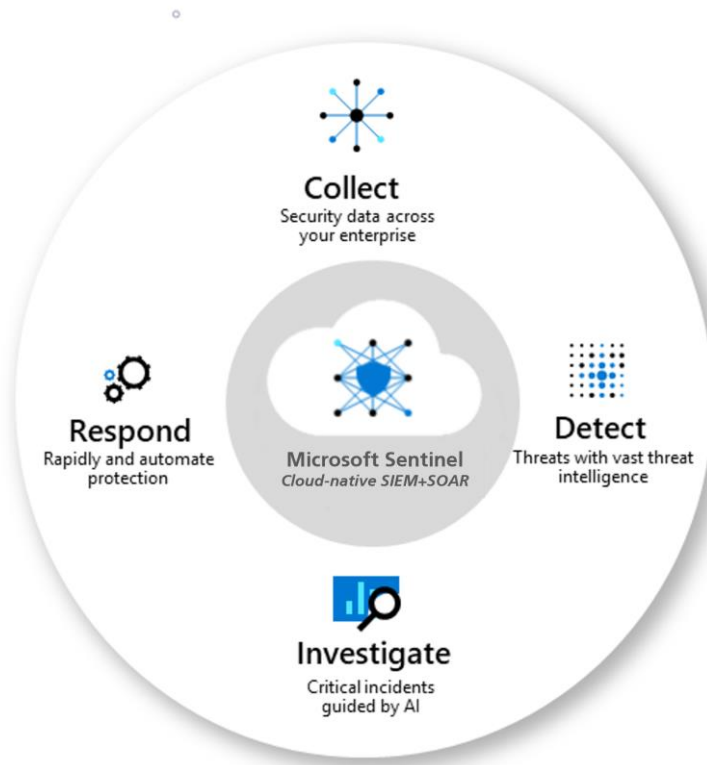


# Microsoft Sentinel SIEM Lab

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.

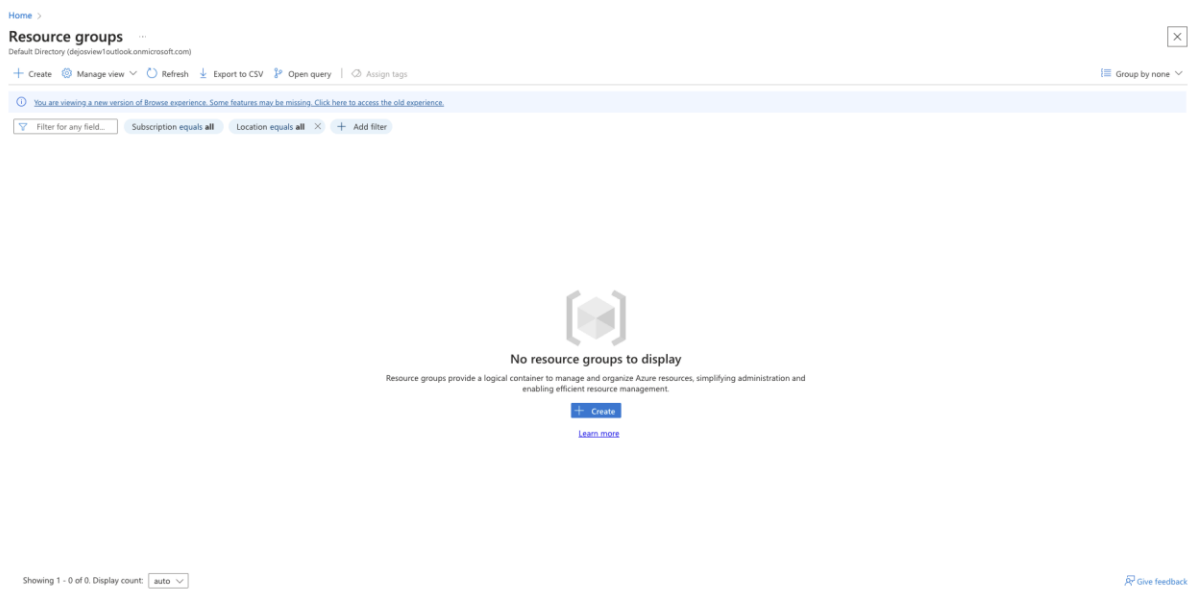
## Key components:

- 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

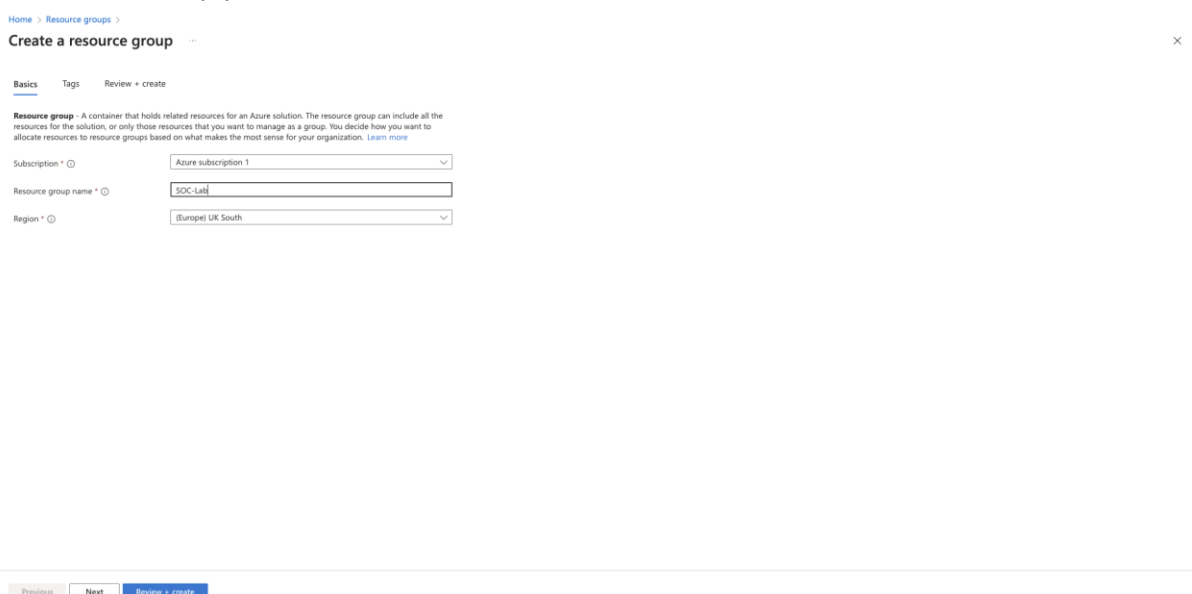
## Create the Honey Pot (Azure Virtual Machine)

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.

The screenshot shows the Azure portal interface for the 'SOC-Lab' resource group. The left sidebar contains navigation links for 'Resource groups', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings', 'Cost Management', 'Monitoring', 'Automation', and 'Help'. The main content area shows the 'Overview' tab for the 'SOC-Lab' resource group. It displays the subscription ID 'edce9016-6f65-4626-9991-854d8cf9b086' and the location 'UK South'. A message states 'No resources match your filters' with buttons to 'Create resources' and 'Clear filters'. A notification on the right confirms the resource group creation.

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

The screenshot shows the Azure portal interface for the 'Virtual networks' service. The left sidebar contains navigation links for 'Virtual networks', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings', 'Cost Management', 'Monitoring', 'Automation', and 'Help'. The main content area shows the 'Overview' tab for the 'Virtual networks' service. It displays the subscription ID 'edce9016-6f65-4626-9991-854d8cf9b086' and the location 'UK South'. A message states 'No virtual networks to display' with a button to 'Create virtual network'. A notification on the right confirms the resource group creation.

- 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

Basics 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 \*

Resource group \*   
[Create new](#)

### Instance details

Virtual network name \*

Region \*   
[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 Inputs Outputs Template

**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 : 74733e88-6d64-4252-450e-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 >](#)

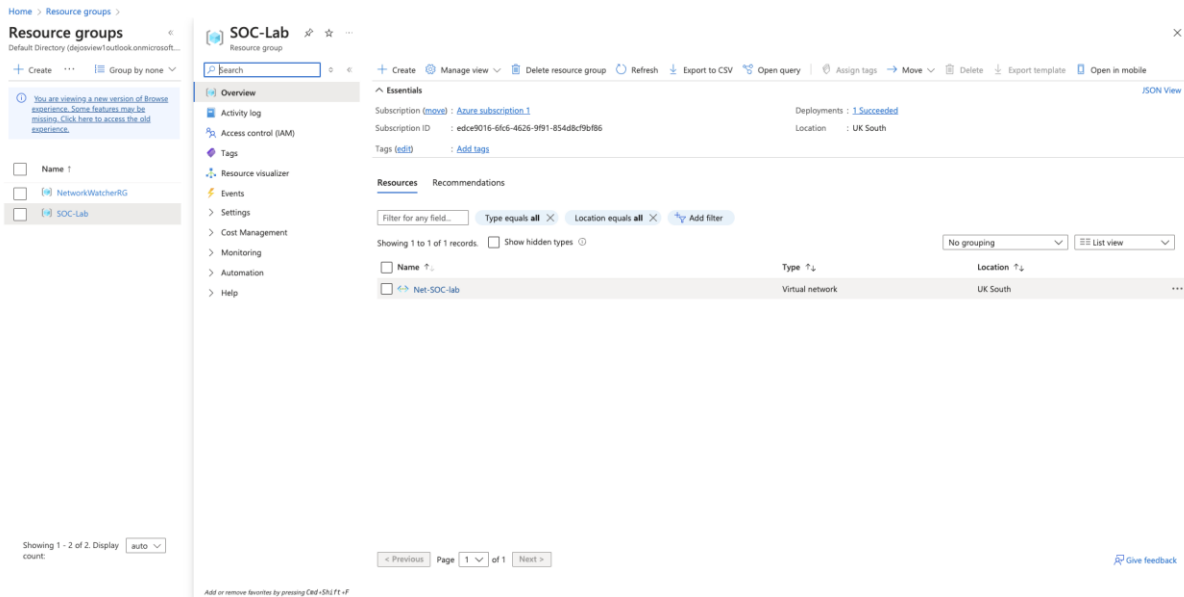
**Microsoft Defender for Cloud**  
Secure your apps and infrastructure  
[Go to Microsoft Defender for Cloud >](#)

