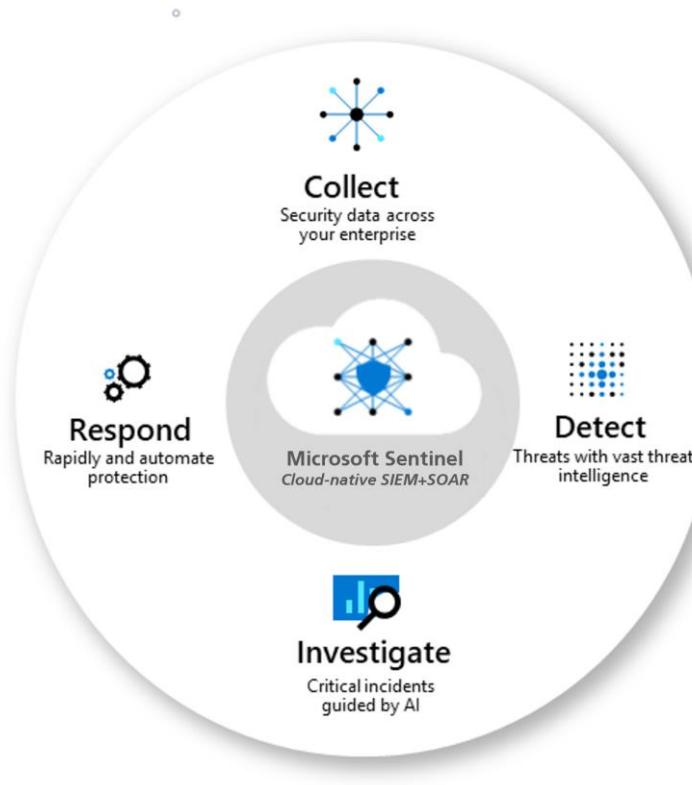


Microsoft Sentinel SIEM Lab

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.

The screenshot shows the Azure Resource Groups page. At the top, there is a header with 'Home > Resource groups ...'. Below the header, there are buttons for '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A note says 'You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.' There are filters for 'Subscription equals all' and 'Location equals all'. The main content area displays a message: 'No resource groups to display' with a small icon of a cube. Below the message, it says 'Resource groups provide a logical container to manage and organize Azure resources, simplifying administration and enabling efficient resource management.' There are 'Create' and 'Learn more' buttons. At the bottom, it says 'Showing 1 - 0 of 0. Display count: auto' and has a 'Give feedback' link.

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

The screenshot shows the 'Create a resource group' wizard in the 'Basics' step. At the top, there is a header with 'Home > Resource groups > Create a resource group ...'. Below the header, there are tabs for 'Basics', 'Tags', and 'Review + create'. A note about 'Resource group' is provided: 'A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.' There are fields for 'Subscription' (set to 'Azure subscription 1'), 'Resource group name' (set to 'SOC-Lab'), and 'Region' (set to '(Europe) UK South'). At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons.

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

The screenshot shows the Azure Resource Groups blade. On the left, there's a navigation bar with options like 'Create', 'Group by none', and a search bar. Below that is a list of existing resource groups, with 'SOC-Lab' selected. The main area is titled 'SOC-Lab' and shows the 'Overview' tab. It displays basic information: Subscription (Azure subscription 1), Subscription ID (edce9016-6fc6-4626-9f91-854d8cf9bf86), Tags (empty), and Location (UK South). A modal window titled 'Notifications' is open, showing a single event: 'Resource group created' (Creating resource group 'SOC-Lab' in subscription 'Azure subscription 1' succeeded). At the bottom of the main view, there's a message 'No resources match your filters' with a 'Create resources' button.

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

The screenshot shows the Azure Virtual Networks blade. The navigation bar includes 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A filter bar at the top allows filtering by 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. The main area shows a message 'No virtual networks to display' with a note: 'Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.' Below this is a 'Create virtual network' button and a 'Learn more' link. To the right, a 'Notifications' panel shows the same 'Resource group created' event as the previous screenshot, indicating the successful creation of the 'SOC-Lab' resource group.

- 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.

Home > Virtual networks >

Create virtual network

[Basic](#) [Security](#) [IP addresses](#) [Tags](#) [Review + create](#)

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[Learn more](#) [?](#)

Project details

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

Subscription * [Azure subscription 1](#)

Resource group * [SOC-Lab](#) [Create new](#)

Instance details

Virtual network name * [Net-SOC-lab](#)

Region * [\(Europe\) UK South](#)

[Deploy to an Azure Extended Zone](#)

[Previous](#) [Next](#) [Review + create](#) [Give feedback](#)

- 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:

Home >

Net-SOC-lab-1744945490145 | Overview

[Deployment](#)

[Search](#) [Delete](#) [Cancel](#) [Redeploy](#) [Download](#) [Refresh](#)

Overview

Your deployment is complete

Deployment name : Net-SOC-lab-1744945490145
Subscription : Azure subscription 1
Resource group : SOC-Lab

Start time : 4/18/2025, 4:05:15 AM
Correlation ID : 74733e88-d4d4-4252-a50e-225f7e99c3e9

[Deployment details](#) [Next steps](#) [Go to resource](#)

[Give feedback](#) [Tell us about your experience with deployment](#)

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
[Set up cost alerts >](#)

Microsoft Defender for Cloud
Secure your apps and infrastructure
[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials
[Start learning today >](#)

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
[Find an Azure expert >](#)

Add or remove favorites by pressing [Ctrl+Shift+F1+F2](#)

- 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.

The screenshot shows the Azure Resource Groups blade. The left sidebar lists 'Resource groups' with items: 'Name ?', 'NetworkWatcherRG', and 'SOC-Lab'. The main area is titled 'SOC-Lab' and shows an 'Overview' with the following details:

- Subscription (move) : Azure subscription 1
- Subscription ID : edce9016-6fc6-4626-9f91-854dbcf9b76
- Deployments : 1Succeeded
- Location : UK South
- Tags (edit) : Add tags

The 'Resources' section shows one item:

Name	Type	Location
Net-SOC-lab	Virtual network	UK South

At the bottom, there are navigation links: < Previous, Page 1 of 1, Next >, and a feedback link.

- 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.

The screenshot shows the Azure Compute Infrastructure | Virtual machines blade. The left sidebar lists 'Virtual machines' under 'Compute infrastructure' and includes 'Virtual Machine Scale Set (VMSS)', 'Compute Fleet (preview)', 'Disks + images', 'Capacity + placement', 'Related services', and 'Help'.

The main area displays a message: "No virtual machines to display. Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image." Below this is a large 'Create' button.

Below the 'Create' button, there are two 'Learn more at' links:

- Azure virtual machine: Create a virtual machine hosted by Azure
- Azure virtual machine configuration: Create a virtual machine with presets based on your workloads

At the bottom, there is a 'More VMs and related solutions' section with a 'Discover' button.

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.

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host Encryption at host is not registered for the selected subscription. [Learn more](#)

OS disk

OS disk size Image default (127 GiB) Premium SSD (locally-redundant storage)

OS disk type * Premium SSD (locally-redundant storage) Standard SSD (locally-redundant storage)

Delete with VM

Key management Platform-managed key Customer-managed key

Enable Ultra Disk compatibility

Data disks for CORPORATE-NET

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
0	[new] CORPORATE-NET-disk0	100	Premium SSD (locally-redundant storage)	None	<input type="checkbox"/>

Create and attach a new disk [Attach an existing disk](#)

Advanced

< Previous Next : Networking > Review + create

Give feedback

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

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

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

Virtual network * Net-SOC-lab Create new

Subnet * default (10.0.0.0/24) Manage subnet configuration

Public IP [new] CORPORATE-NET-ip Create new

NIC network security group None Basic Advanced

Public inbound ports * None Allow selected ports

Select inbound ports * RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted

Enable accelerated networking

Load balancing

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

Load balancing options None Azure load balancer Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.

< Previous Next : Management > Review + create

Give feedback

13) The management page does not require any changes.

The screenshot shows the 'Management' tab of the Azure VM creation wizard. It includes sections for Microsoft Defender for Cloud, basic plan selection, Identity (system assigned managed identity), Microsoft Entra ID (with RBAC role assignment), Auto-shutdown, Backup, Site Recovery, Guest OS updates, and Diagnostics (with Boot diagnostics set to 'Disable'). Buttons at the bottom include '< Previous', 'Next : Monitoring >', 'Review + create', and 'Give feedback'.

14) I chose to disable boot diagnostics.

The screenshot shows the 'Monitoring' tab of the Azure VM creation wizard. It includes sections for Alerts (recommended alert rules), Diagnostics (Boot diagnostics set to 'Disable'), and Health (application health monitoring). Buttons at the bottom include '< Previous', 'Next : Advanced >', 'Review + create', and 'Give feedback'.

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:

The screenshot shows the Azure portal's VM deployment overview. The main panel displays a green checkmark indicating the deployment is complete. It provides details such as the deployment name (CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20250418042057), subscription (Azure subscription 1), resource group (SOC-Lab), start time (4/18/2025, 4:47:30 AM), and correlation ID (af68d310-65f4-4e9f-a2ae-dad8369a10e9). Below this, sections for deployment details and next steps are shown, along with links to Go to resource and Create another VM. A feedback link is also present. To the right, there are promotional cards for Cost Management, Microsoft Defender for Cloud, and Free Microsoft tutorials.

- 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.

The screenshot shows the Azure portal's Resource Groups blade for the 'SOC-Lab' group. The left sidebar lists resources like NetworkWatcherRG and SOC-Lab. The main pane shows the 'Overview' tab for the SOC-Lab resource group, which includes activity logs, access control (IAM), tags, and a resource visualizer. The 'Resources' tab is selected, displaying a list of resources including a Virtual machine (Public IP address), Network security group, Network interface, Disk, and Virtual network. The list is filtered by Type equals all and Location equals all. At the bottom, there are navigation links for previous, next, and a feedback link.

