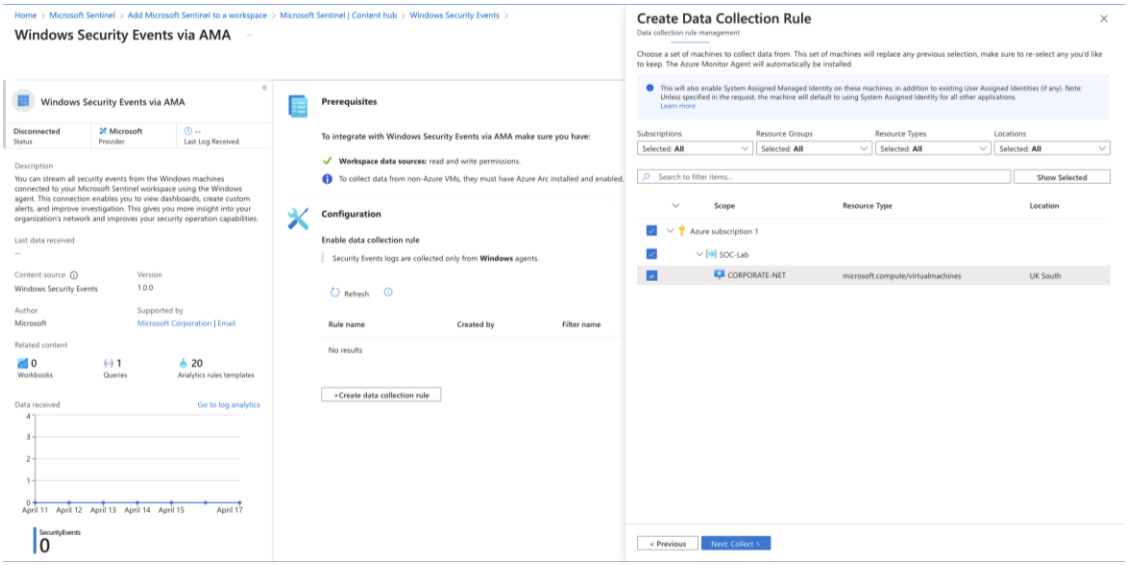
4) Select “Windows Security Events via AMA”. If you scroll there will be a chart that displays how much data has been ingested, which is currently 0 due to there currently being no connection. The following step is to click “Open connector page”.



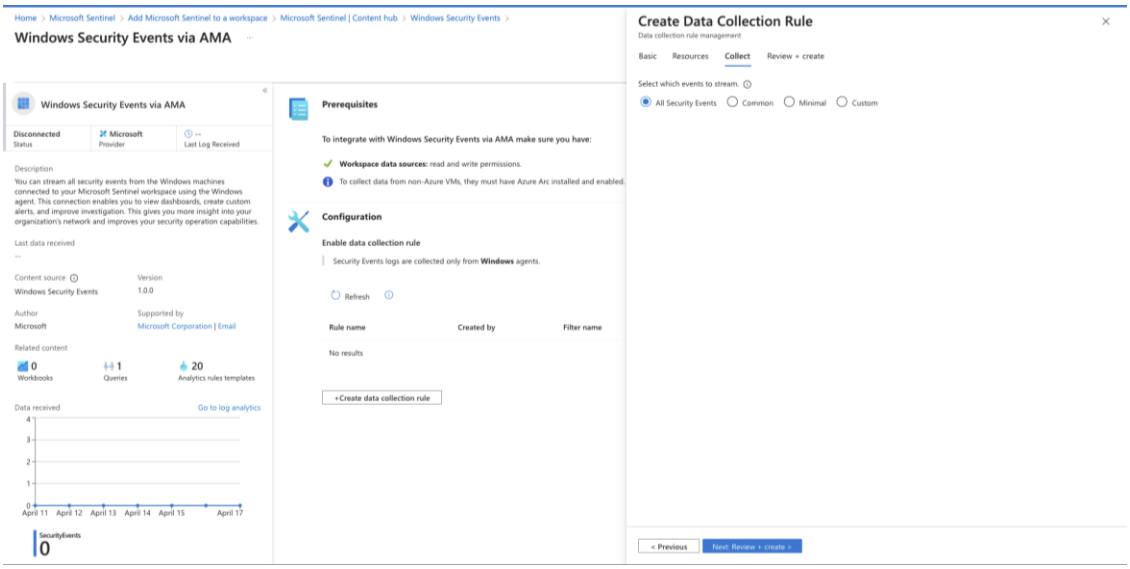
5) We are going to create a data collection rule. The virtual machine uses this rule to forward logs into the logs analytics workspace, in turn allowing access to them inside of the SIEM. Enter a rule name and ensure you select the correct resource group.

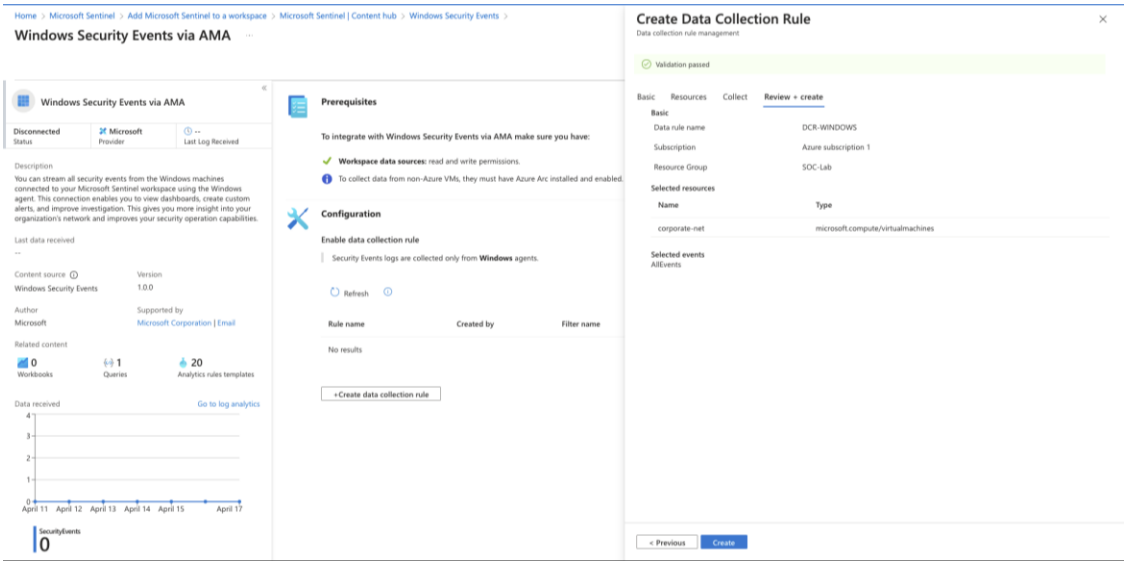


6) Click on the arrows to expand the scope and select the network.