**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 >](#)

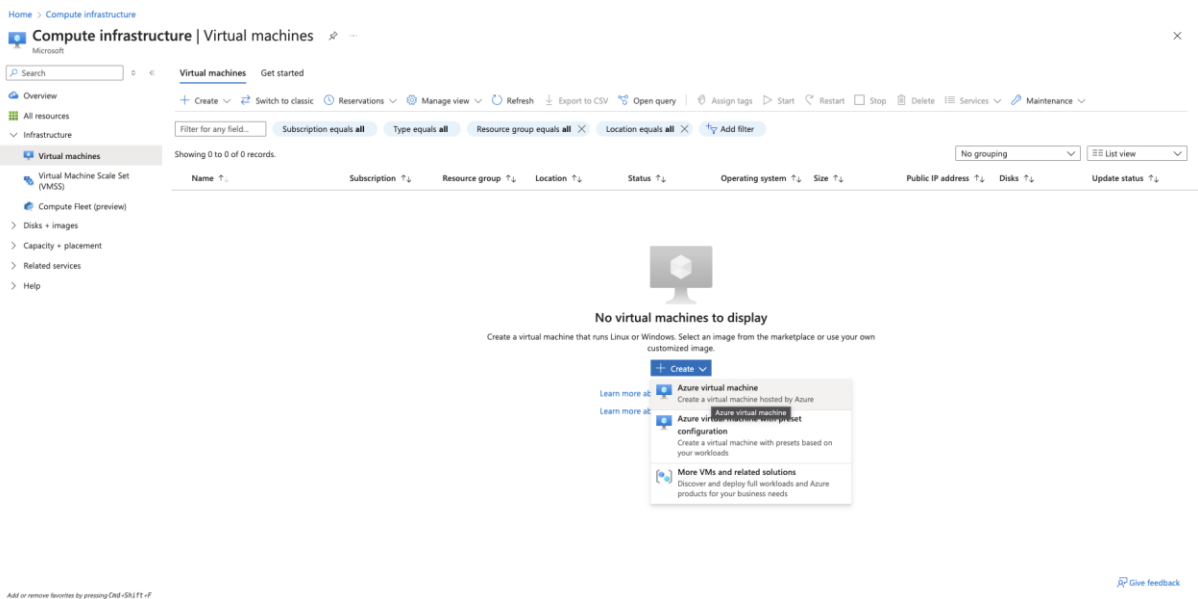
Add or remove favorites by pressing Cmd+Shift+F

- 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.

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

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 machine name \* CORPORATE-NET

Region \* (Europe) UK South

Availability options \* Availability zone

Zone options \*  
☒ Self-selected zone  
Choose up to 3 availability zones, one VM per zone  
☐ Azure-selected zone (Preview)  
Let Azure assign the best zone for your needs

Availability zone \* Zone 1  
☒ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type \* Trusted launch virtual machines  
[Configure security features](#)  
☒ Trusted launch virtual machine is required when using IP Gallery images.

Image \* Windows 10 Pro, version 22H2 - x64 Gen2 (three services eligible)  
[See all images](#) [Configure VM generation](#)

VM architecture \*  
☐ Arm64  
☒ x64  
☐ Arm64 is not supported with the selected image.

Run with Azure Spot discount ☐

< Previous Next : Disks > Review + create

[Give feedback](#)

- 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.

Home > Compute infrastructure | Virtual machines >

### Create a virtual machine

Changing Basic options may reset selections you have made. Review all options prior to creating the 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

Size \* Standard\_D4s\_v3 - 4 vcpus, 16 GiB memory (\$169.36/month)  
[See all sizes](#)

Enable Hibernation ☐  
☒ Hibernation is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more](#)

**Administrator account**

Username \* Cybersecurity

Password \*

Confirm password \*

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

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.

**Licensing**

☒ I confirm I have an eligible Windows 10/11 license with multi-tenant hosting rights. [Review multi-tenant hosting rights for Windows 10/11 compliance](#)

< Previous Next : Disks > Review + create

[Give feedback](#)

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:

OS disk type:

Delete with VM: ☒

Key management:

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
-----	------	------------	-----------	--------------	----------------

[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:   
[Create new](#)

Subnet:   
[Manage subnet configuration](#)

Public IP:   
[Create new](#)

NIC network security group: ☐ None ☒ Basic ☐ Advanced

Public inbound ports: ☐ None ☒ Allow selected ports

Select inbound ports:

**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 ☐ Annsilation mawaww

[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.

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

Configure management options for your VM.

**Microsoft Defender for Cloud**  
Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

Enable basic plan for free ☒ This will apply to every VM in the selected subscription

**Identity**  
Enable system assigned managed identity ☐

**Microsoft Entra ID**  
Login with Microsoft Entra ID ☐  
RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Microsoft Entra ID login. [Learn more](#)

**Auto-shutdown**  
Enable auto-shutdown ☐

**Backup**  
Enable backup ☐

**Site Recovery**  
Enable Disaster Recovery ☐

**Guest OS updates**  
Enable periodic assessment ☐

< Previous | Next: Monitoring > | **Review + create**

[Give feedback](#)

14) I chose to disable boot diagnostics.

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

Configure monitoring options for your VM.

**Alerts**  
Enable recommended alert rules ☐

**Diagnostics**  
Boot diagnostics ☐ Enable with managed storage account (recommended)  
☐ Enable with custom storage account  
☒ Disable

Enable OS guest diagnostics ☐

**Health**  
Enable application health monitoring ☐

< Previous | Next: Advanced > | **Review + create**

[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:





Home > Resource groups > SOC-Lab > CORPORATE-NET-nsg

Network security group

Search

Move Delete Refresh Give feedback

**Overview**

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Monitoring

Automation

Help

**Delete security rule**

Do you want to delete the security rule 'RDP'?

Yes No

Subscription ID : edce9016-6ffc-4626-99f1-854d8c79b9b6

Tags (edit) : Add tags

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

**Inbound Security Rules**

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

**Outbound Security Rules**

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
65500	DenyAllOutbound	Any	Any	Any	Any	Deny

Custom security rules : 1 inbound, 0 outbound

Associated with : 0 subnets, 1 network interfaces

JSON View

Add or remove favorites by pressing Ctrl+Shift+F

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.

Home > Resource groups > SOC-Lab > CORPORATE-NET-nsg

Network security group

Search

Move Delete Refresh Give feedback

**Overview**

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

**Inbound security rules**

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Help

**Add inbound security rule**

CORPORATE-NET-nsg

Source

Any

Source port ranges \*

\*

Destination

Any

Service

Custom

Destination port ranges \*

\*

Protocol

Any

TCP

UDP

ICMPv4

Action

Allow

Deny

Priority \*

100

Name \*

DANGER\_AllowAnyCustomAnyInbound

Description

Add Cancel Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule with a higher priority is evaluated first. You can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source
65000	AllowVnetInbound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer
65500	DenyAllInbound	Any	Any	Any