- 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.

Custom security rules : 1 inbound, 0 outbound
Associated with : 0 subnets, 1 network interfaces

- 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.

Add inbound security rule
Source: Any
Destination: Any
Protocol: Any
Action: Allow
Priority: 100
Name: DANGER_AllowAnyCustomAnyInbound
Description:

Add inbound security rule
Source: Any
Destination: Any
Protocol: Any
Action: Deny
Priority: 100
Name: DANGER_AllowAnyCustomAnyInbound
Description:

Add inbound security rule
Source: Any
Destination: Any
Protocol: Any
Action: Allow
Priority: 100
Name: DANGER_AllowAnyCustomAnyInbound
Description:

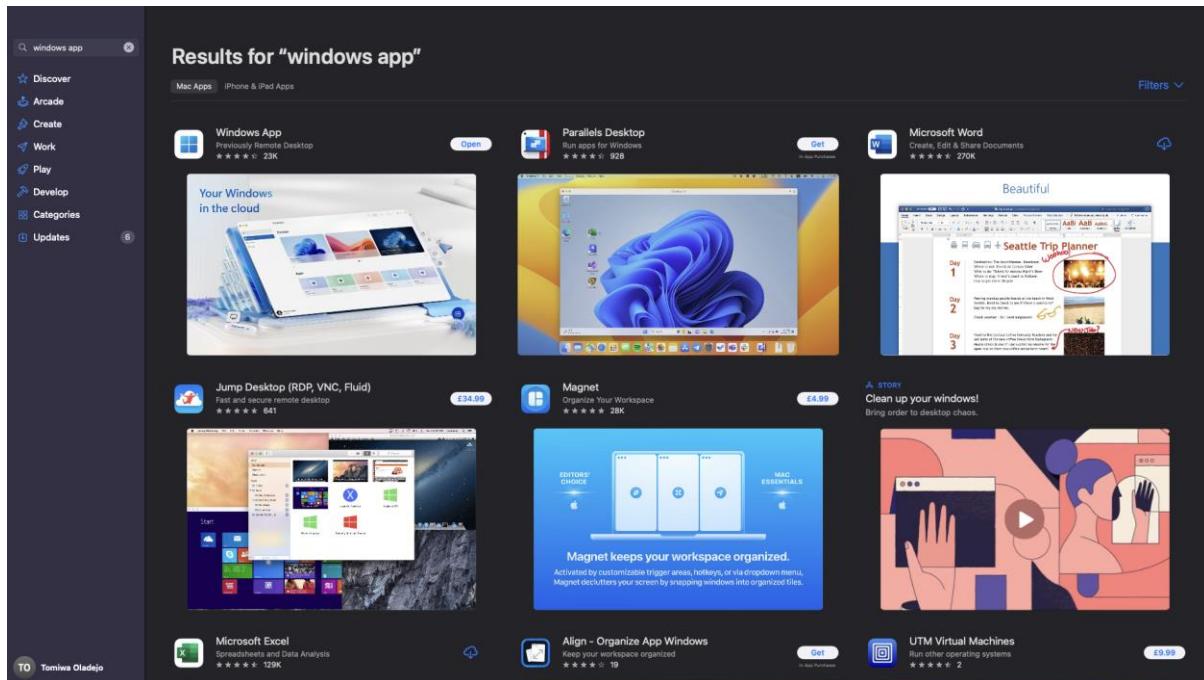
MS SQL DB port 1433 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

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.

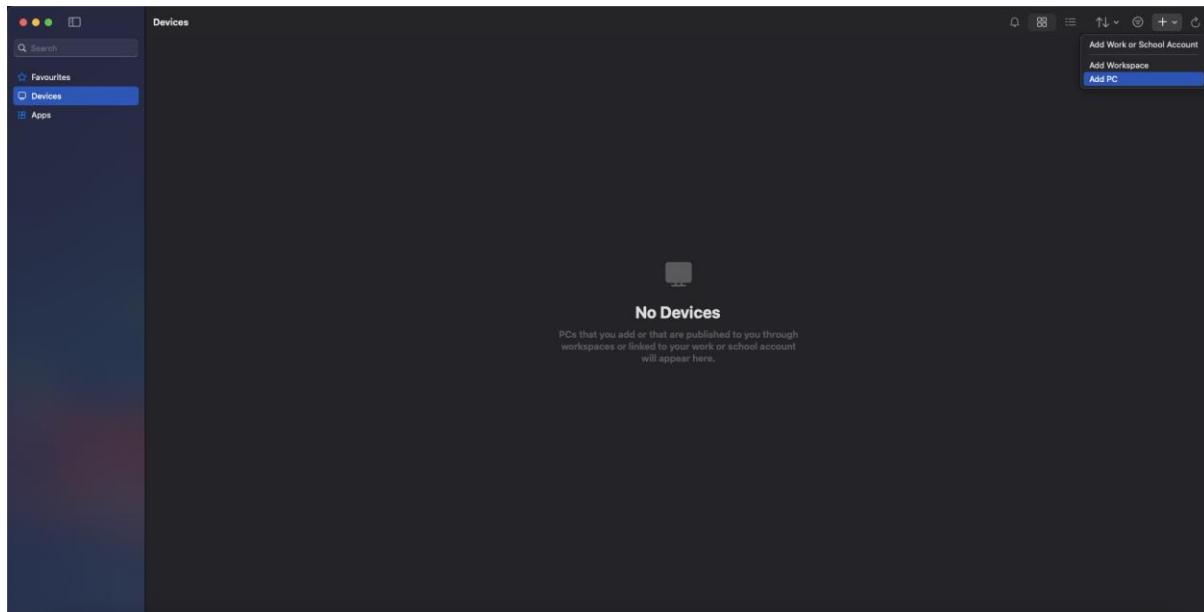
MySQL DB port 3306 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

PostgreSQL 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.

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.

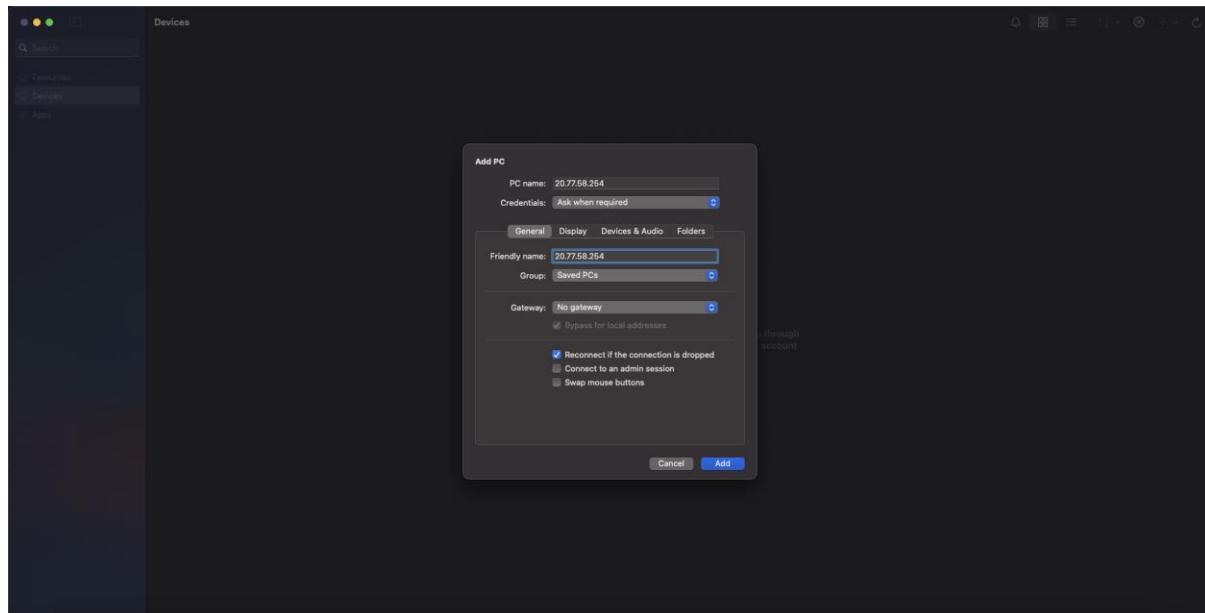


20) Open the windows app after it has installed and select add PC.