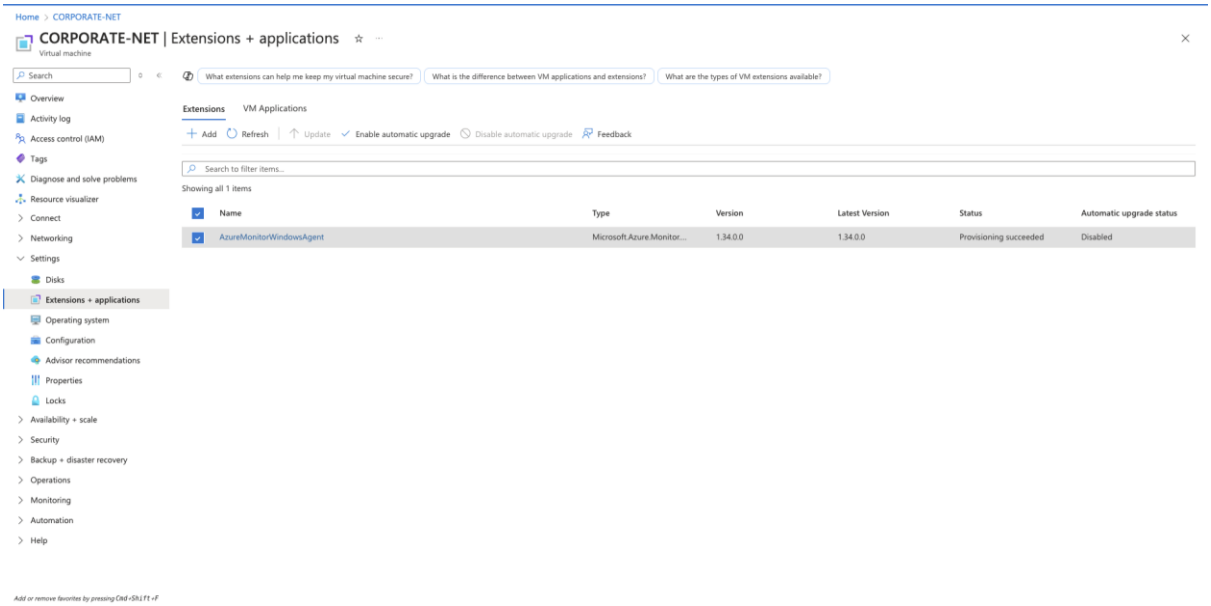


7) Proceed through review and create and then create.



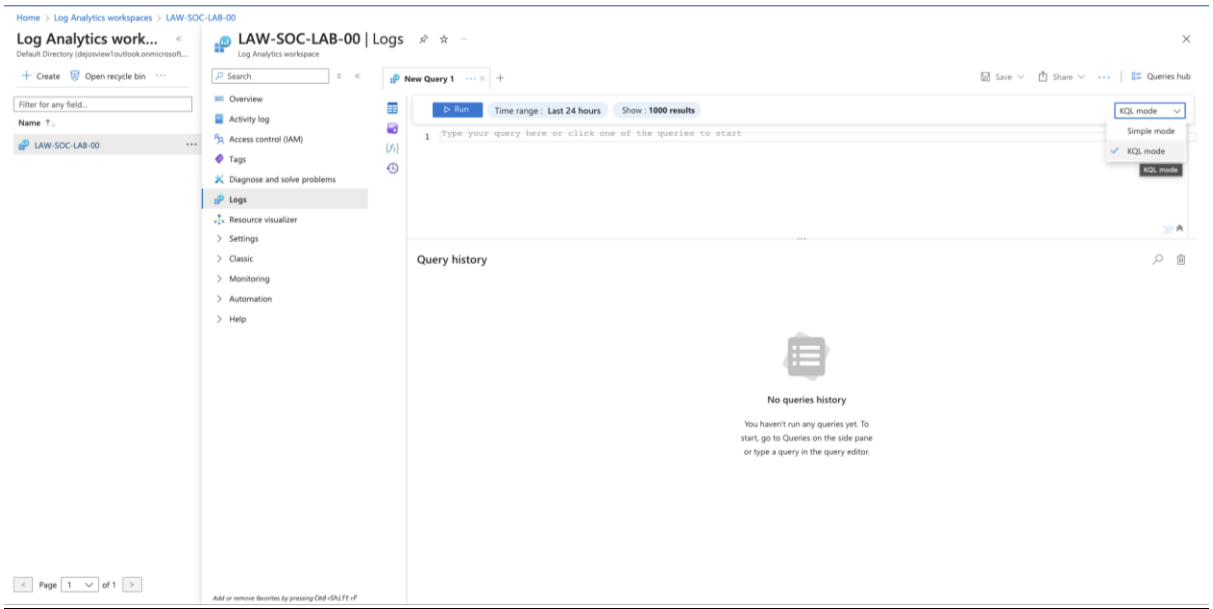


8) If you go to the extensions + applications section inside the network, you should find the “AzureMonitorWindowsAgent”. This is what forwards the logs to the log analytics workspace. You may have to wait sometime (eg. 20-30 minutes) before the logs being to appear in the log analytics. As long as the status shows “Provisioning Succeeded”, the application should be working as intended.