**Add inbound security rule**

CORPORATE-NET-nsg

Source

Any

Source port ranges \*

\*

Destination

Any

Service

Custom

Destination port ranges \*

\*

Protocol

Any

TCP

UDP

ICMPv4

Action

Allow

Deny

Priority \*

100

Name \*

DANGER\_AllowAnyCustomAnyInbound

Description

Add Cancel Give feedback

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

Oracle DB port 1521 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

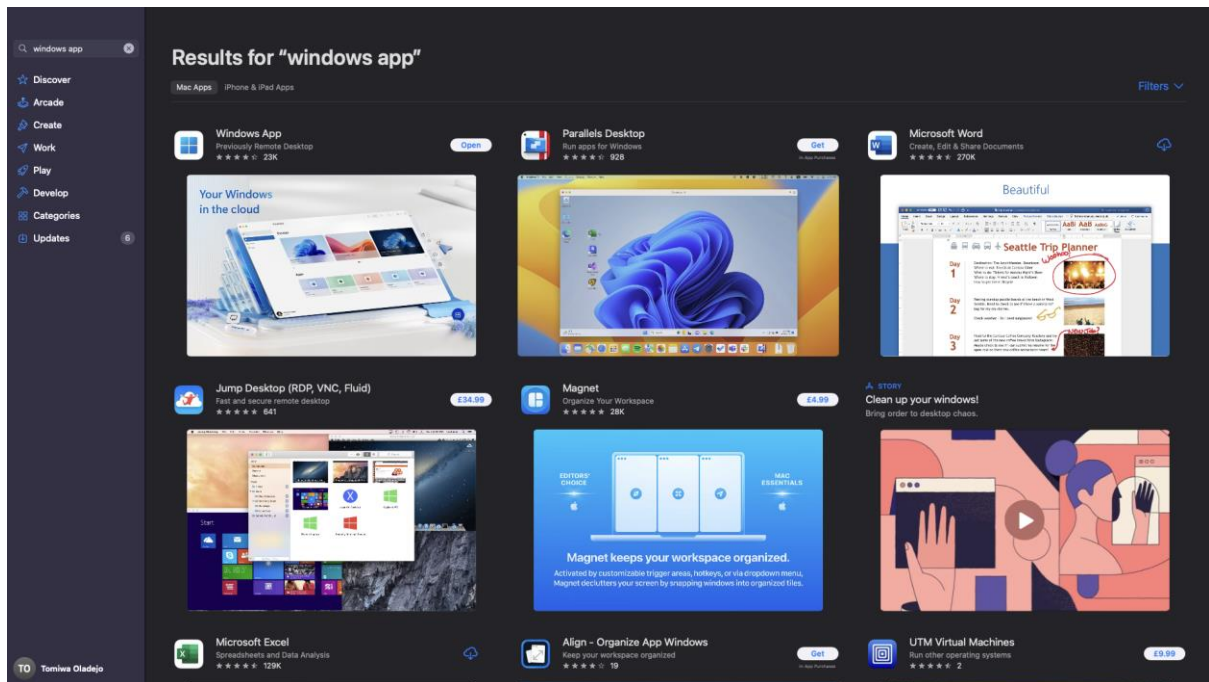
MySQL DB port 3306 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

Postgres DB port 5432 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

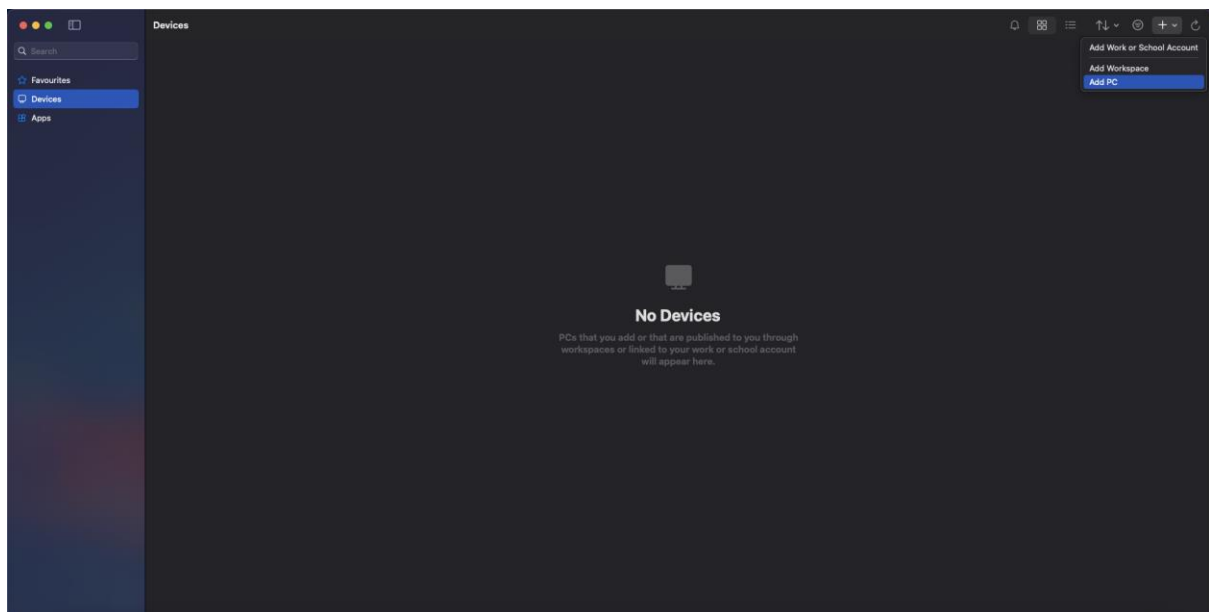
Add Cancel Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

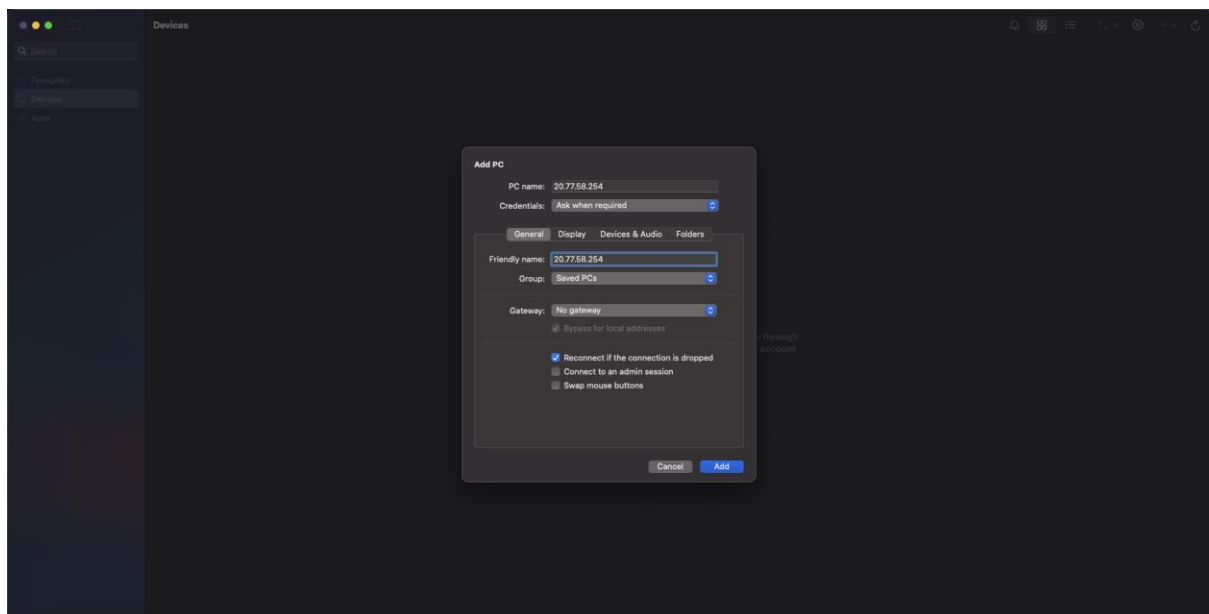
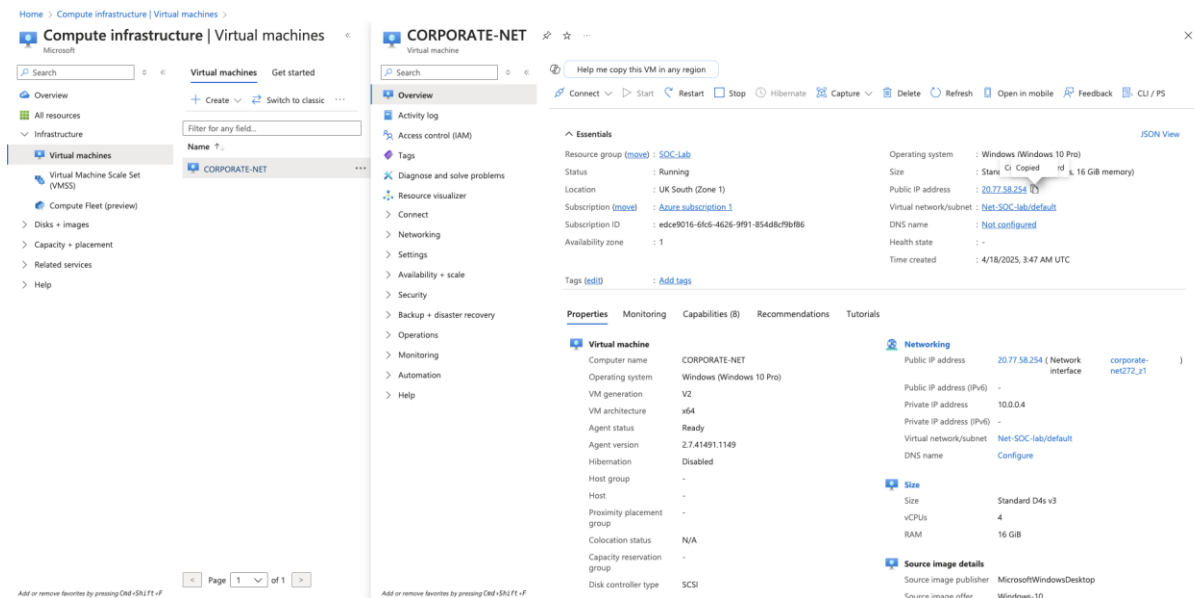
- 19) After configuring the security rule, we now want to disable the firewalls within the virtual machine. As I carried out this lab on Mac, I downloaded “Windows App” to access the virtual machine. However, if you are using windows you should be able to find a remote desktop through a quick search.