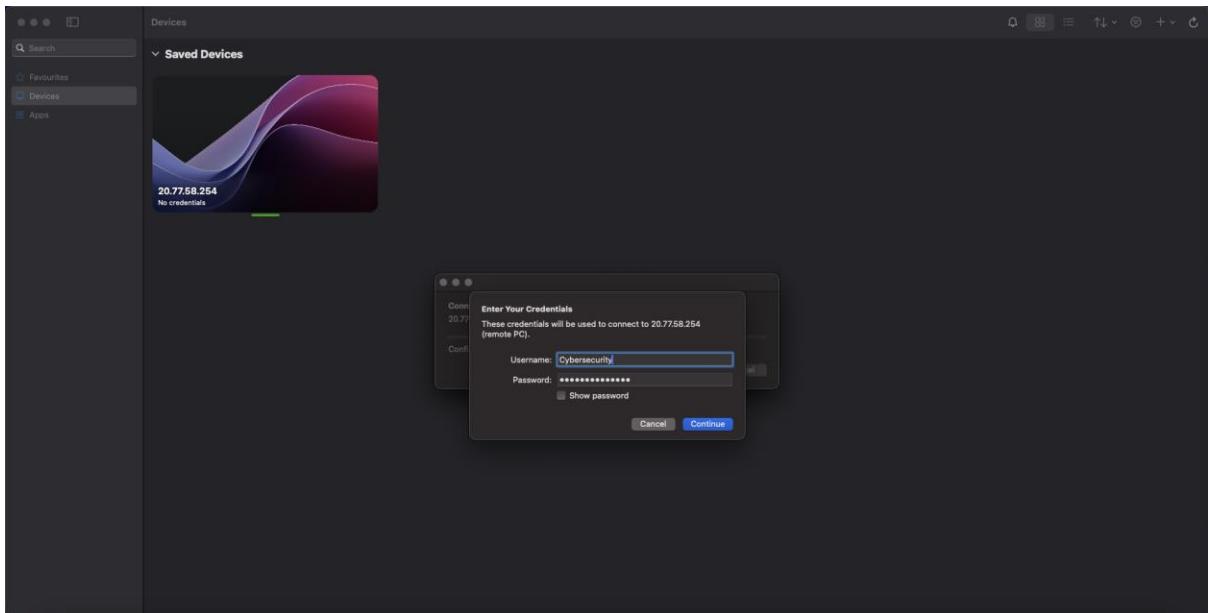


- 21) You will be prompted to enter the public IP address for the virtual machine. This can be found in the overview section of the virtual machine that you created. Once located, copy and paste the public IP address into the “PC name” section. Make sure the credentials are set to ask when required,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

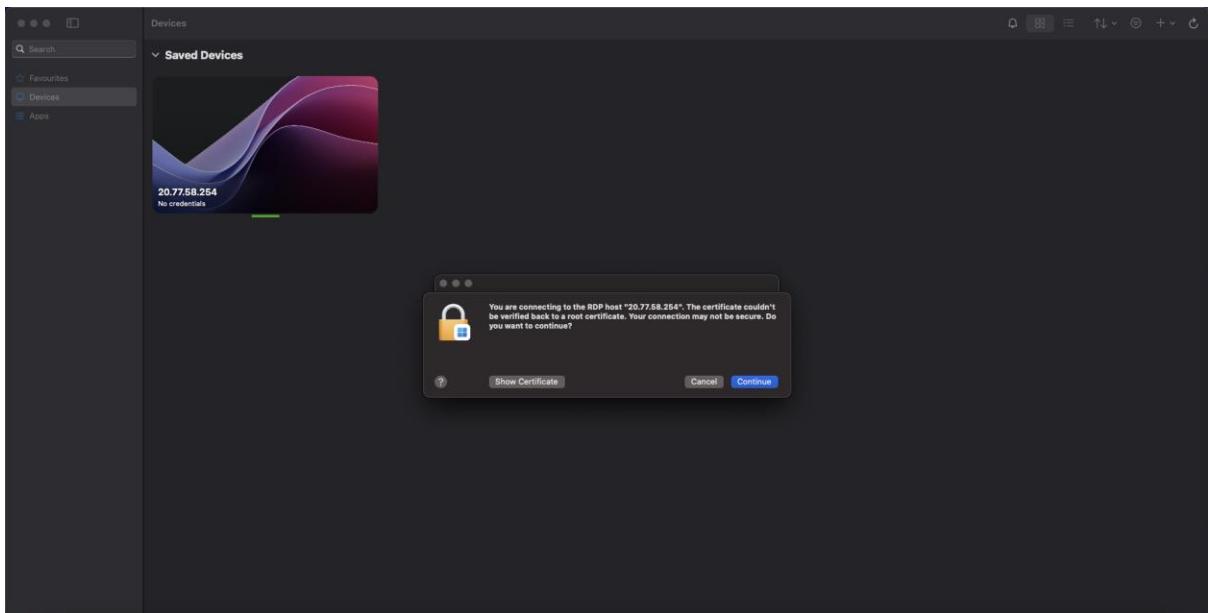
The screenshot shows the Azure Compute Infrastructure Virtual Machines blade. On the left, a navigation pane includes 'Virtual machines' under 'Infrastructure'. The main area displays the 'CORPORATE-NET' VM details. The 'Overview' tab is selected, showing the VM's status as 'Running', location as 'UK South (Zone 1)', and operating system as 'Windows (Windows 10 Pro)'. It also lists network information like 'Public IP address: 20.77.58.254' and 'Virtual network/subnet: Net-SOC-lab/default'. The 'Networking' section shows the VM has a public IP of 20.77.58.254 and is connected to a network interface named 'corporate-net272_z1'. The 'Size' section indicates it's a Standard D4s v3 VM with 4 vCPUs and 16 GB RAM. The 'Source image details' section shows the VM was created from the 'Windows-10' image offer by Microsoft Windows Desktop.



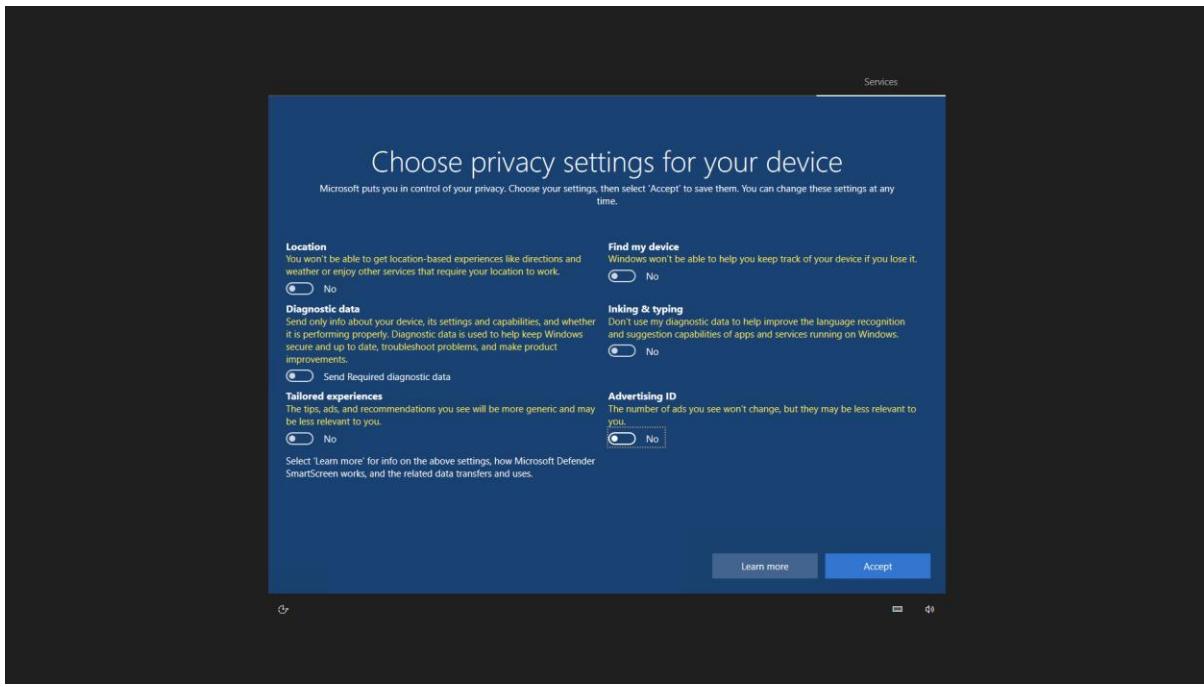
- 22) Enter the username and password that has been set for the virtual machine.



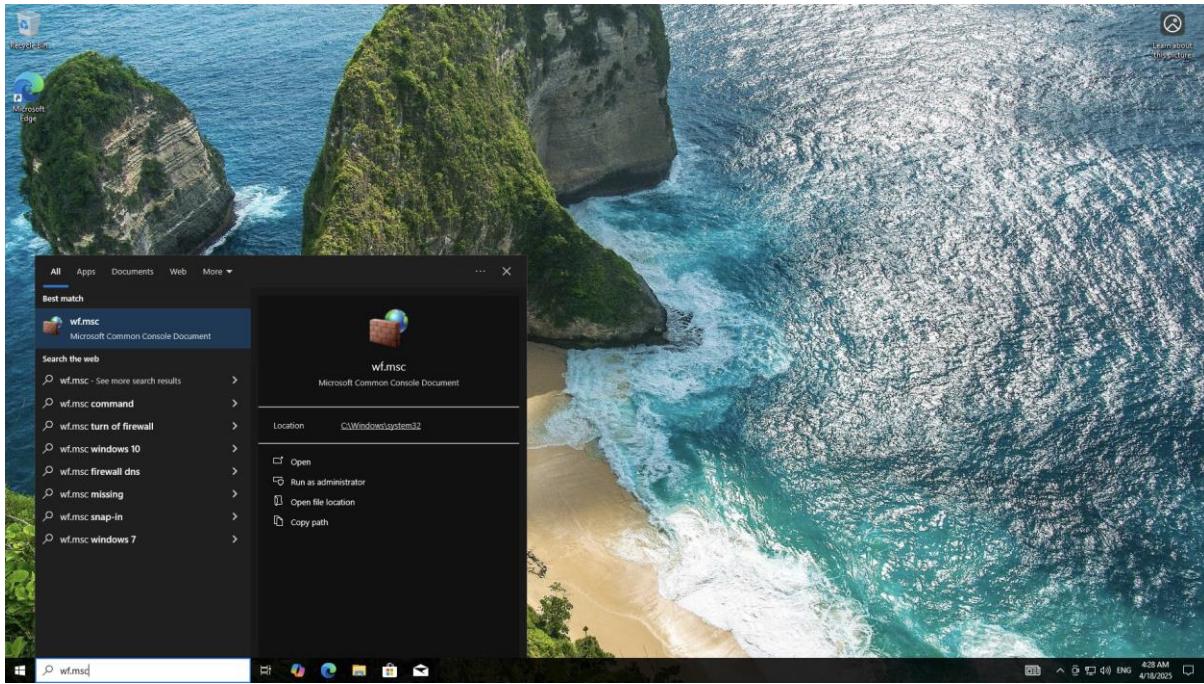
23) Click continue.