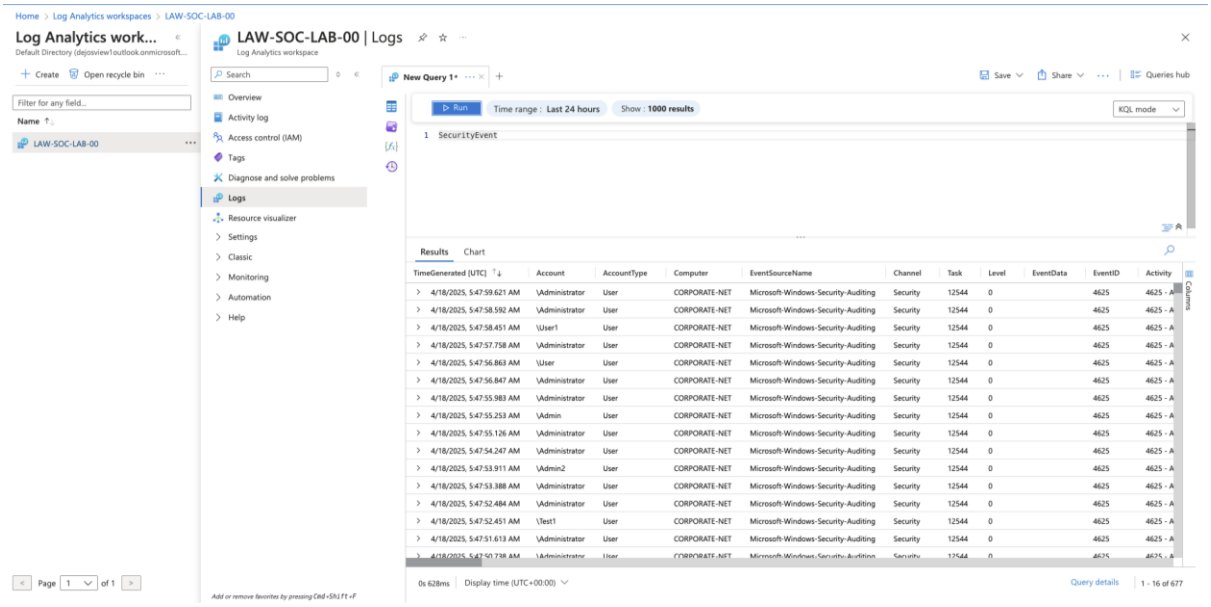


Log Analytics Workspace

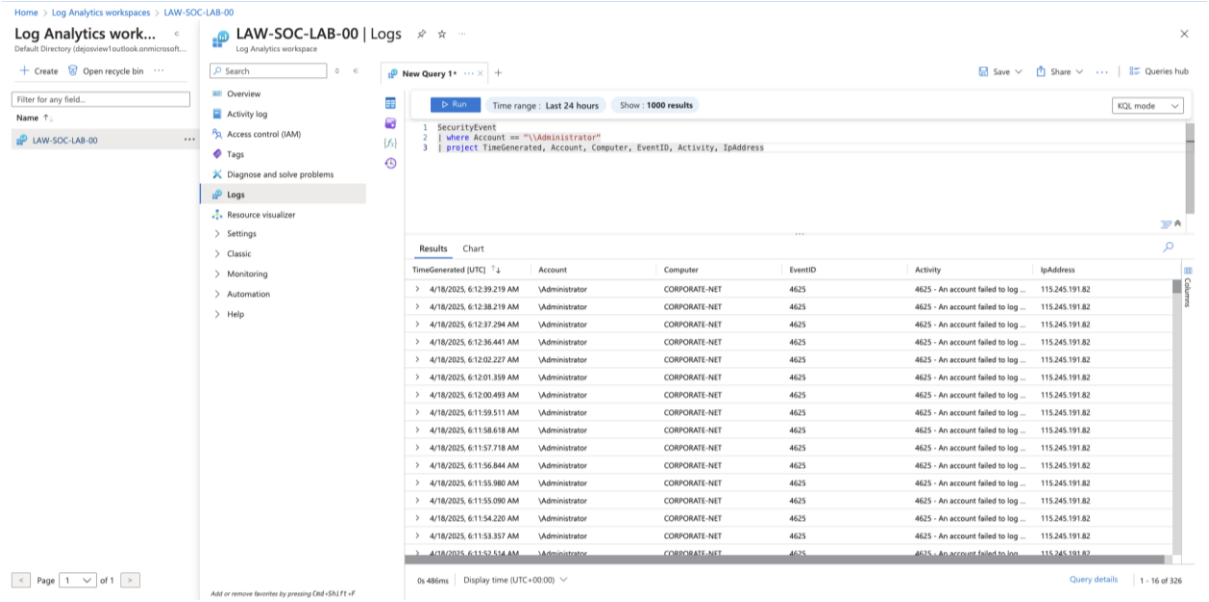
1) Go to the Log Analytics Workspace, select the workspace and navigate to the Logs section. Once the logs are open, you may need to select KQL mode on the right as seen in the image below.



2) To view all the security logs, type the query SecurityEvent into the log, then select run.

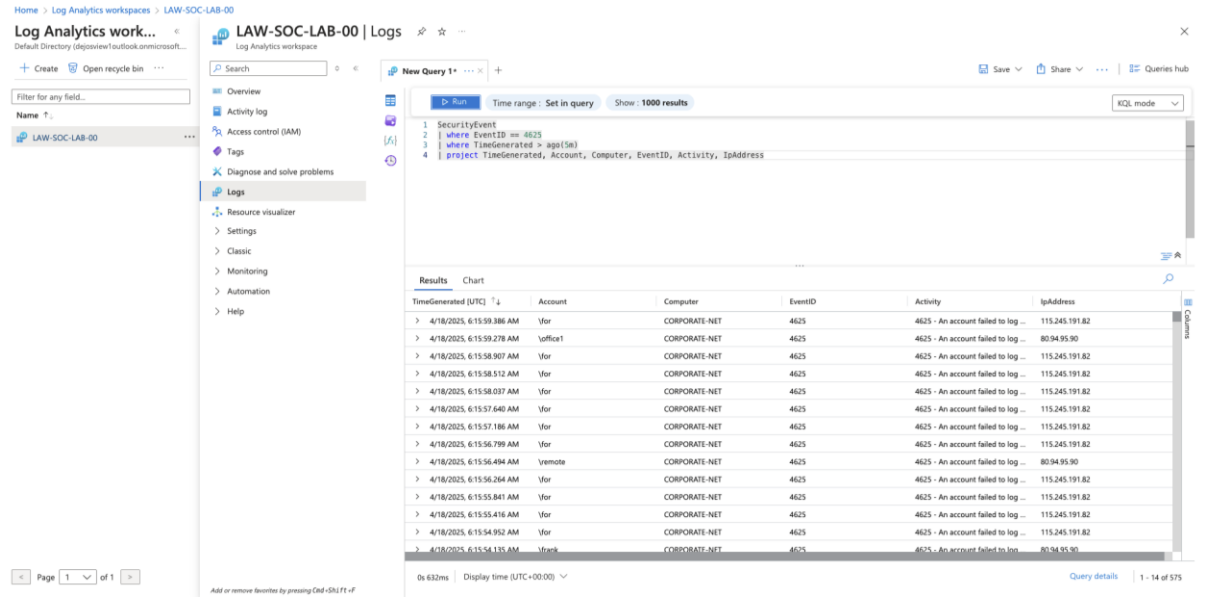


3) The query in the screenshot below can be used to filter the given output.
Where Account == "\\Administrator" filters the results to only include accounts that are named \Administrator.
Project TimeGenerated, Account, Computer, EventID, Activity, IpAddress further filters the results to display only the elements stated within the query.



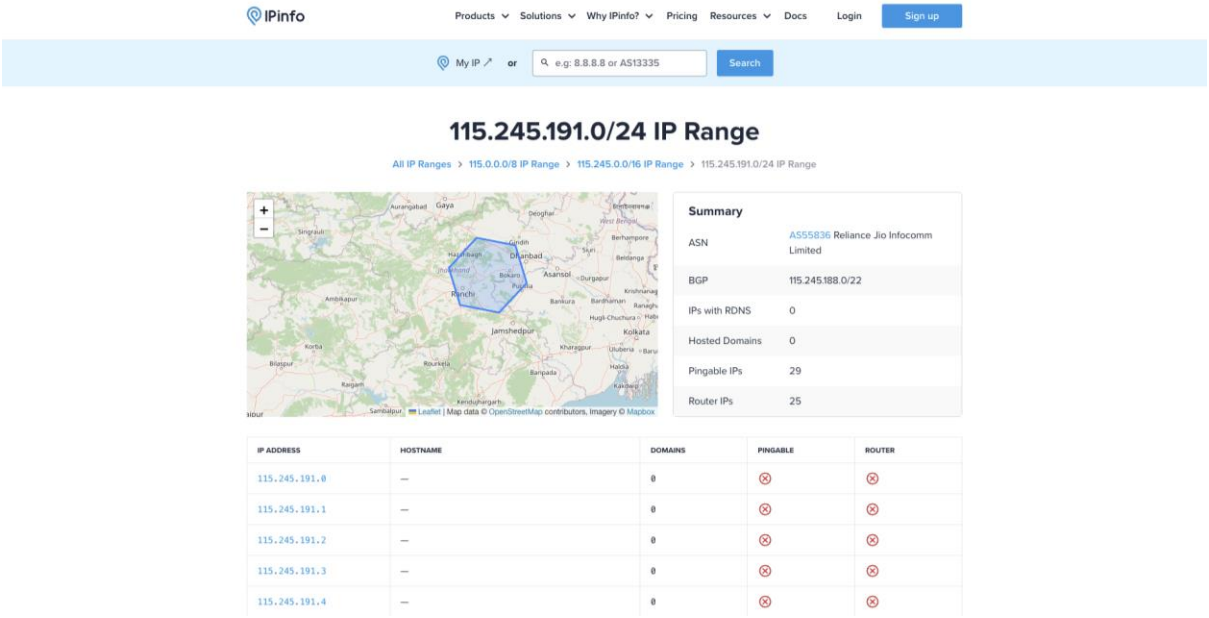
4) In the scenario you only wanted to view the failed login attempts, the eventID the specific eventID can be used to filter the results. Earlier in the lab we observed the eventID for these attempts is 4265, so this can be implemented into a query for accurate filtering:
where EventID == 4625

Using where TimeGenerated > ago(5m) the results will then only show events that took place within the last 5 minutes. The time can be customised for the user's desired results.