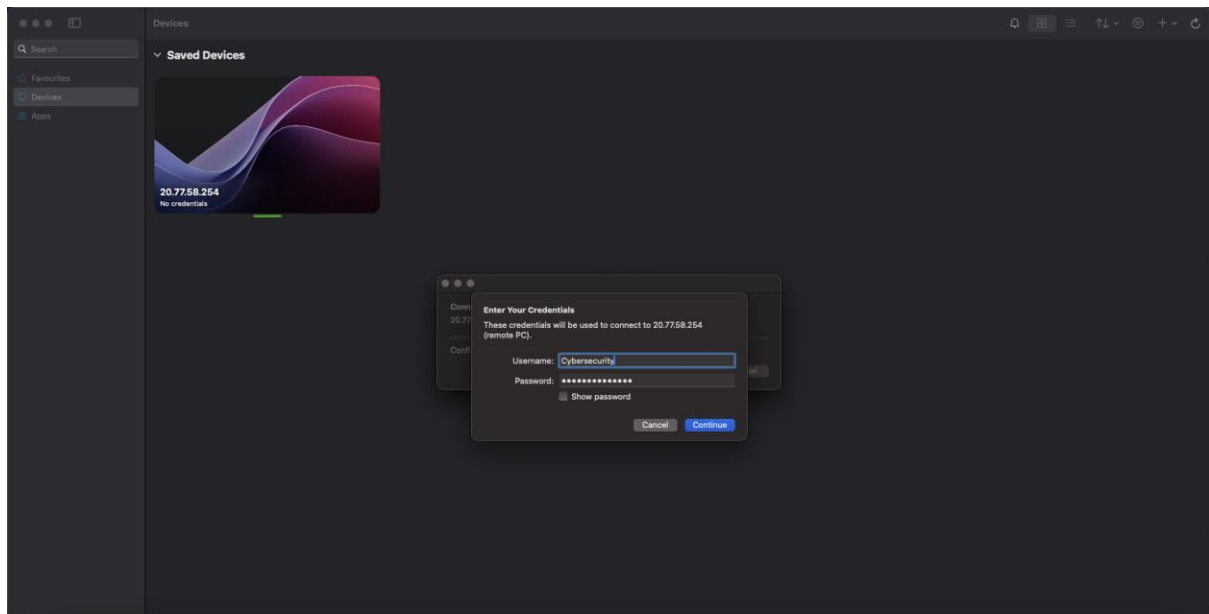
- 20) Open the windows app after it has installed and select add PC.



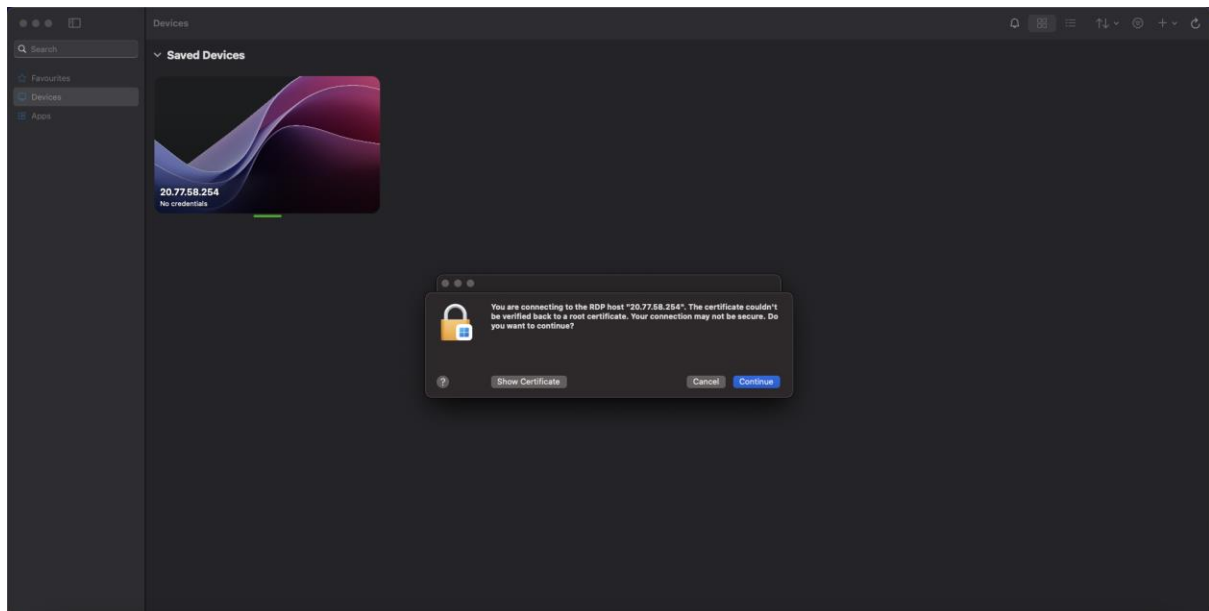
21) You will be prompted to enter the public IP address for the virtual machine. This can be found in the overview section of the virtual machine that you created. Once located, copy and paste the public IP address into the “PC name” section. Make sure the credentials are set to ask when required, and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



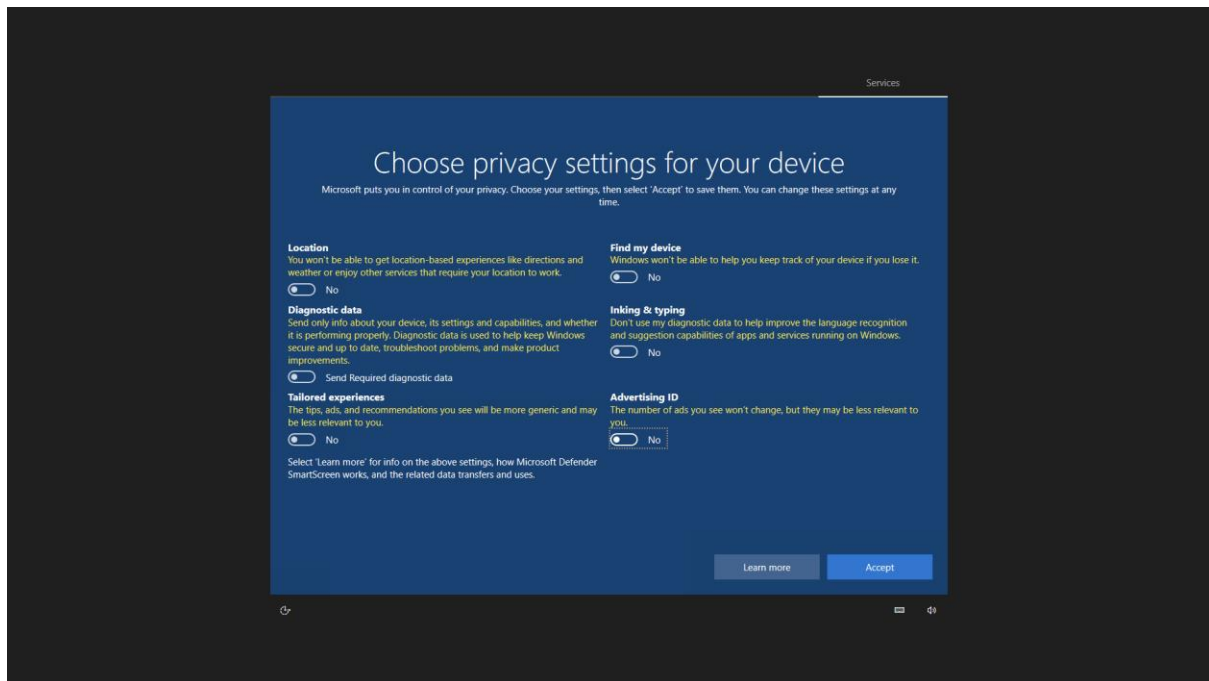
22) Enter the username and password that has been set for the virtual machine.



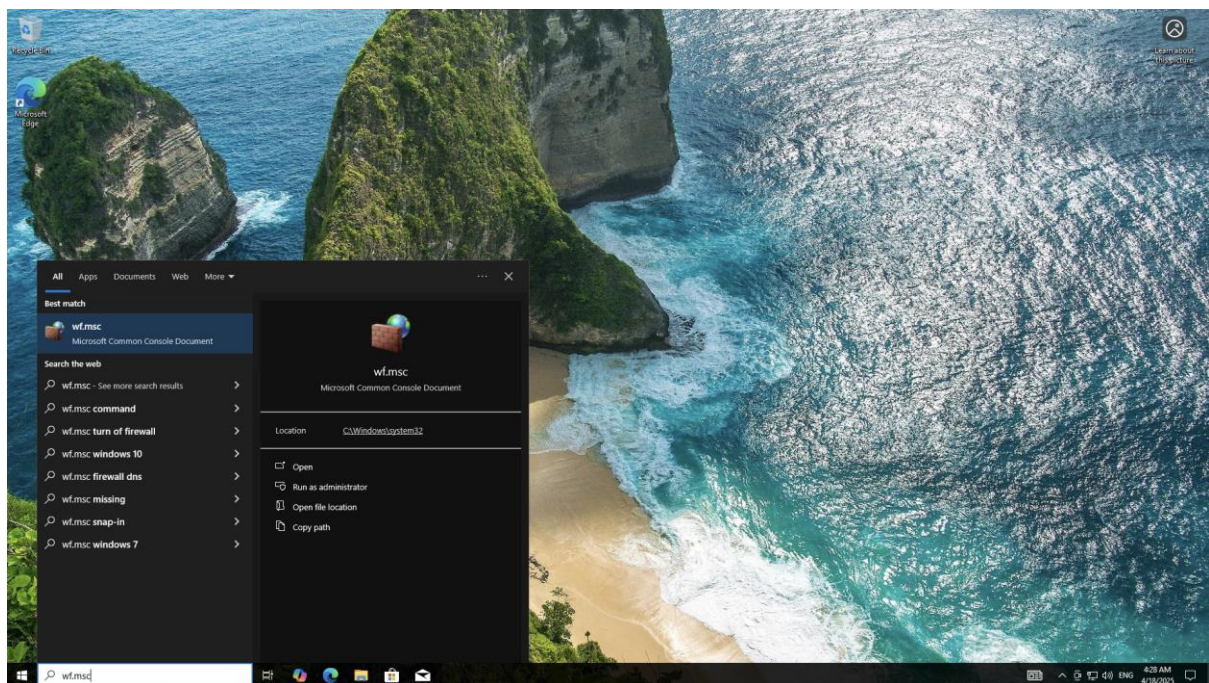
23) Click continue.