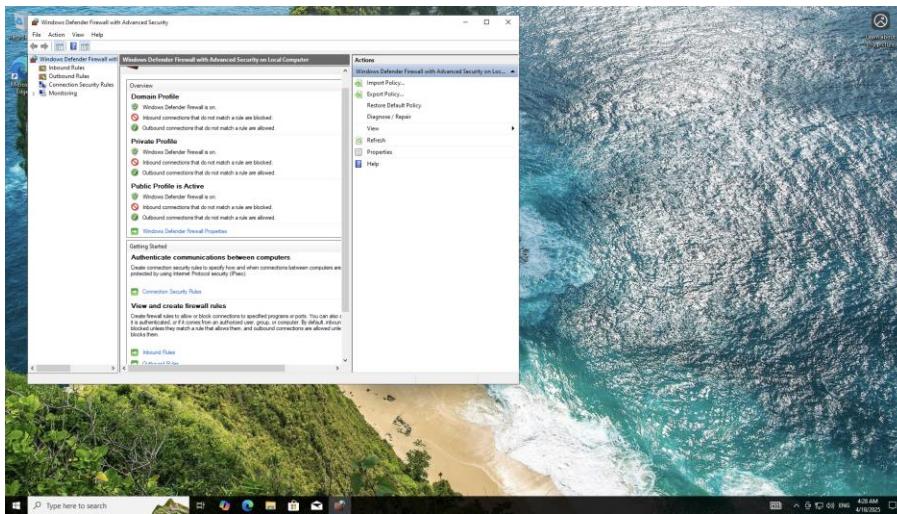
24) Select no for all options.



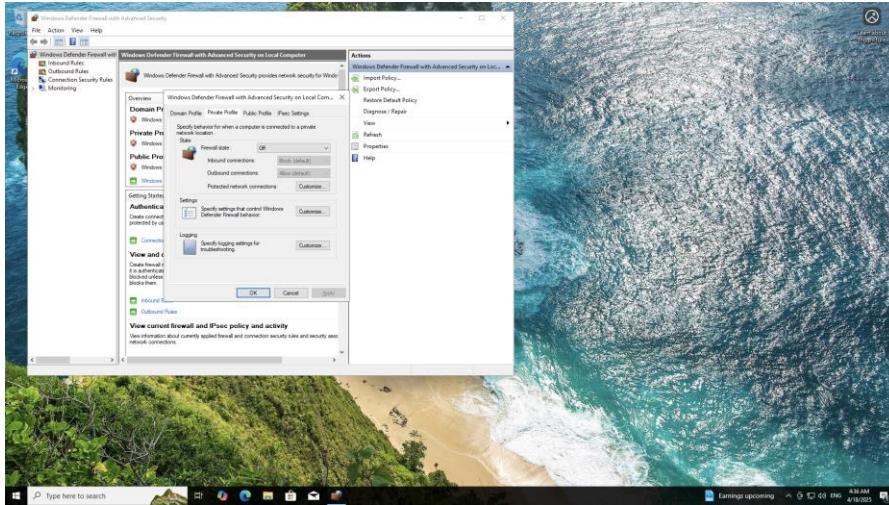
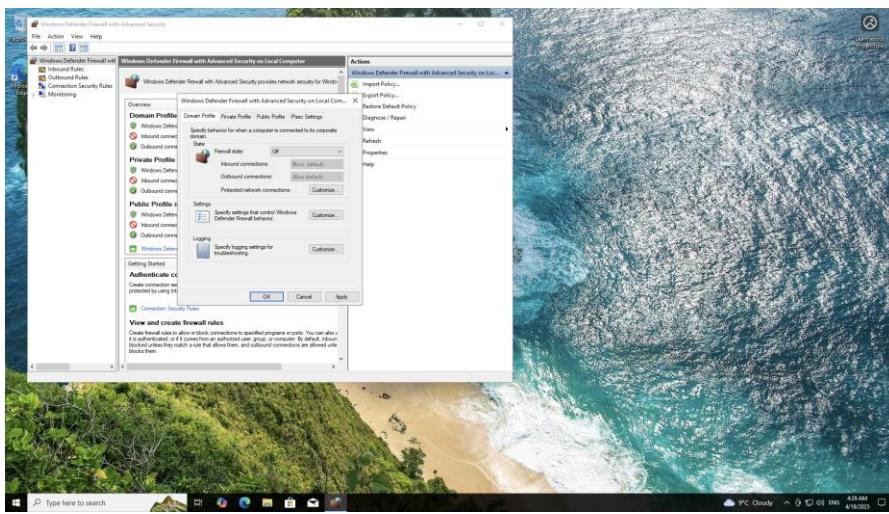
25) Now that we are logged into the virtual machine, the next step is to disable the firewall. So type wf.msc in the search bar below.

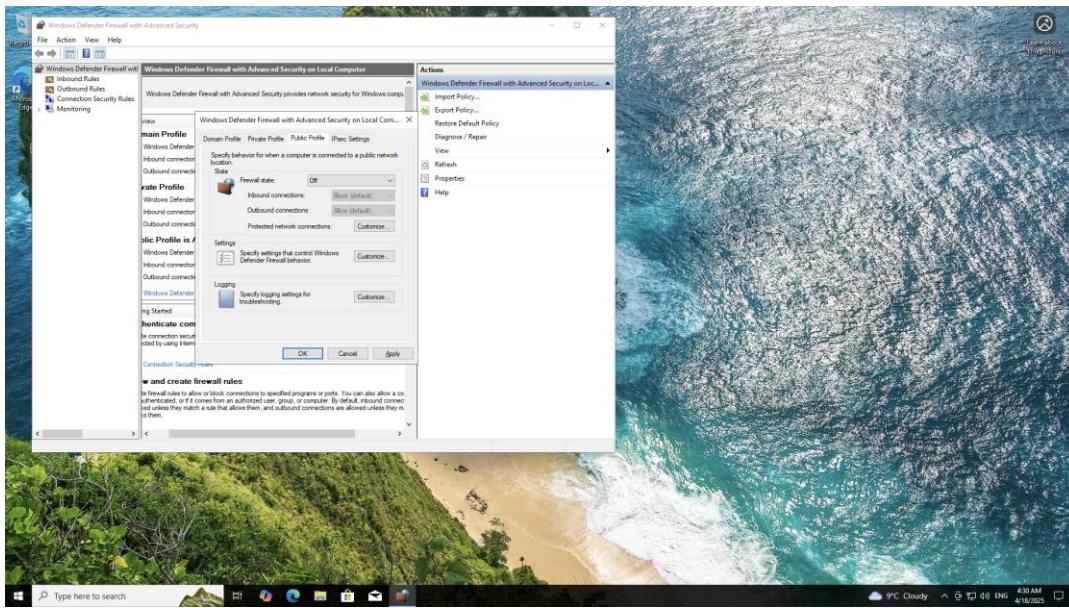


26) "Windows Defender Firewall with Advanced Security" should open.



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.

Operating system	Windows (Windows 10 Pro)
Size	Standard D4s v3
Public IP address	20.77.58.254
Virtual network/subnet	Net-SOC-lab/default
DNS name	Not configured
Health state	Up
Time created	4/18/2025, 3:47 AM UTC
Networking	
Public IP address	20.77.58.254 (Network interface)
Private IP address (IPv6)	-
Private IP address (IPv4)	10.0.0.4
Virtual network/subnet	Net-SOC-lab/default
DNS name	Configure
Size	
Size	Standard D4s v3
vCPUs	4
RAM	16 GiB
Source image details	
Source image publisher	MicrosoftWindowsDesktop
Source image offer	Windows-10

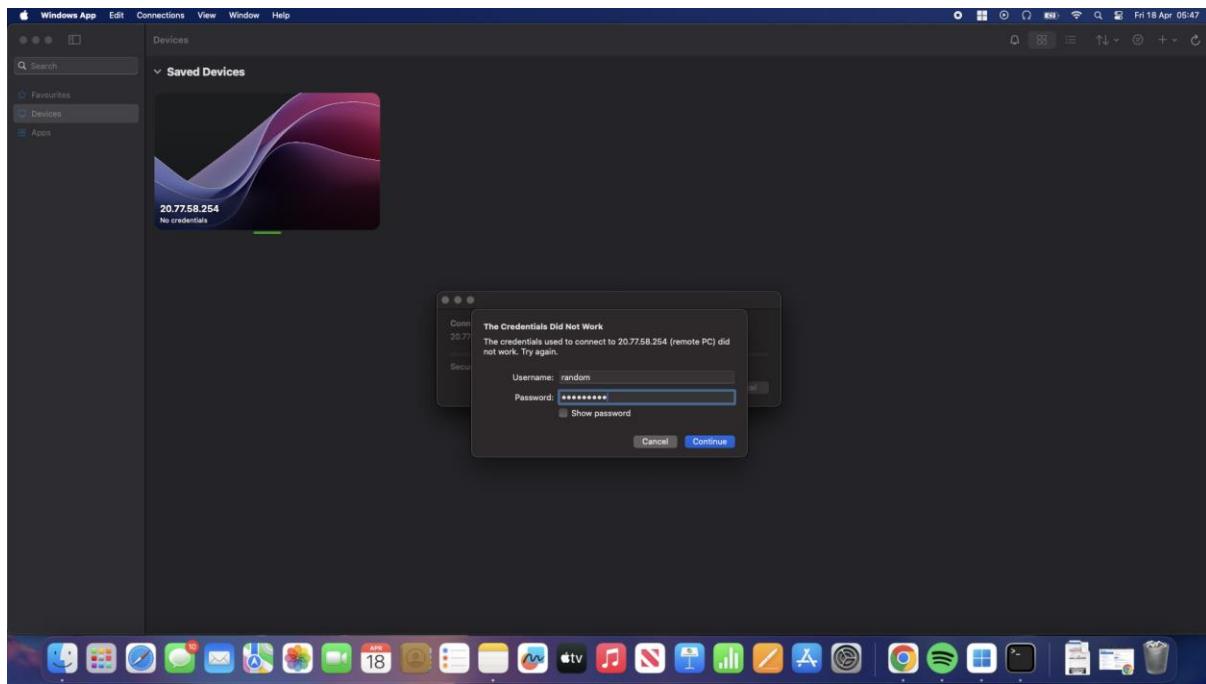
29) Once the terminal has opened, type “ping” press spacebar and then enter the public IP address for the virtual machine. Click enter and you should see bytes being returned from the IP address.