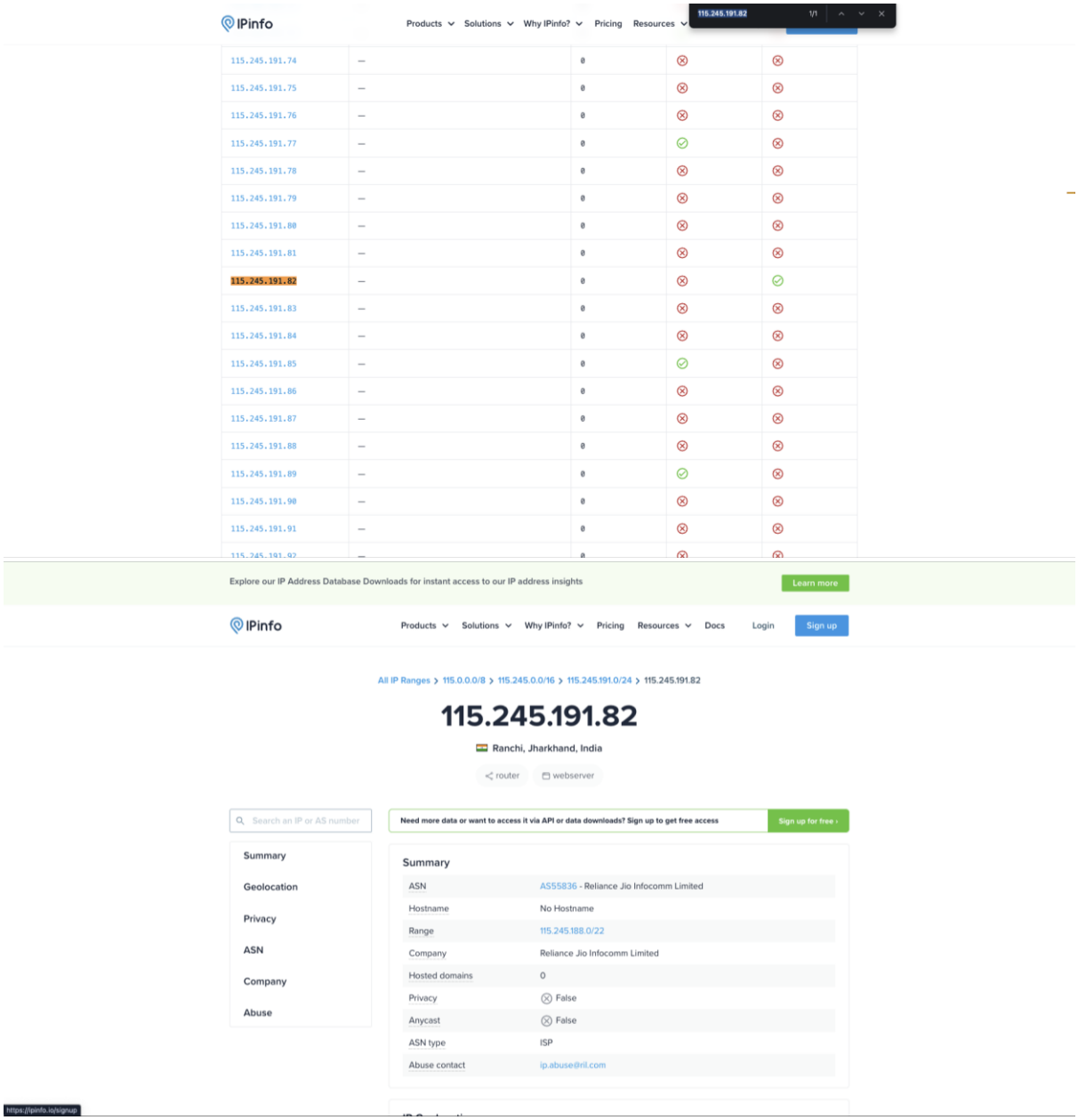


5) It is also possible to locate the geographic location of the hackers as the IpAddress is an element that is presented in the results table. For example, we can take the IpAddress from the first result in the image above, and use IPinfo to search for the location.

The IpAddress was located in India as seen in the screenshot below:



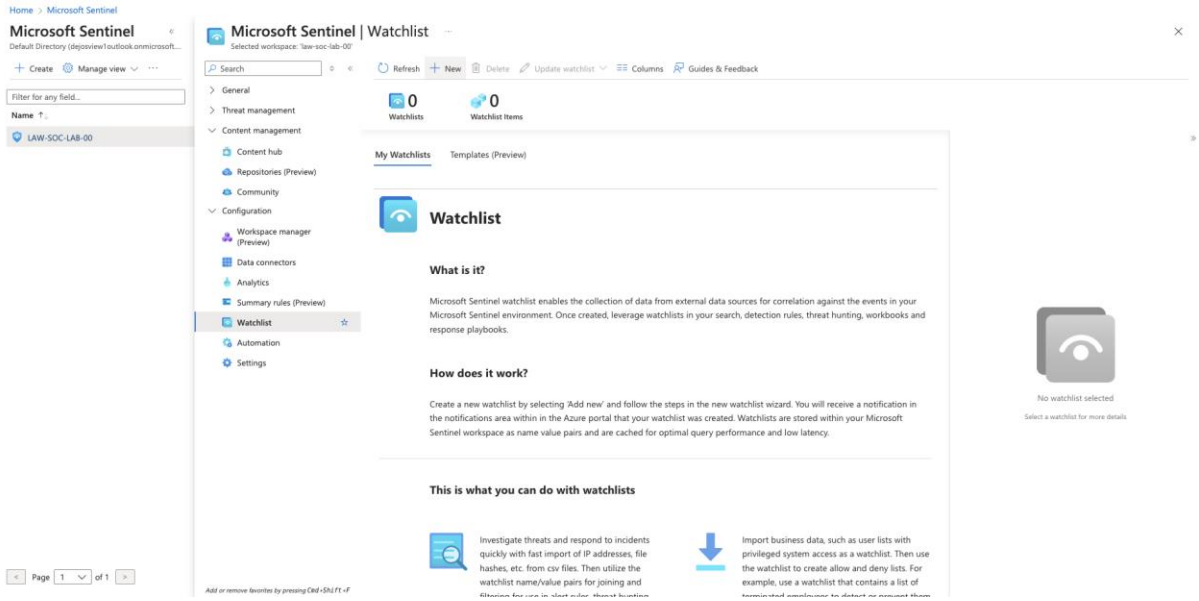
6) Using ctrl + f you can paste the IpAddress to find the exact one amongst various others. After clicking it, more information connected to the address was visible.