24) Select no for all options.

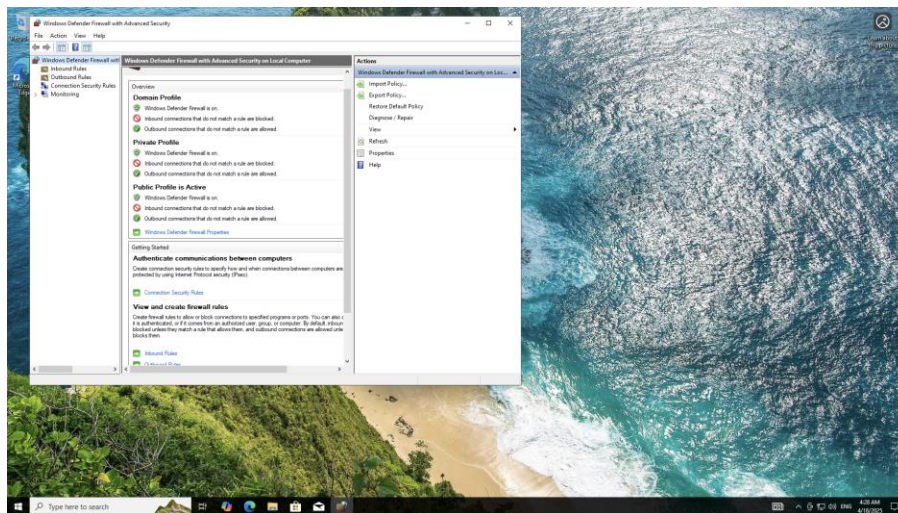


25) Now that we are logged into the virtual machine, the next step is to disable the firewall. So type wf.msc in the search bar below.

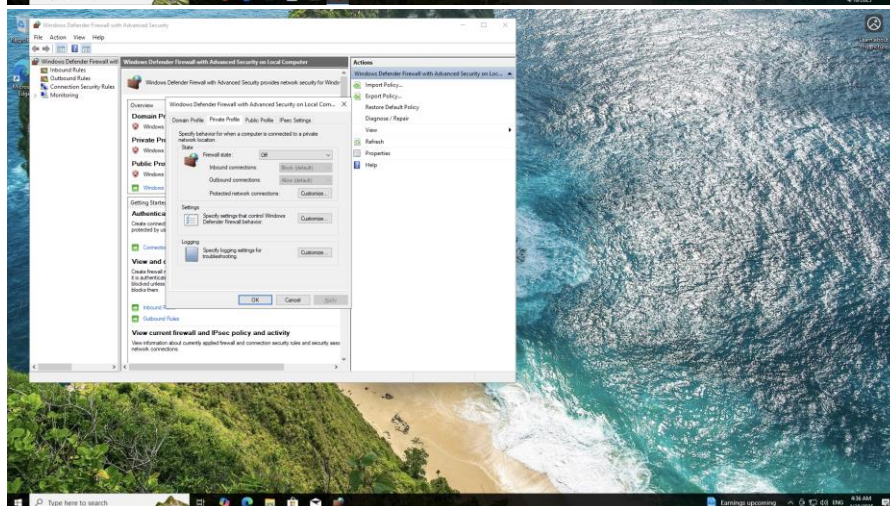
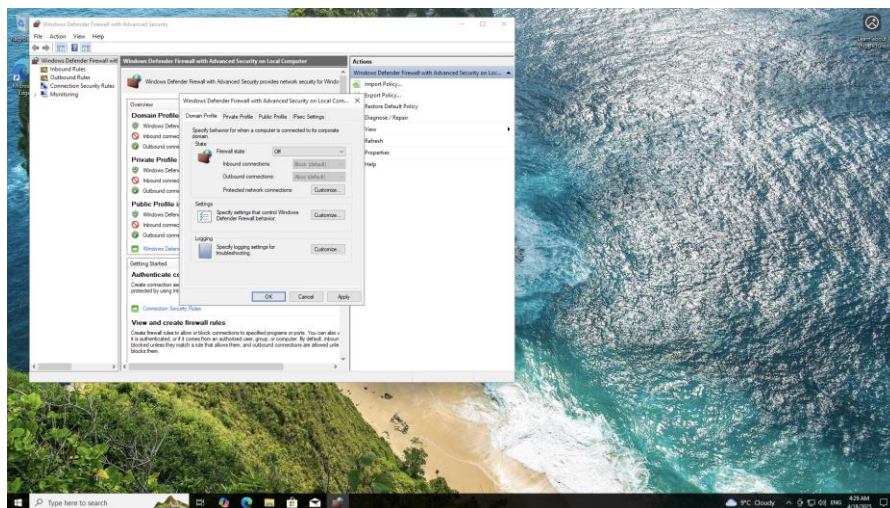


26) “Windows Defender Firewall with Advanced Security” should open.





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





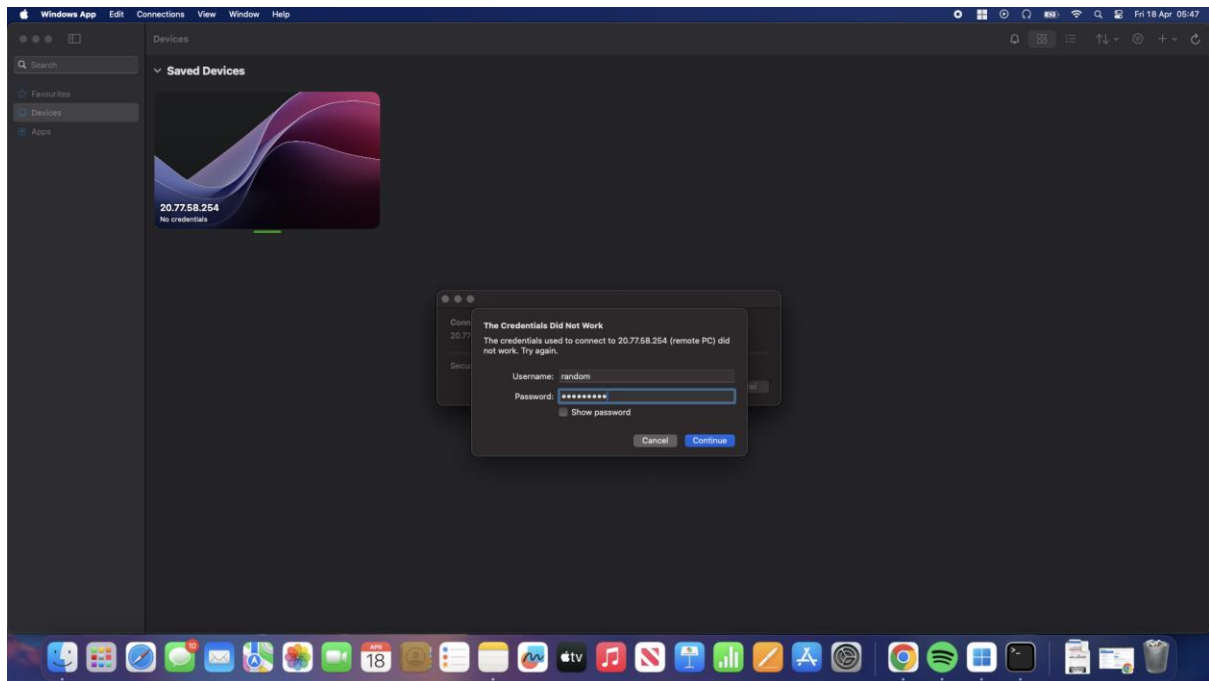


When the pinging has shown to be successful, it can be stopped with ctrl + c. In the scenario the ping has not been successful, the firewall may not be off.