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.

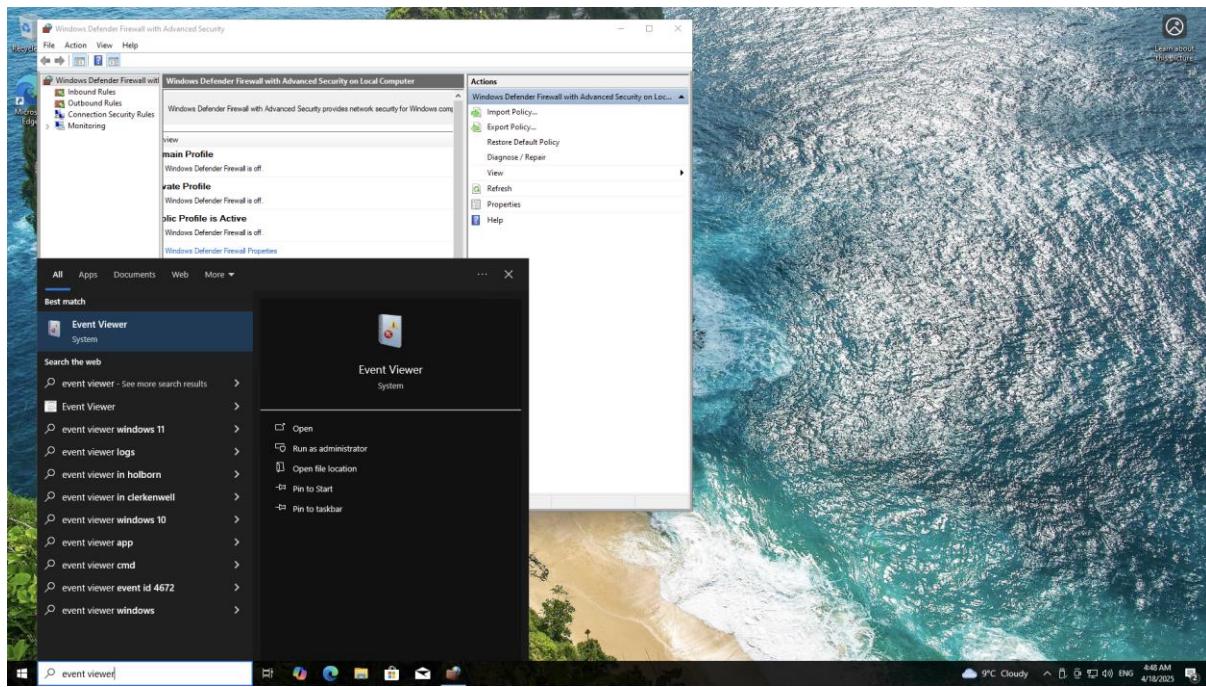
```
Last login: Wed Mar 12 11:31:07 on console
tomy@TomyMacBook-Air ~ % ping 29.77.58.254
```

```
64 bytes from 29.77.58.254: icmp_seq=169 ttl=158 time=11.487 ms
64 bytes from 29.77.58.254: icmp_seq=170 ttl=158 time=12.180 ms
64 bytes from 29.77.58.254: icmp_seq=171 ttl=158 time=11.425 ms
64 bytes from 29.77.58.254: icmp_seq=172 ttl=158 time=12.735 ms
64 bytes from 29.77.58.254: icmp_seq=173 ttl=158 time=11.482 ms
64 bytes from 29.77.58.254: icmp_seq=174 ttl=158 time=11.444 ms
64 bytes from 29.77.58.254: icmp_seq=175 ttl=158 time=11.848 ms
64 bytes from 29.77.58.254: icmp_seq=176 ttl=158 time=11.444 ms
64 bytes from 29.77.58.254: icmp_seq=177 ttl=158 time=12.433 ms
64 bytes from 29.77.58.254: icmp_seq=178 ttl=158 time=12.966 ms
64 bytes from 29.77.58.254: icmp_seq=179 ttl=158 time=11.553 ms
64 bytes from 29.77.58.254: icmp_seq=180 ttl=158 time=13.186 ms
64 bytes from 29.77.58.254: icmp_seq=181 ttl=158 time=10.384 ms
64 bytes from 29.77.58.254: icmp_seq=182 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=183 ttl=158 time=14.579 ms
64 bytes from 29.77.58.254: icmp_seq=184 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=185 ttl=158 time=11.477 ms
64 bytes from 29.77.58.254: icmp_seq=186 ttl=158 time=11.857 ms
64 bytes from 29.77.58.254: icmp_seq=187 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=188 ttl=158 time=11.116 ms
64 bytes from 29.77.58.254: icmp_seq=189 ttl=158 time=13.483 ms
64 bytes from 29.77.58.254: icmp_seq=190 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=191 ttl=158 time=10.884 ms
64 bytes from 29.77.58.254: icmp_seq=192 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=193 ttl=158 time=10.329 ms
64 bytes from 29.77.58.254: icmp_seq=194 ttl=158 time=12.774 ms
64 bytes from 29.77.58.254: icmp_seq=195 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=196 ttl=158 time=11.378 ms
64 bytes from 29.77.58.254: icmp_seq=197 ttl=158 time=11.853 ms
64 bytes from 29.77.58.254: icmp_seq=198 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=199 ttl=158 time=12.491 ms
64 bytes from 29.77.58.254: icmp_seq=200 ttl=158 time=11.158 ms
64 bytes from 29.77.58.254: icmp_seq=201 ttl=158 time=12.176 ms
64 bytes from 29.77.58.254: icmp_seq=202 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=203 ttl=158 time=10.579 ms
64 bytes from 29.77.58.254: icmp_seq=204 ttl=158 time=11.197 ms
64 bytes from 29.77.58.254: icmp_seq=205 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=206 ttl=158 time=14.935 ms
64 bytes from 29.77.58.254: icmp_seq=207 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=208 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=209 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=210 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=211 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=212 ttl=158 time=10.471 ms
64 bytes from 29.77.58.254: icmp_seq=213 ttl=158 time=13.328 ms
64 bytes from 29.77.58.254: icmp_seq=214 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=215 ttl=158 time=12.625 ms
64 bytes from 29.77.58.254: icmp_seq=216 ttl=158 time=9.962 ms
64 bytes from 29.77.58.254: icmp_seq=217 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=218 ttl=158 time=11.746 ms
64 bytes from 29.77.58.254: icmp_seq=219 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=220 ttl=158 time=10.297 ms
64 bytes from 29.77.58.254: icmp_seq=221 ttl=158 time=10.731 ms
64 bytes from 29.77.58.254: icmp_seq=222 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=223 ttl=158 time=11.811 ms
64 bytes from 29.77.58.254: icmp_seq=224 ttl=158 time=12.171 ms
64 bytes from 29.77.58.254: icmp_seq=225 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=226 ttl=158 time=9.901 ms
64 bytes from 29.77.58.254: icmp_seq=227 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=228 ttl=158 time=12.419 ms
64 bytes from 29.77.58.254: icmp_seq=229 ttl=158 time=12.338 ms
64 bytes from 29.77.58.254: icmp_seq=230 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=231 ttl=158 time=12.491 ms
64 bytes from 29.77.58.254: icmp_seq=232 ttl=158 time=10.812 ms
64 bytes from 29.77.58.254: icmp_seq=233 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=234 ttl=158 time=12.785 ms
64 bytes from 29.77.58.254: icmp_seq=235 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=236 ttl=158 time=12.595 ms
64 bytes from 29.77.58.254: icmp_seq=237 ttl=158 time=11.858 ms
64 bytes from 29.77.58.254: icmp_seq=238 ttl=158 time=11.453 ms
64 bytes from 29.77.58.254: icmp_seq=239 ttl=158 time=12.848 ms
--C
-- 29.77.58.254 ping statistics --
248 packets transmitted, 248 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.794/11.979/28.612/1.567 ms
tomy@TomyMacBook-Air ~ %
```