IPinfo
Products
Solutions
Why IPinfo?
Pricing
Resources
115.245.191.82
1/1
115.245.191.74
115.245.191.75
115.245.191.76
115.245.191.77
115.245.191.78
115.245.191.79
115.245.191.80
115.245.191.81
115.245.191.82
115.245.191.83
115.245.191.84
115.245.191.85
115.245.191.86
115.245.191.87
115.245.191.88
115.245.191.89
115.245.191.90
115.245.191.91
Explore our IP Address Database Downloads for instant access to our IP address insights
Learn more
IPinfo
Products
Solutions
Why IPinfo?
Pricing
Resources
Docs
Login
Sign up
All IP Ranges › 115.0.0.0/8 › 115.245.0.0/16 › 115.245.191.0/24 › 115.245.191.82
115.245.191.82
Ranchi, Jharkhand, India
router
webserver
Search an IP or AS number
Need more data or want to access it via API or data downloads? Sign up to get free access
Sign up for free ›
Summary
Geolocation
Privacy
ASN
Company
Abuse
Summary
ASN
AS55836 - Reliance Jio Infocomm Limited
Hostname
No Hostname
Range
115.245.188.0/22
Company
Reliance Jio Infocomm Limited
Hosted domains
0
Privacy
False
Anycast
False
ASN type
ISP
Abuse contact
ip.abuse@ril.com
https://ipinfo.io/signup

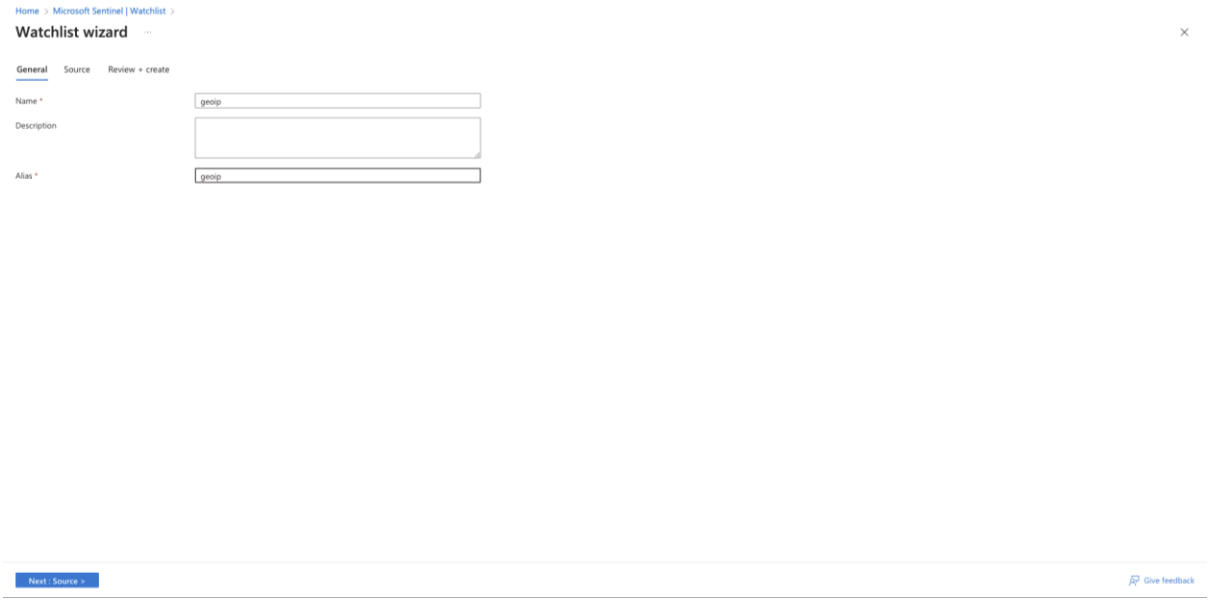
Geographic Attack Map

To make it easier and more efficient when it comes to locating where the attacks stem from, we can upload geographic data to the SIEM. This data will then plot on a geographical map, highlighting areas where attacks have originated from.

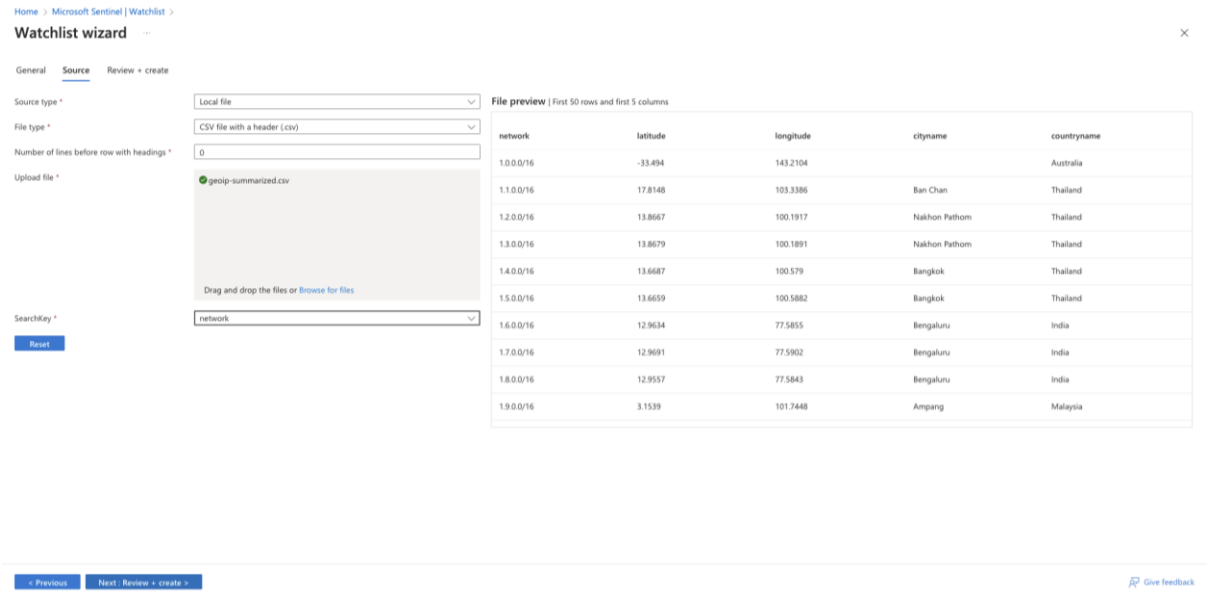
1) The first step of this process is creating a watchlist in Microsoft Sentinel, so navigate to Sentinel > Watchlist and then select new.



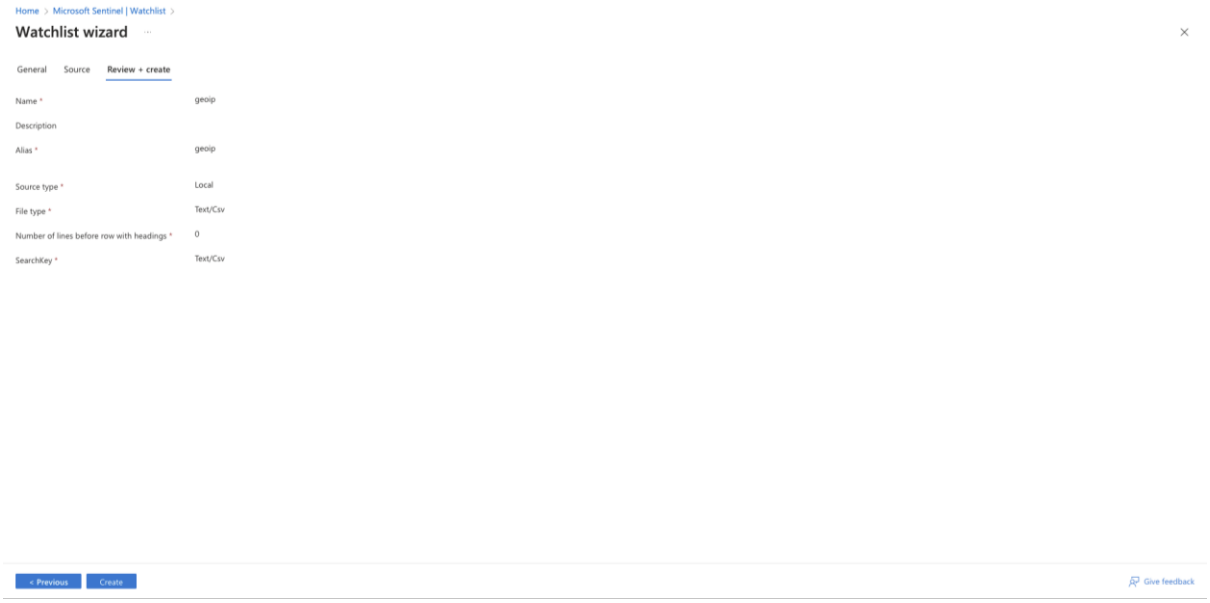
2) Input the name and alias. To avoid potential errors, you can make them the same.