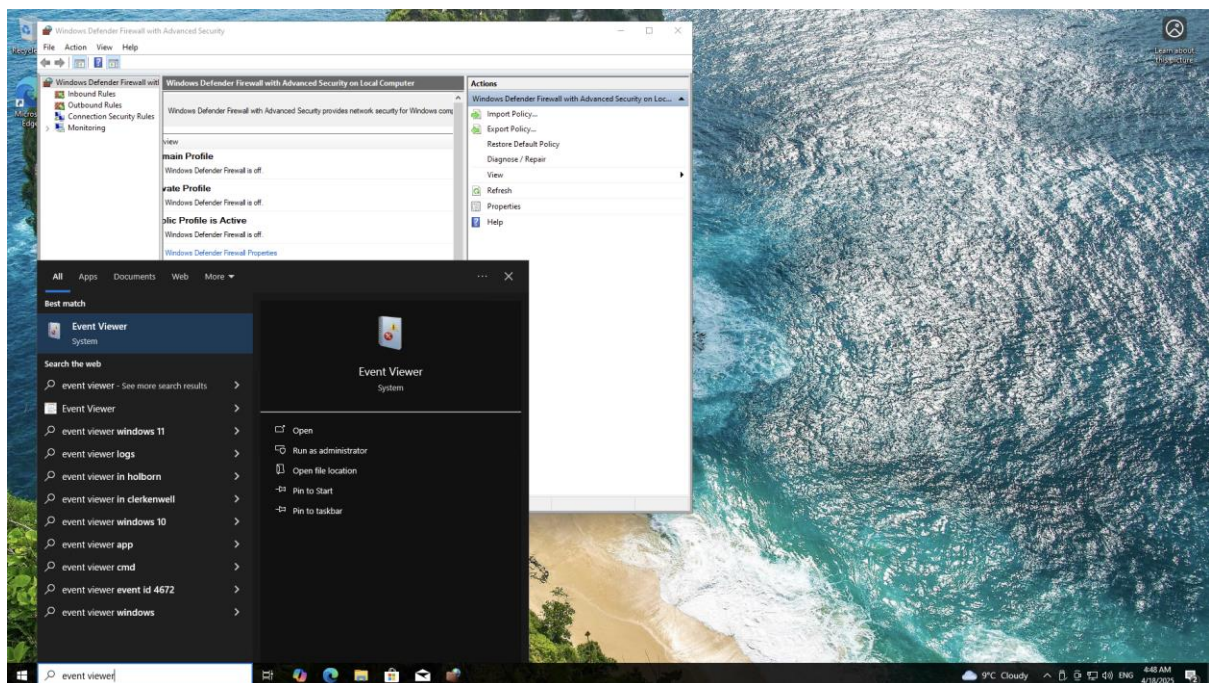
```
last login: Wed Mar 23 11:15:57 on console
comp@linux-machine-1:~$ % ping 10.10.10.200

64 bytes from 20.77.58.204: icmp_seq=169 ttl=115 time=11.687 ms
64 bytes from 20.77.58.204: icmp_seq=170 ttl=115 time=12.180 ms
64 bytes from 20.77.58.204: icmp_seq=171 ttl=115 time=11.225 ms
64 bytes from 20.77.58.204: icmp_seq=172 ttl=115 time=12.735 ms
64 bytes from 20.77.58.204: icmp_seq=173 ttl=115 time=11.485 ms
64 bytes from 20.77.58.204: icmp_seq=174 ttl=115 time=11.446 ms
64 bytes from 20.77.58.204: icmp_seq=175 ttl=115 time=11.868 ms
64 bytes from 20.77.58.204: icmp_seq=176 ttl=115 time=19.651 ms
64 bytes from 20.77.58.204: icmp_seq=177 ttl=115 time=12.433 ms
64 bytes from 20.77.58.204: icmp_seq=178 ttl=115 time=12.966 ms
64 bytes from 20.77.58.204: icmp_seq=179 ttl=115 time=11.968 ms
64 bytes from 20.77.58.204: icmp_seq=180 ttl=115 time=13.186 ms
64 bytes from 20.77.58.204: icmp_seq=181 ttl=115 time=18.386 ms
64 bytes from 20.77.58.204: icmp_seq=182 ttl=115 time=11.863 ms
64 bytes from 20.77.58.204: icmp_seq=183 ttl=115 time=14.579 ms
64 bytes from 20.77.58.204: icmp_seq=184 ttl=115 time=9.906 ms
64 bytes from 20.77.58.204: icmp_seq=185 ttl=115 time=9.877 ms
64 bytes from 20.77.58.204: icmp_seq=186 ttl=115 time=11.617 ms
64 bytes from 20.77.58.204: icmp_seq=187 ttl=115 time=19.826 ms
64 bytes from 20.77.58.204: icmp_seq=188 ttl=115 time=11.116 ms
64 bytes from 20.77.58.204: icmp_seq=189 ttl=115 time=13.483 ms
64 bytes from 20.77.58.204: icmp_seq=190 ttl=115 time=18.969 ms
64 bytes from 20.77.58.204: icmp_seq=191 ttl=115 time=19.884 ms
64 bytes from 20.77.58.204: icmp_seq=192 ttl=115 time=12.371 ms
64 bytes from 20.77.58.204: icmp_seq=193 ttl=115 time=13.129 ms
64 bytes from 20.77.58.204: icmp_seq=194 ttl=115 time=12.774 ms
64 bytes from 20.77.58.204: icmp_seq=195 ttl=115 time=18.466 ms
64 bytes from 20.77.58.204: icmp_seq=196 ttl=115 time=11.379 ms
64 bytes from 20.77.58.204: icmp_seq=197 ttl=115 time=11.613 ms
64 bytes from 20.77.58.204: icmp_seq=198 ttl=115 time=11.627 ms
64 bytes from 20.77.58.204: icmp_seq=199 ttl=115 time=12.491 ms
64 bytes from 20.77.58.204: icmp_seq=200 ttl=115 time=12.899 ms
64 bytes from 20.77.58.204: icmp_seq=201 ttl=115 time=11.130 ms
64 bytes from 20.77.58.204: icmp_seq=202 ttl=115 time=12.174 ms
64 bytes from 20.77.58.204: icmp_seq=203 ttl=115 time=13.986 ms
64 bytes from 20.77.58.204: icmp_seq=204 ttl=115 time=18.479 ms
64 bytes from 20.77.58.204: icmp_seq=205 ttl=115 time=11.197 ms
64 bytes from 20.77.58.204: icmp_seq=206 ttl=115 time=13.868 ms
64 bytes from 20.77.58.204: icmp_seq=207 ttl=115 time=14.935 ms
64 bytes from 20.77.58.204: icmp_seq=208 ttl=115 time=19.467 ms
64 bytes from 20.77.58.204: icmp_seq=209 ttl=115 time=12.861 ms
64 bytes from 20.77.58.204: icmp_seq=210 ttl=115 time=11.617 ms
64 bytes from 20.77.58.204: icmp_seq=211 ttl=115 time=17.418 ms
64 bytes from 20.77.58.204: icmp_seq=212 ttl=115 time=18.471 ms
64 bytes from 20.77.58.204: icmp_seq=213 ttl=115 time=13.108 ms
64 bytes from 20.77.58.204: icmp_seq=214 ttl=115 time=13.343 ms
64 bytes from 20.77.58.204: icmp_seq=215 ttl=115 time=12.426 ms
64 bytes from 20.77.58.204: icmp_seq=216 ttl=115 time=9.962 ms
64 bytes from 20.77.58.204: icmp_seq=217 ttl=115 time=11.614 ms
64 bytes from 20.77.58.204: icmp_seq=218 ttl=115 time=11.746 ms
64 bytes from 20.77.58.204: icmp_seq=219 ttl=115 time=11.178 ms
64 bytes from 20.77.58.204: icmp_seq=220 ttl=115 time=19.297 ms
64 bytes from 20.77.58.204: icmp_seq=221 ttl=115 time=18.751 ms
64 bytes from 20.77.58.204: icmp_seq=222 ttl=115 time=12.863 ms
64 bytes from 20.77.58.204: icmp_seq=223 ttl=115 time=11.811 ms
64 bytes from 20.77.58.204: icmp_seq=224 ttl=115 time=12.171 ms
64 bytes from 20.77.58.204: icmp_seq=225 ttl=115 time=19.622 ms
64 bytes from 20.77.58.204: icmp_seq=226 ttl=115 time=9.988 ms
64 bytes from 20.77.58.204: icmp_seq=227 ttl=115 time=13.289 ms
64 bytes from 20.77.58.204: icmp_seq=228 ttl=115 time=12.819 ms
64 bytes from 20.77.58.204: icmp_seq=229 ttl=115 time=12.138 ms
64 bytes from 20.77.58.204: icmp_seq=230 ttl=115 time=11.926 ms
64 bytes from 20.77.58.204: icmp_seq=231 ttl=115 time=12.691 ms
64 bytes from 20.77.58.204: icmp_seq=232 ttl=115 time=18.812 ms
64 bytes from 20.77.58.204: icmp_seq=233 ttl=115 time=13.728 ms
64 bytes from 20.77.58.204: icmp_seq=234 ttl=115 time=12.785 ms
64 bytes from 20.77.58.204: icmp_seq=235 ttl=115 time=11.815 ms
64 bytes from 20.77.58.204: icmp_seq=236 ttl=115 time=12.095 ms
64 bytes from 20.77.58.204: icmp_seq=237 ttl=115 time=11.868 ms
64 bytes from 20.77.58.204: icmp_seq=238 ttl=115 time=13.888 ms
64 bytes from 20.77.58.204: icmp_seq=239 ttl=115 time=12.868 ms
^C
--- 20.77.58.204 ping statistics ---
240 packets transmitted, 240 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.794/11.976/28.612/1.567 ms
comp@linux-machine-1:~$
```