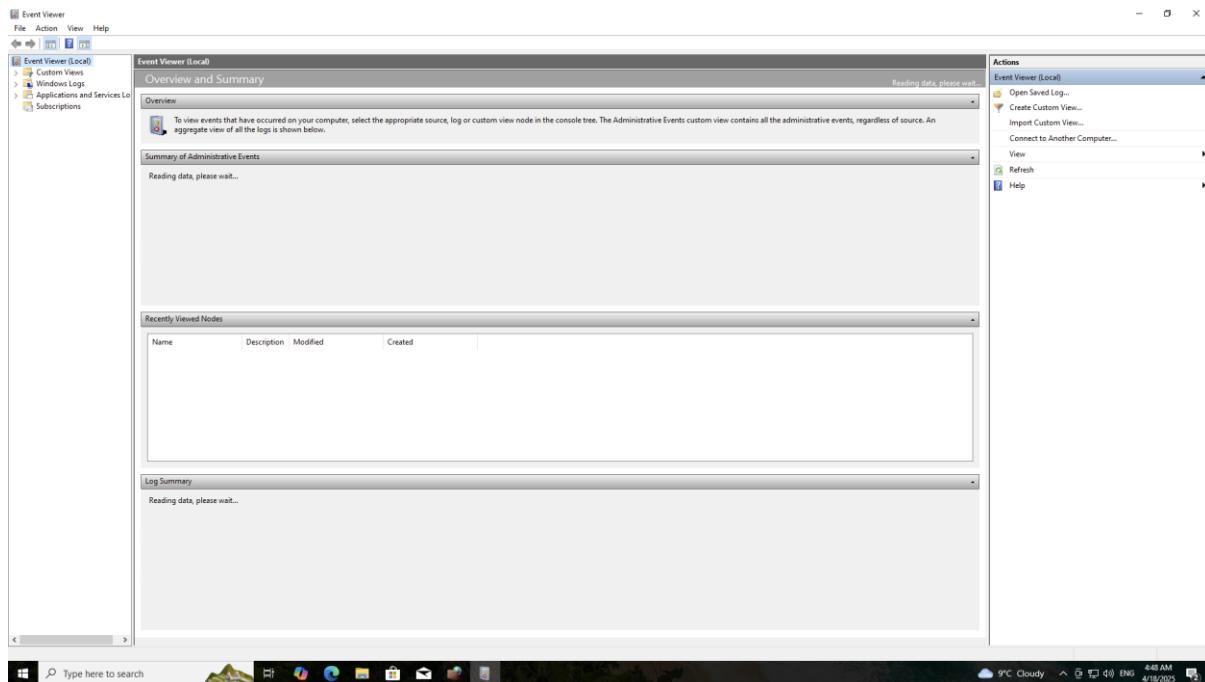
30) Next, log out of the virtual machine account, and intentionally enter incorrect credential a few times to fail the login attempt.



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

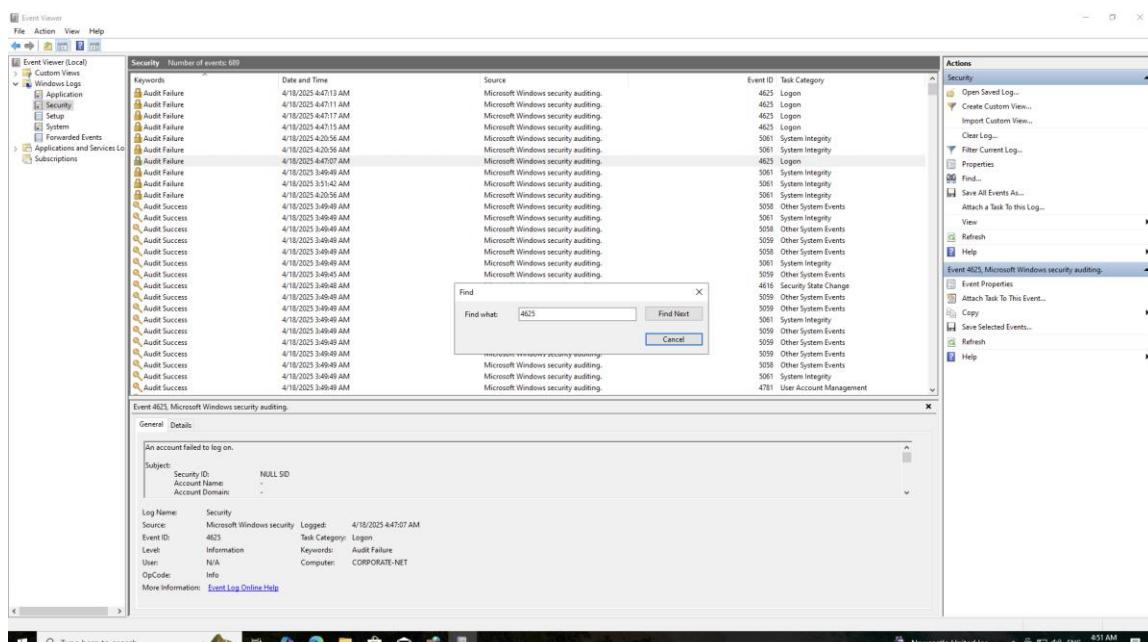


32) If anything happens on the computer, it gets logged. There are certain configurations that can be used to log specific activities, but there are already default settings in place that log activities, which is what we will be viewing.



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.

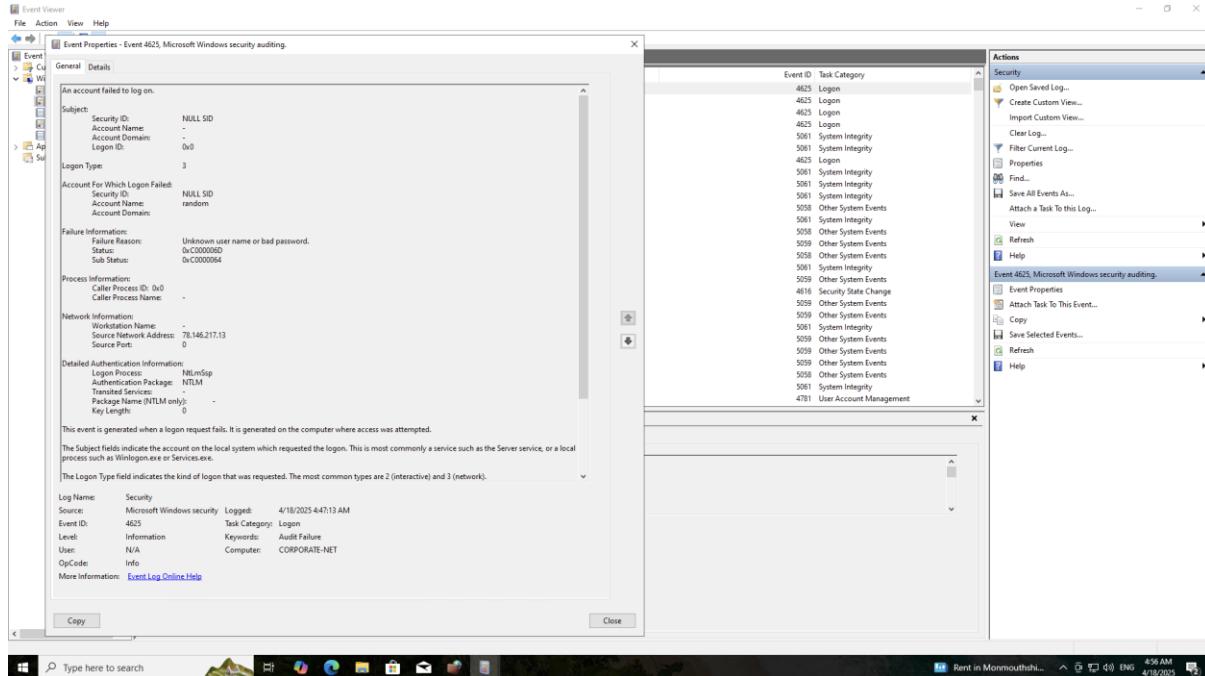
In the screenshot below I searched for the events with the ID “4625” using **ctrl + f**. This event ID number is given to failed login attempts.



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

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists categories like Windows Logs, Application, Security, System, and Forwarded Events. The main pane displays a list of security events with columns for Date and Time, Source, Event ID, and Task Category. A 'Filter Current Log' dialog box is open in the center, allowing users to refine their search by time, event level (Critical, Warning, Error, Information), log source (Security), task category (e.g., Logon, System Integrity), keywords, user, and computer. The 'Event ID' dropdown in the dialog is set to '4625'. The right pane shows the context menu for a selected event (Event 4625, Microsoft Windows security auditing), which includes options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To This Log..., View, Refresh, Help, Event Properties, Attach Task To This Event..., Save Selected Events..., Copy, Refresh, and Help. The taskbar at the bottom shows the date and time as 4/18/2025 5:01 AM.

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.

The screenshot shows the Microsoft Azure portal search results for 'log analytics workspace'. The search bar at the top contains the query. The results page shows a list of items under 'All' category, including:

- Services (28)**: Log Analytics workspaces, Activity log, Log Analytics query packs, Firmware analysis workspaces.
- Marketplace (1)**: Log Analytics Workspace.
- Documentation**: Create Log Analytics workspaces - Azure Monitor, Log Analytics workspace overview - Azure Monitor, Manage tables in a Log Analytics workspace - Azure Monitor, Log Analytics Workspace Insights - Azure Monitor.

At the bottom, there is a link to 'Continue searching in Microsoft Entra ID' and a note: 'Leverage unified authentication with Microsoft Entra ID'.

<https://portal.azure.com/#blade/HubsExtension/BrowseResourceBlade/resourceType/Microsoft.OperationalInsights/%2Fworkspaces>

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.

Home > Log Analytics workspaces >

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 * Resource group *

Instance details

Name * Region *

Review + Create

Home > Microsoft.LogAnalyticsOMS | Overview

Deployment

Search

Overview

Your deployment is complete

Deployment name : MicrosoftLogAnalyticsOMS
Subscription : Azure subscription 1
Resource group : SOC-Lab

Start time : 4/18/2025, 6:20:30 AM
Correlation ID : 34a26c34-c700-421e-a7b8-fa5a677fb32d

Deployment details

Next steps

[Go to resource](#)

Give feedback

Add or remove favorites by pressing **Ctrl+Shift+T** ↴

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
[Set up cost alerts >](#)

Microsoft Defender for Cloud
Secure your apps and infrastructure
[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials
[Start learning today >](#)

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
[Find an Azure expert >](#)

Creating Microsoft Sentinel

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

The screenshot shows the Microsoft Sentinel workspace selection screen. The 'Microsoft Sentinel' workspace is highlighted in the list of resources. The interface includes navigation links like 'Home', 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'View incidents'. There are filters for 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. A search bar at the top says 'Filter for any field...'. The right side of the screen shows a detailed view of the selected workspace, including its service type (Microsoft Sentinel), resource type (Microsoft Cache/RedisEnterprise), and various configuration options like 'Language', 'Azure Managed Redis (Preview)', and 'Twilio SendGrid'. A 'Documentation' section is also present.