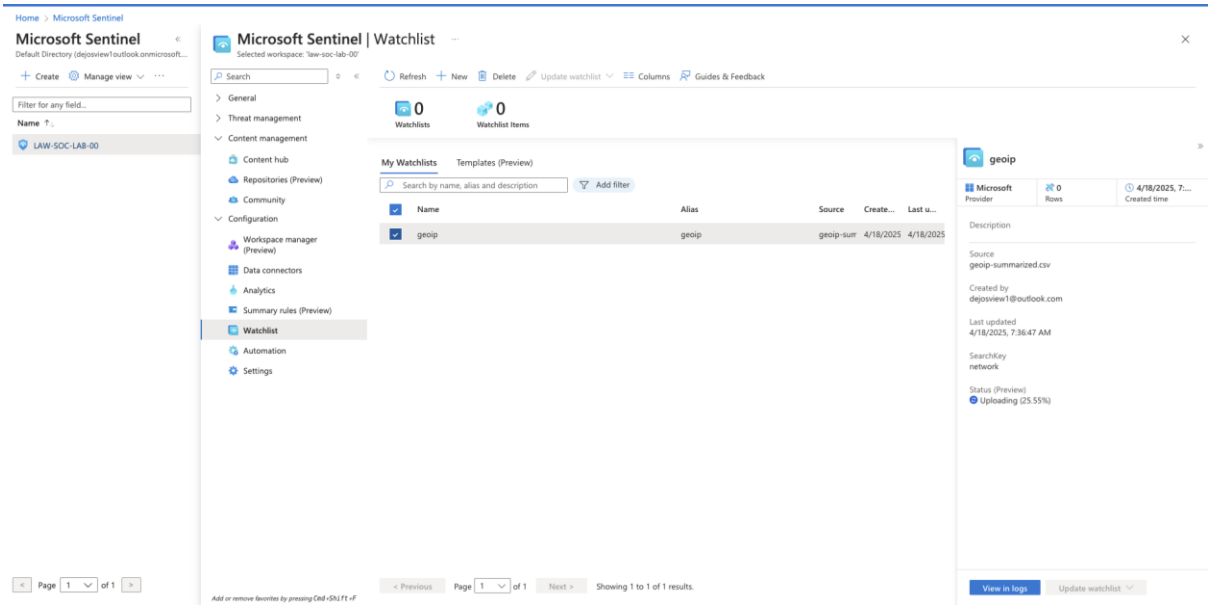
3) Browse and select the correct file that will be used. In this case it is the geoip-summarized.csv spreadsheet. For the SearchKey, choose network. Then proceed to review + create.



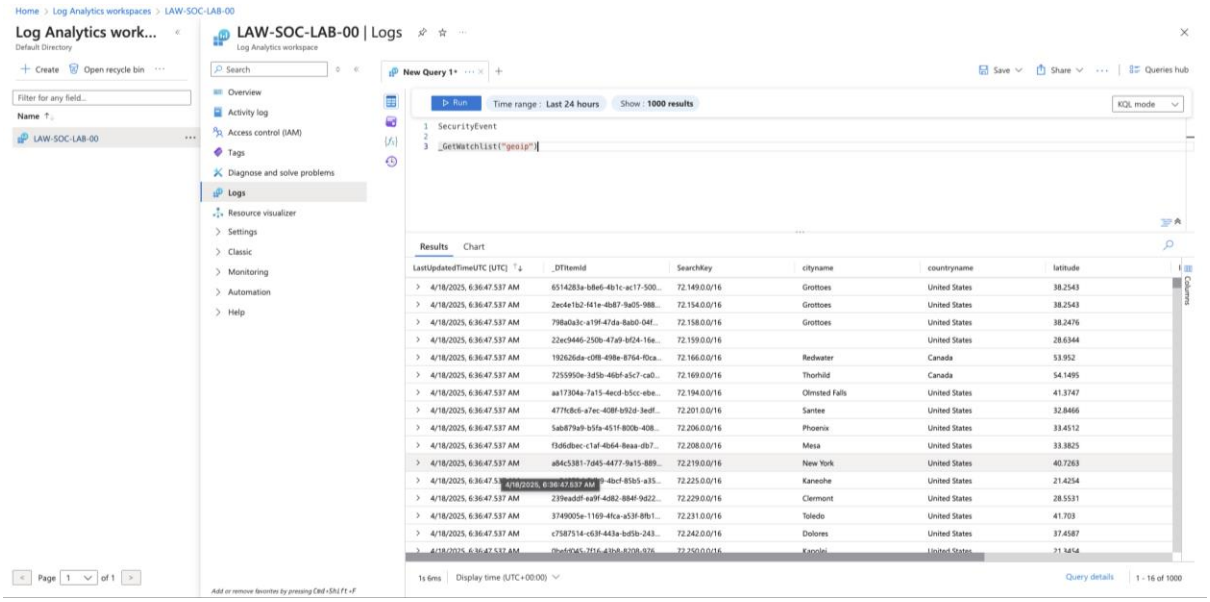
4) Click create.



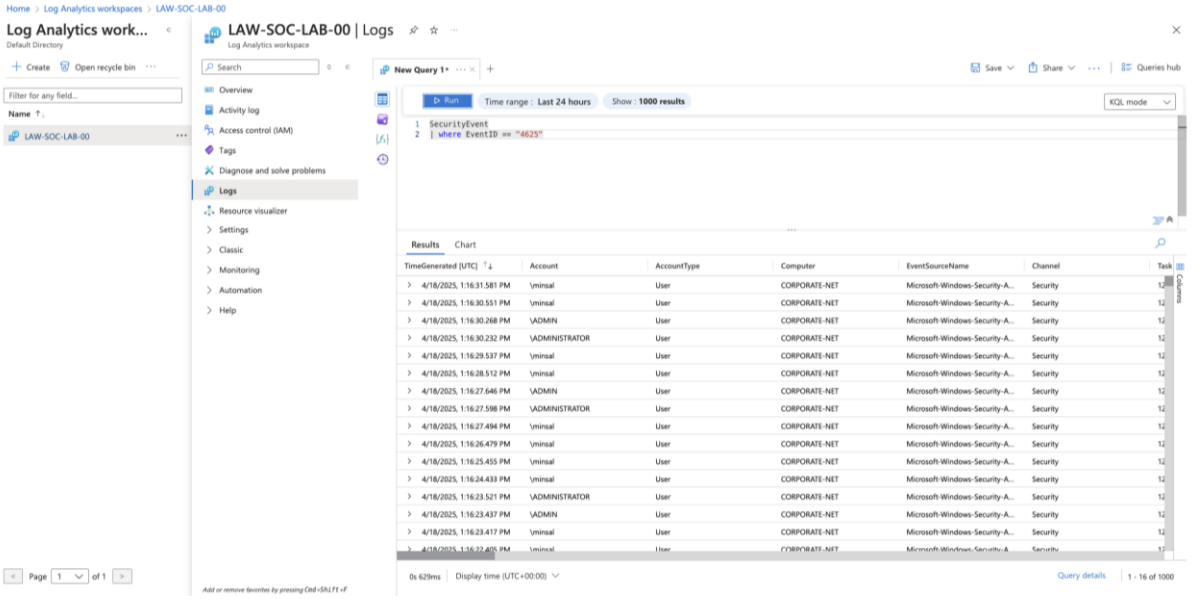
5) It is a regular occurance to be directed back to the Watchlist page by default. You may need to refresh the page to see the upload taking place.