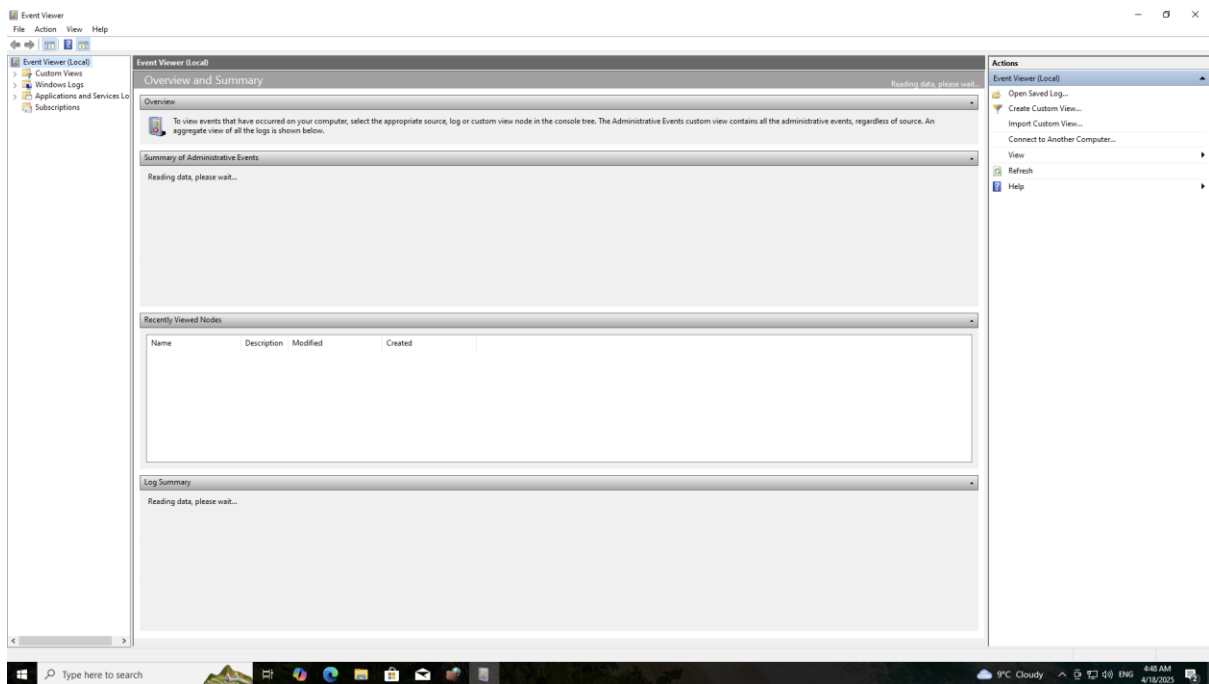
30) Next, log out of the virtual machine account, and intentionally enter incorrect credential a few times to fail the login attempt.



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

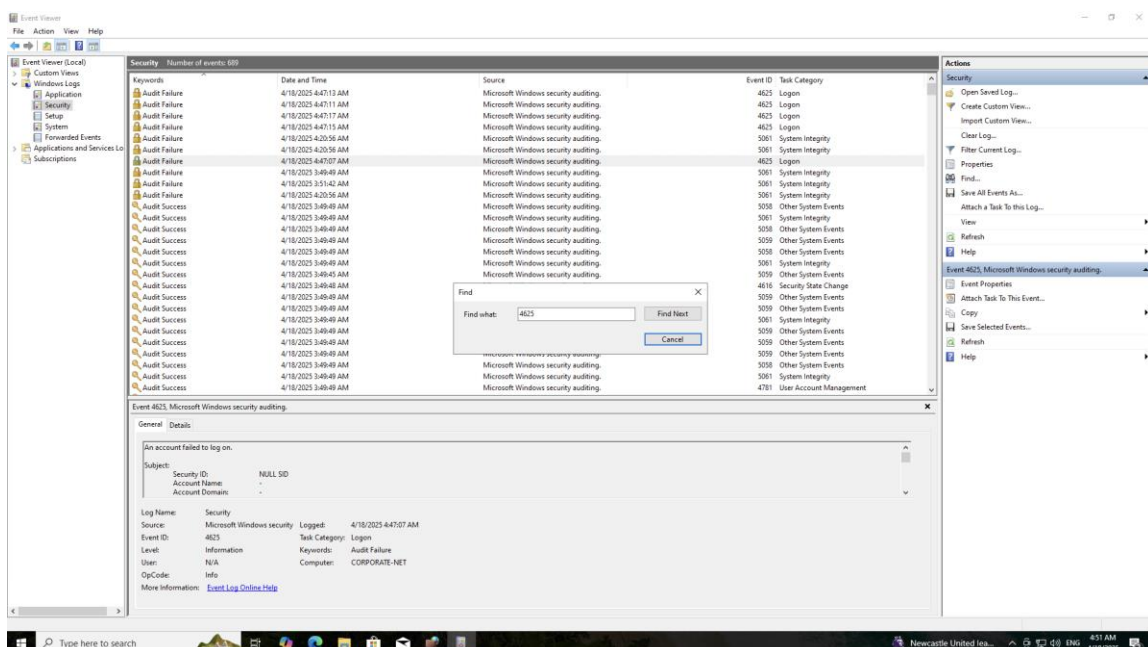


32) If anything happens on the computer, it gets logged. There are certain configurations that can be used to log specific activities, but there are already default settings in place that log activities, which is what we will be viewing.

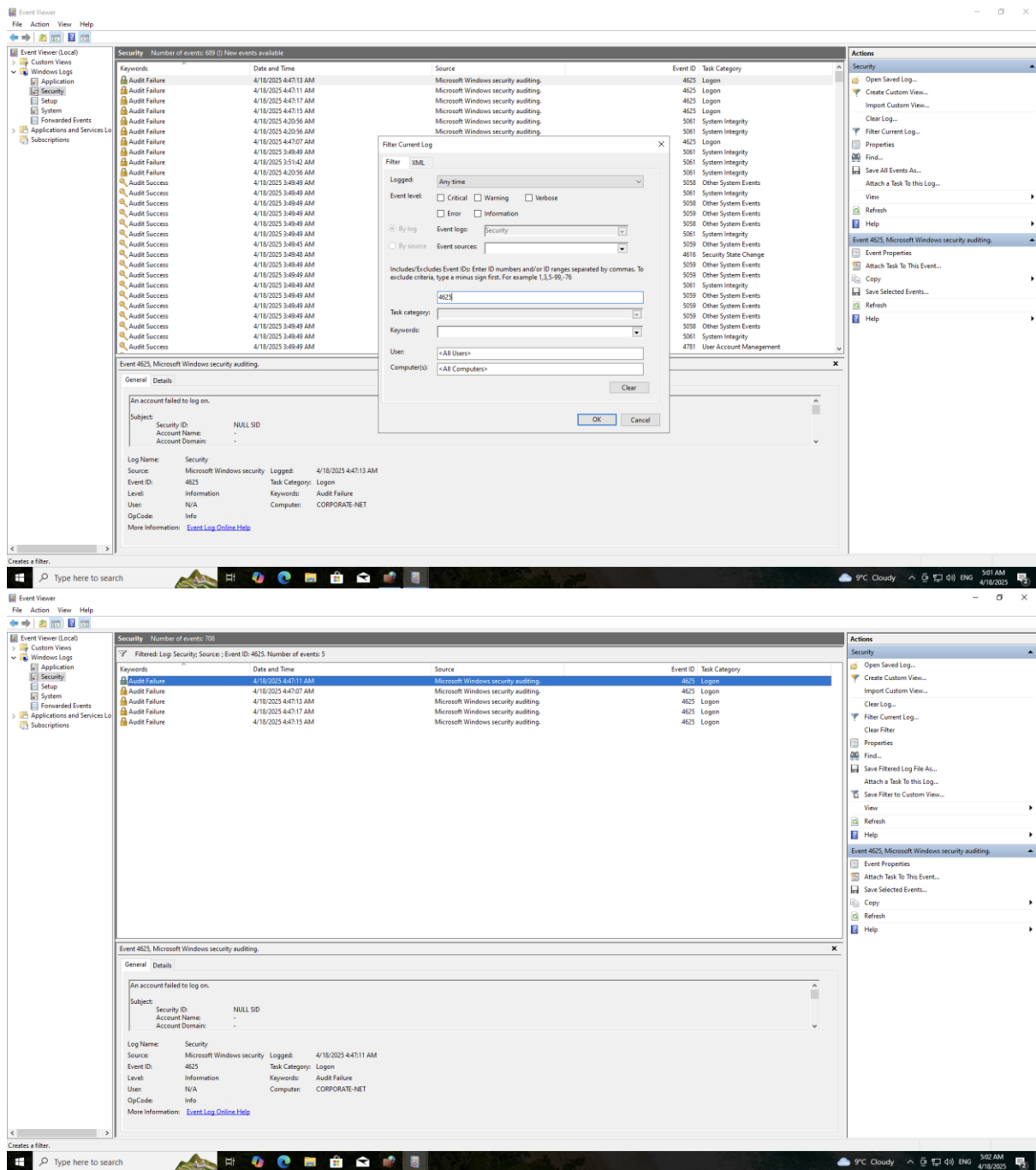


33) Look to the left of the screen and navigate to the security logs. Here you can see the different security events that took place. Each log is categorised into an event type, and is then labelled with a specific event ID.