The screenshot shows the 'Add Microsoft Sentinel to a workspace' dialog box. It displays the workspace 'LAW-SOC-LAB-00' with location 'uksouth', resource group 'soc-lab', subscription 'Azure subscription 1', and directory 'Default Directory'. At the bottom, there are 'Add' and 'Cancel' buttons.

- 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.

The screenshot shows the Microsoft Sentinel Content hub interface. At the top, there are statistics: 385 Solutions, 307 Standalone contents, 0 Installed, and 0 Updates. A search bar is present with the query "security event". The main area displays a table of security events, with one entry for "Windows Security Events" marked as "Installed". On the right side, a detailed view of the "Windows Security Events" connector is shown, including its provider (Microsoft), support (Microsoft Support), and version (3.0.9). It also includes notes about the connector's functionality and compatibility.

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

This screenshot is identical to the previous one, showing the Microsoft Sentinel Content hub with the Windows Security Events connector installed. The "Manage" button is visible at the bottom right of the connector's details panel.

- 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”.

The screenshot shows the Microsoft Sentinel Content hub interface. On the left, there's a summary for 'Windows Security Events' with 74 installed content items and 22 configuration needed. Below this is a detailed view of the 'Windows Security Events via AMA' connector, which is disconnected. It shows the content source as 'Windows Security Events', provider as 'Microsoft Support', and version as '3.0.9'. A note says: 'The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security Events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.' Below this are sections for 'Analytics rules' (20 listed), 'Workbooks' (0), and 'Queries' (1). On the right, a large list of 74 analytics rules is displayed, each with columns for 'Content name', 'Created content', 'Content type', 'Version', and 'Status'. A chart on the right shows 'Data received' over time from April 11 to April 17, with a value of 0. A button 'Open connector page' is at the bottom.

- 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.

The screenshot shows the 'Create Data Collection Rule' wizard. Step 1, 'Prerequisites', asks to integrate with Windows Security Events via AMA, noting it requires Azure Arc and specific permissions. Step 2, 'Configuration', shows a table for enabling data collection rules. A 'Basic' tab is selected, showing a 'Rule name' field with 'DCR-WINDOWS', a 'Subscription' dropdown set to 'Azure subscription 1', and a 'Resource group' dropdown set to 'SOC-Lab'. A 'Next: Resources >' button is at the bottom.

- Click on the arrows to expand the scope and select the network.

[Home](#) > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub > Windows Security Events > Windows Security Events via AMA

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

- ✓ **Workspace data sources:** read and write permissions.
- To collect data from non-Azure VMs, they must have Azure Arc installed and enabled.

Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Refresh

Rule name Created by Filter name

No results

+Create data collection rule

Create Data Collection Rule

Data collection rule management

Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other applications.

Learn more

Subscriptions	Resource Groups	Resource Types	Locations
Selected: All	Selected: All	Selected: All	Selected: All
Search to filter items... Show Selected			
Scope	Resource Type	Location	
Azure subscription 1	SOC-Lab	CORPORATE-NET microsoft.compute/virtualmachines UK South	

< Previous Next: Collect >

7) Proceed through review and create and then create.

[Home](#) > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub > Windows Security Events > Windows Security Events via AMA

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

- ✓ **Workspace data sources:** read and write permissions.
- To collect data from non-Azure VMs, they must have Azure Arc installed and enabled.

Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Refresh

Rule name Created by Filter name

No results

+Create data collection rule

Create Data Collection Rule

Data collection rule management

Basic Resources Collect Review + create

Select which events to stream:

All Security Events Common Minimal Custom

< Previous Next: Review + create >

[Home](#) > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub > Windows Security Events > Windows Security Events via AMA

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

- ✓ **Workspace data sources:** read and write permissions.
- To collect data from non-Azure VMs, they must have Azure Arc installed and enabled.

Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Refresh

Rule name Created by Filter name

No results

+Create data collection rule

Create Data Collection Rule

Data collection rule management

Validation passed

Basic Resources Collect Review + create

Basic

Data rule name: DCR-WINDOWS

Subscription: Azure subscription 1

Resource Group: SOC-Lab

Selected resources

Name	Type
corporate-net	microsoft.compute/virtualmachines

Selected events: AllEvents

< Previous 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.

Name	Type	Version	Latest Version	Status	Automatic upgrade status
AzureMonitorWindowsAgent	Microsoft.Azure.Monitor	1.34.0.0	1.34.0.0	Provisioning succeeded	Disabled

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.

The screenshot shows the Log Analytics workspace interface for the 'LAW-SOC-LAB-00' workspace. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Logs. The main area displays a table of log entries with the following columns: TimeGenerated (UTC), Account, AccountType, Computer, EventSourceName, Channel, Task, Level, EventData, EventID, and Activity. The table shows numerous log entries from April 18, 2025, with EventID 4625 and Activity '4625 - An account failed to log...' repeated multiple times.

- 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.

This screenshot shows the same Log Analytics workspace interface, but with a modified query in the 'New Query' pane. The query now includes a WHERE clause to filter for the '\Administrator' account and a PROJECT clause to specify the columns returned. The resulting table shows a subset of the previous data, specifically focusing on failed login attempts for the '\Administrator' account.

- 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.

The screenshot shows the Microsoft Log Analytics workspace interface. On the left, there is a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Resource visualizer, Settings, Classic, Monitoring, Automation, and Help. The main area is titled "LAW-SOC-LAB-00 | Logs". A search bar at the top has the placeholder "Search". Below it is a "New Query" button and a dropdown menu for "Time range: Set in query". The results table shows 1000 results with columns: TimeGenerated (UTC), Account, Computer, EventID, Activity, and IpAddress. The first few rows of the table are as follows:

TimeGenerated (UTC)	Account	Computer	EventID	Activity	IpAddress
> 4/18/2025, 6:15:59.386 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:59.278 AM	\ofice1	CORPORATE-NET	4625	4625 - An account failed to log...	80.94.95.90
> 4/18/2025, 6:15:58.907 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:58.512 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:58.037 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:57.640 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:57.186 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:56.799 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:56.494 AM	\remote	CORPORATE-NET	4625	4625 - An account failed to log...	80.94.95.90
> 4/18/2025, 6:15:56.264 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:55.841 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:55.416 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:54.952 AM	\for	CORPORATE-NET	4625	4625 - An account failed to log...	115.245.191.82
> 4/18/2025, 6:15:54.135 AM	\freak	CORPORATE-NET	4625	4625 - An account failed to log...	80.94.95.90

At the bottom of the page, there are pagination controls ("Page 1 of 1") and a note: "Add or remove favorites by pressing Cmd+Shift+F".

- 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:

The screenshot shows the IPInfo website interface. At the top, there is a navigation bar with links for Products, Solutions, Why IPInfo, Pricing, Resources, Docs, Login, and Sign up. Below the navigation is a search bar with placeholder "e.g. 8.8.8.8 or AS13335" and a "Search" button. The main content area is titled "115.245.191.0/24 IP Range". It includes a map of India with a blue polygon highlighting the IP range. To the right of the map is a summary table with the following data:

Summary	
ASN	A555836 Reliance Jio Infocomm Limited
BGP	115.245.188.0/22
IPs with RDNS	0
Hosted Domains	0
Pingable IPs	29
Router IPs	25

Below the summary is a table showing the five pingable IP addresses in the range:

IP ADDRESS	HOSTNAME	DOMAINS	PINGABLE	ROUTER
115.245.191.0	—	0	☒	☒
115.245.191.1	—	0	☒	☒
115.245.191.2	—	0	☒	☒
115.245.191.3	—	0	☒	☒
115.245.191.4	—	0	☒	☒

- 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	—	0	☒	☒
115.245.191.75	—	0	☒	☒
115.245.191.76	—	0	☒	☒
115.245.191.77	—	0	✓	☒
115.245.191.78	—	0	☒	☒
115.245.191.79	—	0	☒	☒
115.245.191.80	—	0	☒	☒
115.245.191.81	—	0	☒	☒
115.245.191.82	—	0	☒	✓
115.245.191.83	—	0	☒	☒
115.245.191.84	—	0	☒	☒
115.245.191.85	—	0	✓	☒
115.245.191.86	—	0	☒	☒
115.245.191.87	—	0	☒	☒
115.245.191.88	—	0	☒	☒
115.245.191.89	—	0	✓	☒
115.245.191.90	—	0	☒	☒
115.245.191.91	—	0	☒	☒
115.245.191.92	—	a	☒	☒

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

ASN	AS55836 - Reliance Jio Infocomm Limited
Hostname	No Hostname
Range	115.245.198.0/22
Company	Reliance Jio Infocomm Limited
Hosted domains	0
Privacy	☒ False
Anycast	☒ False
ASN type	ISP
Abuse contact	ip.abuse@rjl.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.

The screenshot shows the Microsoft Sentinel interface with the 'Watchlist' section selected. The left sidebar includes options like General, Threat management, Content hub, Repositories (Preview), Community, Configuration (Workspace manager, Data connectors, Analytics, Summary rules (Preview), Watchlist, Automation, Settings), and a search bar. The main content area displays 'My Watchlists' and 'Templates (Preview)'. A 'Watchlist' card is highlighted, containing sections for 'What is it?' (explaining Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment), 'How does it work?' (describing the creation process and storage), and 'This is what you can do with watchlists' (listing investigate threats, import business data, and join watchlists). A message at the bottom right says 'No watchlist selected. Select a watchlist for more details.'