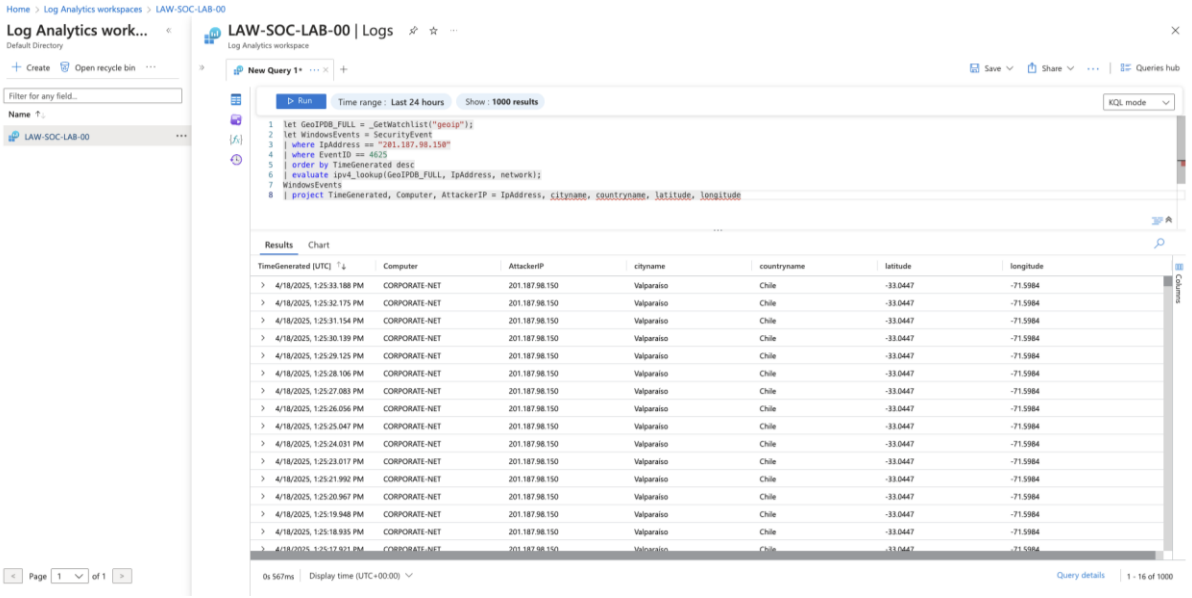
6) Whilst the upload is still taking place, you can go to the Log analytics. You will find when you use the query _GetWatchlist("geoip"), the headings for the log repository are identical to the headings found in the uploaded spreadsheet.



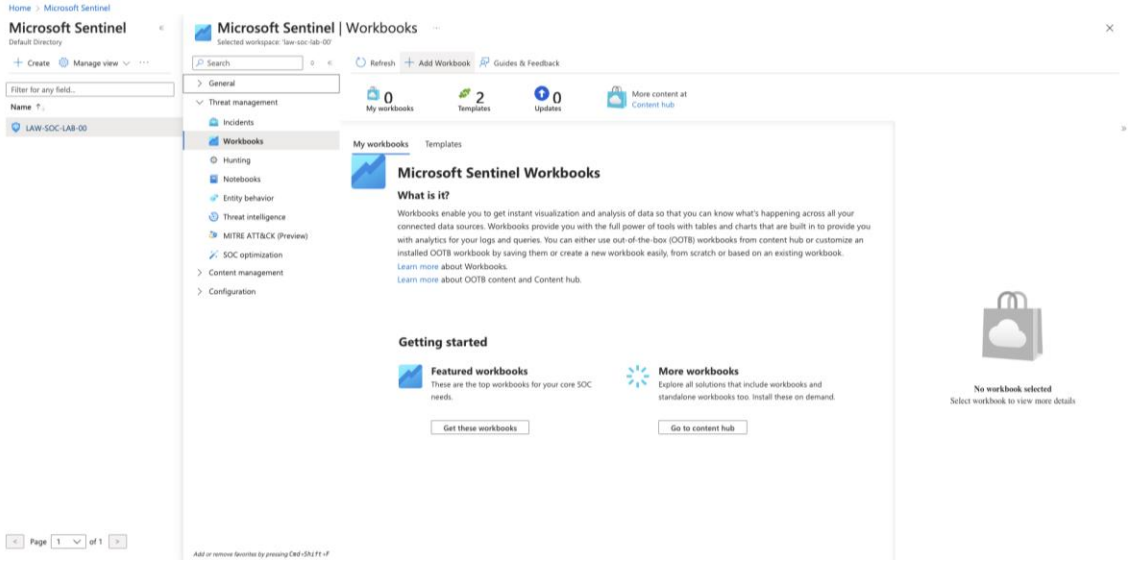
7) Use the query in the image below to copy an IpAddress .



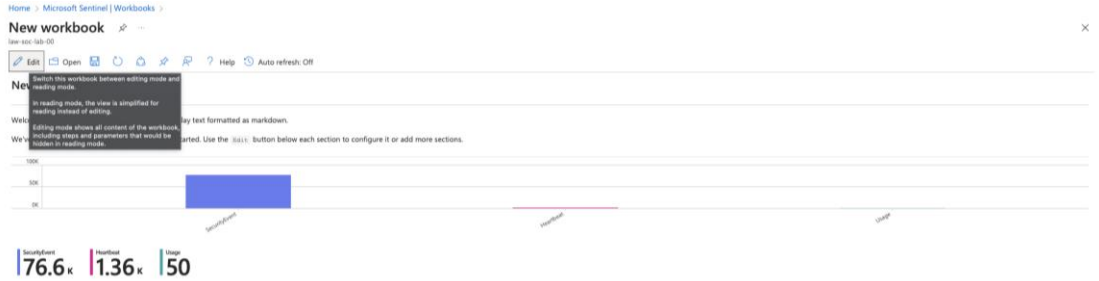
8) Copy this query but replace the IpAddress with the address you just copied during the previous step.
This query is showing the security logs with a specified IpAddress, along with limiting the columns to the select few.
order by TimeGenerated desc orders the logs from most to least recent.
AttackerIP = IpAddress renames the column, helping prevent confusion in terms of what is being observed.



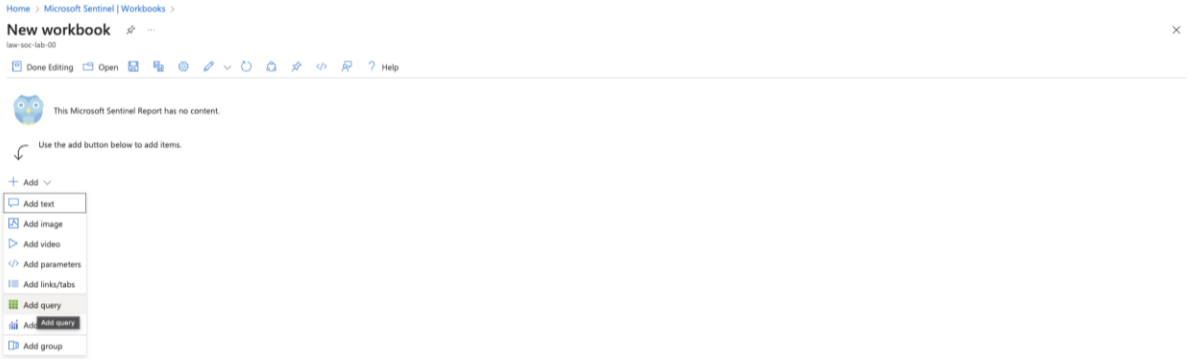
9) Go to Sentinel and select Workbooks



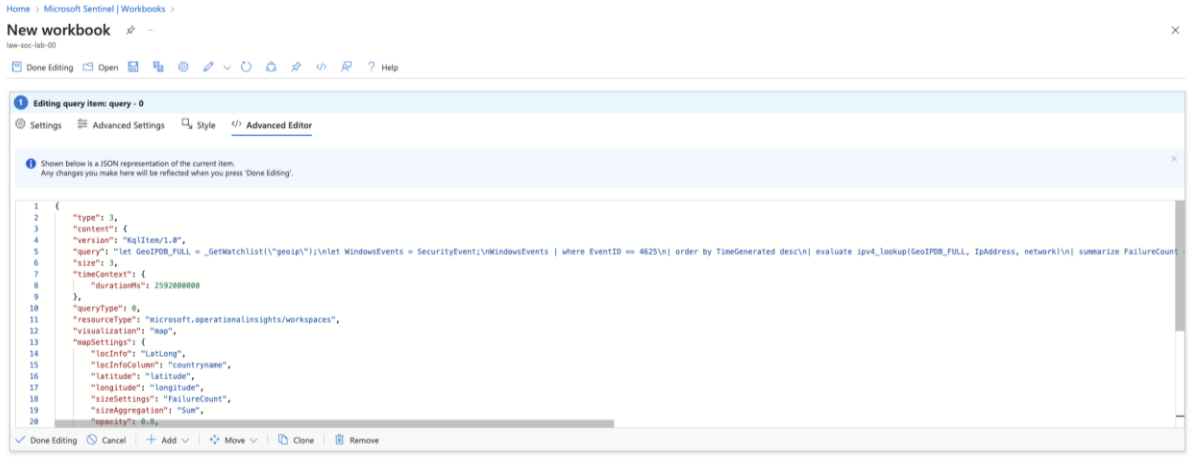
10) Click edit, then remove all the elements that are preset in the workbook.

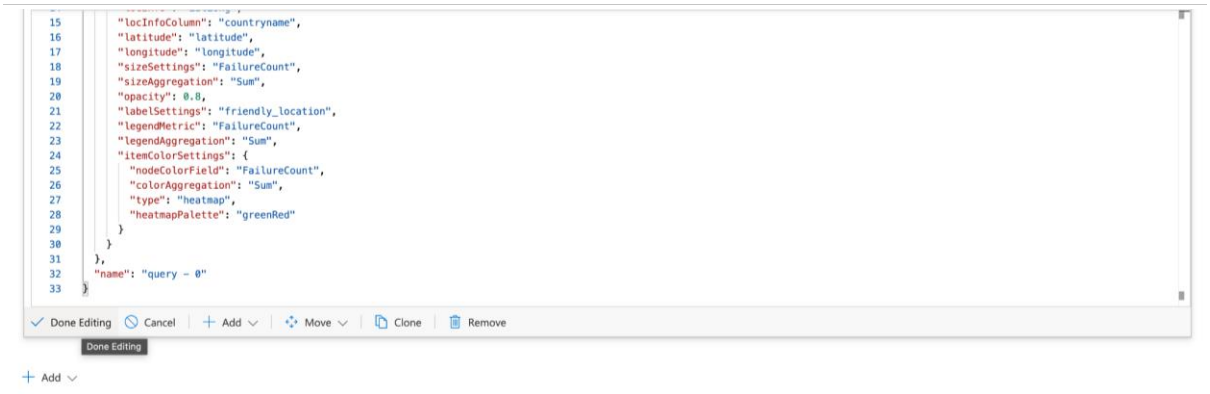


11) Select add, then click add query.

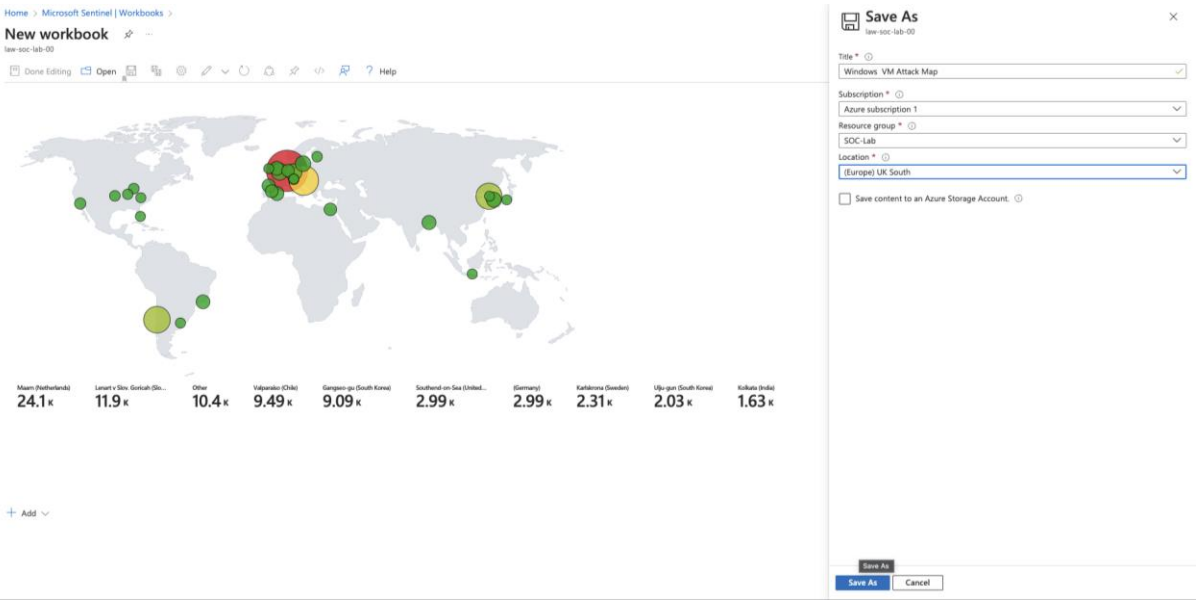


12) I pasted the text from a json file for the creation of the attack map.





13) Save the attack map, assigning it to the correct resource group.



Looking at the map, you can view the different areas attacks have derived from. The larger the circle, the more attacks have stemmed from the location. In the screenshot the large red circle is the Maarn, located in the Netherlands, with 24,000 failed login attempts into the honey pot.