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

The screenshot shows the 'Watchlist wizard' in the 'General' step. It has tabs for General, Source, Review + create. Under 'General', there are fields for 'Name' (set to 'geopl'), 'Description' (empty), and 'Alias' (set to 'geopl'). Below the fields are 'Next: Source >' and 'Give feedback' buttons.

- 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.

Home > Microsoft Sentinel | Watchlist >

Watchlist wizard .. X

General Source Review + create

Source type * Local file

File type * CSV file with a header (csv)

Number of lines before row with headings * 0

Upload file * geoip-summarized.csv

Drag and drop the files or [Browse for files](#)

SearchKey *

Reset

File preview | First 50 rows and first 5 columns

	network	latitude	longitude	cityname	countryname
1.0.0/16	-33.494	143.2104		Australia	
1.1.0/16	17.8148	103.3386	Ban Chan	Thailand	
1.2.0/16	13.8667	100.1917	Nakhon Pathom	Thailand	
1.3.0/16	13.8679	100.1891	Nakhon Pathom	Thailand	
1.4.0/16	13.6687	100.579	Bangkok	Thailand	
1.5.0/16	13.6659	100.5882	Bangkok	Thailand	
1.6.0/16	12.9634	77.5855	Bengaluru	India	
1.7.0/16	12.9691	77.5902	Bengaluru	India	
1.8.0/16	12.9557	77.5843	Bengaluru	India	
1.9.0/16	3.1539	101.7448	Ampang	Malaysia	

[« Previous](#) [Next : Review + create »](#) [Give feedback](#)

4) Click create.

Home > Microsoft Sentinel | Watchlist >

Watchlist wizard .. X

General Source **Review + create**

Name * geoip

Description

Alias * geoip

Source type * Local

File type * Text/Csv

Number of lines before row with headings * 0

SearchKey *

Text/Csv

[« Previous](#) [Create](#) [Give feedback](#)

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

The screenshot shows the Microsoft Sentinel interface. On the left, a navigation sidebar includes 'Create', 'Manage view', 'Content hub', 'Repositories (Preview)', 'Community', 'Configuration' (with 'Workspace manager (Preview)', 'Data connectors', 'Analytics', 'Summary rules (Preview)'), 'Watchlist' (selected), 'Automation', and 'Settings'. The main area is titled 'Microsoft Sentinel | Watchlist' with the sub-section 'Selected workspace: LAW-SOC-LAB-00'. It displays a 'My Watchlists' section with a table for 'geoip' and a 'Watchlist Items' section. The 'geoip' table has columns: Name, Alias, Source, Create..., Last u..., and Status (Preview). The status shows 'Uploading (25.55%)'. A right-hand panel shows details for the 'geoip' provider, including 'Source: geoip-summarized.csv', 'Created by: deposview@outlook.com', 'Last updated: 4/18/2025, 7:36:47 AM', and 'SearchKey network'. At the bottom, there are 'View in logs' and 'Update watchlist' buttons.

- 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.

The screenshot shows the Log Analytics workspace for 'LAW-SOC-LAB-00'. The left sidebar includes 'Logs' (selected), 'Resource visualizer', 'Settings', 'Classic', 'Monitoring', 'Automation', and 'Help'. The main area shows a 'New Query 1*' editor with the query `_GetWatchlist("geoip")`. The results table has columns: LastUpdatedTimeUTC (UTC), _DTItemid, SearchKey, cityname, countryname, and latitude. The table lists numerous entries from April 18, 2025, such as Grottoes, United States (38.2543), Santee, United States (32.8466), Phoenix, United States (33.4512), Mesa, United States (33.3825), New York, United States (40.7263), Kareehe, United States (21.4254), Toledo, United States (41.703), and Karolyn, United States (21.8414).

- Use the query in the image below to copy an ipAddress .

The screenshot shows the Log Analytics workspace for 'LAW-SOC-LAB-00'. On the left, the navigation pane includes 'Logs' under 'Diagnose and solve problems'. The main area displays a query results table with columns: TimeGenerated (UTC), Account, AccountType, Computer, EventSourceName, Channel, and Task. The results show multiple entries for 'EventID 4625' from 'Vminal' user on 'CORPORATE-NET' computer, with various account types like User, VADMIN, and ADMINISTRATOR.

- 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.

The screenshot shows the Log Analytics workspace for 'LAW-SOC-LAB-00'. The query in the editor is as follows:

```

1 let GeopIP_Full = _GetWatchlist("geip");
2 WindowsEvents | SecurityEvent
3 | whereIpAddress == "201.187.98.150"
4 | project Computer, AttackerIP, cityname, countryname, latitude, longitude
5 | order by TimeGenerated desc
6 | evaluate ipda_lookup(GeoIP_Full, ipAddress, network);
7 WindowsEvents
8 | project TimeGenerated, Computer, AttackerIP = ipAddress, cityname, countryname, latitude, longitude
  
```

The results table shows security events from 'CORPORATE-NET' computer, with the 'AttackerIP' column renamed to 'ipAddress'.

- 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.

Home > Microsoft Sentinel | Workbooks >

New workbook

law-soc-lab-00

Done Editing Open File Save Undo Redo Print Help

 This Microsoft Sentinel Report has no content.

↓ Use the add button below to add items.

+ Add ▾

- Add text
- Add image
- Add video
- Add parameters
- Add links/tabs
- Add query
- Add query
- Add group

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

Home > Microsoft Sentinel | Workbooks >

New workbook

law-soc-lab-00

Done Editing Open Style Advanced Settings Advanced Editor

Editing query item: query - 0

Show below is a JSON representation of the current item.
Any changes you make here will be reflected when you press 'Done Editing'.

```
1 {  
2     "type": 3,  
3     "version": 1,  
4     "version": "2017-07-08T00:00:00Z",  
5     "query": "let GeoIPOR_FULL = _GetMatchlist('geolookup');\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n| order By TimeGenerated desc\n| evaluate ipv4_lookup(GeoIPOR_FULL,IpAddress, network)\n| summarize FailureCount  
6     "size": 3,  
7     "timeContext": {  
8         "durationIn": 2592000000  
9     },  
10    "queryType": 0,  
11    "resourceType": "microsoft.operationalinsights工作空间",  
12    "visualization": "map",  
13    "map": {  
14        "locInfo": "LatLang",  
15        "locInfoColumn": "countryname",  
16        "latitude": "latitude",  
17        "longitude": "longitude",  
18        "sizeSetting": "FailureCount",  
19        "sizeAggregation": "Sum",  
20        "sizeCapacity": 0.05  
21    }  
22}
```

Done Editing Cancel Add Move Clone Remove

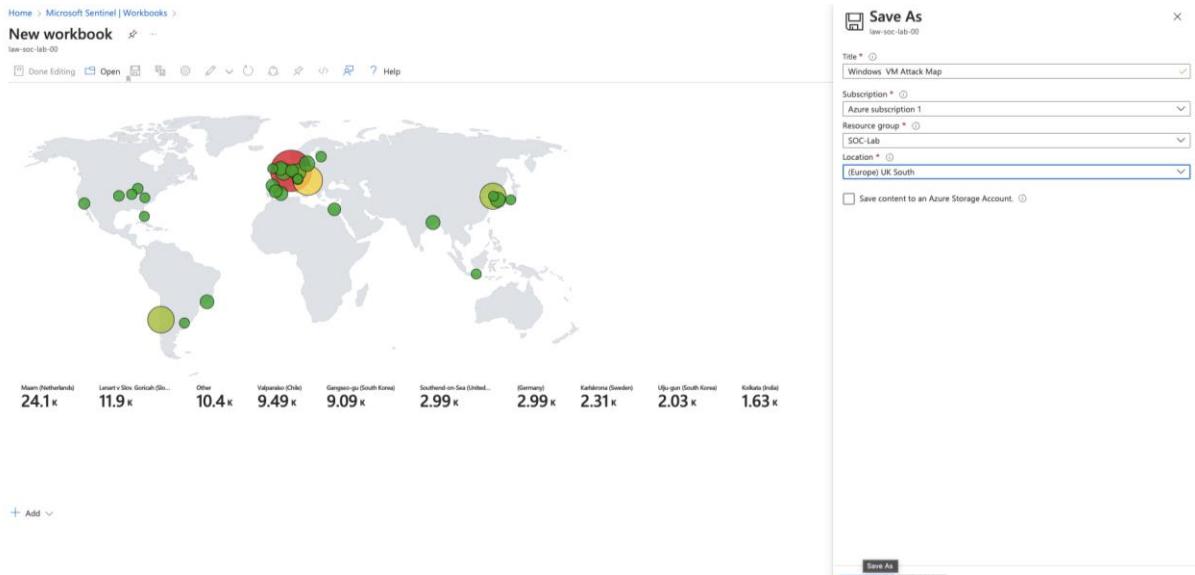
+ Add ▾

```
15 "locInfoColumn": "countryname",
16 "latitude": "latitude",
17 "longitude": "longitude",
18 "sizeSettings": "FailureCount",
19 "sizeAggregation": "Sum",
20 "opacity": 0.8,
21 "labelSettings": "friendly_location",
22 "legendMetric": "FailureCount",
23 "legendAggregation": "Sum",
24 "itemColorSettings": {
25   "nodeColorField": "FailureCount",
26   "colorAggregation": "Sum",
27   "type": "heatmap",
28   "heatmapPalette": "greenRed"
29 }
30 },
31 "name": "query - 0"
32 }
33 }
```

✓ Done Editing

+ Add ▾

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.