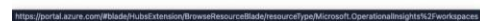
In the screenshot below I searched for the events with the ID “4625” using ctrl + f. This event ID number is given to failed login attempts.



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



- 1) Navigate to Log Analytics Workspace.



## Create Log Analytics workspace ...



Basics Tags Review + Create

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

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

## Project details

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

Subscription \*

Resource group \*   
[Create new](#)

## Instance details

Name \*

Region \*

Review + Create

Review + Create

&lt; Previous

Next: Tags &gt;

## Microsoft.LogAnalyticsOMS | Overview ...



Deployment

 Delete Cancel Redeploy Download Refresh

## Overview

Inputs

Outputs

Template

## Your deployment is complete

Deployment name : Microsoft.LogAnalyticsOMS  
Subscription : Azure subscription 1  
Resource group : SOC-Lab

Start time : 4/18/2025, 6:20:30 AM  
Correlation ID : 34a26c34-c700-421e-a7b8-fa5a677832d

## &gt; 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 >](#)

## 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 console. A modal window is open, displaying a list of services and marketplaces. The 'Add' button is visible in the bottom left corner of the console.

Microsoft Sentinel  
Default Directory (dejaview@outlook.onmicrosoft.com)

Filter for any field... Subscription equals all Resource group equals all Location equals all

Showing 0 to 0 of 0 records.

Name ↑

Subscription ↑

Directory ↑

Services (6) Marketplace (31) More (4)

Services

- Microsoft Sentinel
- Language
  - Keywords sentiment analysis, sentiment, aspect-based sentiment
- Azure Managed Redis (Preview)
  - Resource type: Microsoft.Cache/RedisEnterprise
- All Resources
  - Keywords sentiment analysis

Marketplace

- Language service
- Communication Services
- Twilio SendGrid
- Microsoft Defender for Endpoint

Documentation

- Deploying passwords and other sensitive data to ASP.NET and Azure App Service
- HoloLens (1st gen) and Azure 312 - Bot integration - Mixed Reality

Microsoft Entra ID

- MDC Data Sensitivity
  - Service Principal
- Continue searching in Microsoft Entra ID

Searching all subscriptions.

Give feedback

Home > Microsoft Sentinel

Add Microsoft Sentinel to a workspace

Create a new workspace Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

Workspace ↑	Location ↑	ResourceGroup ↑	Subscription ↑	Directory ↑
LAW-SOC-LAB-00	uksouth	soc-lab	Azure subscription 1	Default Directory

Add Cancel

- 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.



Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

## Microsoft Sentinel | Content hub

Selected workspace: 'law-soc-lab-00'

Search:  Refresh Install/Update Delete SIEM Migration Guides & Feedback

385 Solutions 307 Standalone contents 0 Installed 0 Updates

Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. [Learn more](#)

security event Status: All Content type: All Support: All Provider: All Category: All Content sources: All

Content title	Status	Content source	Provider	Support	Category
SlashNext Security Events	Not installed	Solution	SlashNext	SlashNext	Security - Network
SlashNextSecurityEventsforMicrosoftSentinel	Not installed	Solution	SlashNext	SlashNext	Security - Network
<input checked="" type="checkbox"/> Windows Security Events	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
NRT Security Event log cleared	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Event Analyzer	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
New EXE deployed via Default Domain or ...	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Gain Code Execution on AD FS Server via S...	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Excessive Windows Logon Failures	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Starting or Stopping HealthService to Avoi...	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Process Execution Frequency Anomaly	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
AD FS Remote Auth Sync Connection	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Potential Fodhelper UAC Bypass	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
AD user enabled and password not set wit...	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Scheduled Task Hide	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection

< Previous Page 1 of 2 Next > Showing 1 to 20 of 26 results.

Add or remove favorites by pressing Ctrl+Shift+F

### Windows Security Events

Microsoft Provider Microsoft Support 3.0.9 Version

Description

**Note:** Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

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.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

**NOTE:** Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

**Data Connectors:** 2. **Workbooks:** 2. **Analytic Rules:** 20. **Hunting Queries:** 50

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

[Install](#) [View details](#)

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

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

## Microsoft Sentinel | Content hub

Selected workspace: 'law-soc-lab-00'

Search:  Refresh Install/Update Delete SIEM Migration Guides & Feedback

385 Solutions 307 Standalone contents 1 Installed 0 Updates

Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. [Learn more](#)

security event Status: All Content type: All Support: All Provider: All Category: All Content sources: All

Content title	Status	Content source	Provider	Support	Category
SlashNext Security Events	Not installed	Solution	SlashNext	SlashNext	Security - Network
SlashNextSecurityEventsforMicrosoftSentinel	Not installed	Solution	SlashNext	SlashNext	Security - Network
<input checked="" type="checkbox"/> Windows Security Events	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
NRT Security Event log cleared	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Event Analyzer	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
New EXE deployed via Default Domain or ...	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Gain Code Execution on AD FS Server via S...	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Excessive Windows Logon Failures	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Starting or Stopping HealthService to Avoi...	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Process Execution Frequency Anomaly	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
AD FS Remote Auth Sync Connection	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Potential Fodhelper UAC Bypass	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
AD user enabled and password not set wit...	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Scheduled Task Hide	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection

< Previous Page 1 of 2 Next > Showing 1 to 20 of 26 results.

Add or remove favorites by pressing Ctrl+Shift+F

### Windows Security Events

Microsoft Provider Microsoft Support 3.0.9 Version

Description

**Note:** Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

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.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

**NOTE:** Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

**Data Connectors:** 2. **Workbooks:** 2. **Analytic Rules:** 20. **Hunting Queries:** 50

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

[Manage](#) [Actions](#) [View details](#)

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".



Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub >

## Windows Security Events

Refresh Delete Reinstall

74 Installed content items 22 Configuration needed

### Windows Security Events

Microsoft Provider 3.0.9 Version

Description

**Note:** Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

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.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using this Data Connector.
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

**NOTE:** Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

**Data Connectors:** 2 **Workbooks:** 2 **Analytic Rules:** 20 **Hunting Queries:** 50

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Content type

20 Analytics rule 2 Data connector 50 Hunting query

Manage Actions View details

Search...

Content name	Created content	Content ty...	Version	Status
Security Events via Legacy Agent	1 items	Data connec...	1.0.0	Install
Windows Security Events via AMA	1 items	Data connec...	1.0.0	Install
AD FS Remote Auth Sync Connection	--	Analytics rule	1.0.4	Install
AD FS Remote HTTP Network Connection	--	Analytics rule	1.0.2	Install
AD user enabled and password not set within 48 hours	--	Analytics rule	1.0.4	Install
ADFS Database Named Pipe Connection	--	Analytics rule	1.0.2	Install
Excessive Windows Logon Failures	--	Analytics rule	2.0.3	Install
Exchange OAB Virtual Directory Attribute Containing Potential Webshell	--	Analytics rule	1.0.4	Install
Gain Code Execution on ADFS Server via SMB + Remote Service or Scheduled Task	--	Analytics rule	1.2.1	Install
Microsoft Entra ID Local Device Join Information and Transport Key Registry Keys Access	--	Analytics rule	1.0.5	Install
New EXE deployed via Default Domain or Default Domain Controller Policies	--	Analytics rule	1.0.2	Install
Non Domain Controller Active Directory Replication	--	Analytics rule	1.0.4	Install
NRT Base64 Encoded Windows Process Command-lines	--	Analytics rule	1.0.2	Install
NRT Process executed from binary hidden in Base64 encoded file	--	Analytics rule	1.0.2	Install
NRT Security Event log cleared	--	Analytics rule	1.0.1	Install
Potential Fodhelper UAC Bypass	--	Analytics rule	1.0.2	Install
Potential re-named delete usage	--	Analytics rule	1.0.3	Install
Process Execution Frequency Anomaly	--	Analytics rule	1.0.6	Install

< Previous Page 1 of 3 Next > Showing 1 to 30 of 74 results.

### Windows Security Events via AMA

Disconnected Status Microsoft Provider Last Log Received

Last data received --

Content source Windows Security Events Version 1.0.0

Author Microsoft Supported by Microsoft Corporation | Email

Data received

Go to query

SecurityEvents

0

Data types SecurityEvents --

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.

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub > Windows Security Events >

## Windows Security Events via AMA

### Windows Security Events via AMA

Disconnected Status Microsoft Provider Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received --

Content source Windows Security Events Version 1.0.0

Author Microsoft Supported by Microsoft Corporation | Email

Related content

0 Workbooks 1 Queries 20 Analytics rules templates

Data received

Go to log analytics

SecurityEvents

0

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

**Rule details**

Rule name \* DCR-WINDOWS

Subscription \* Azure subscription 1

Resource group \* SOC-Lab

Next Resources

- 6) 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

Windows Security Events via AMA

Disconnected

Microsoft

Provider

Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

Content source

Windows Security Events

Version

1.0.0

Author

Microsoft

Supported by

Microsoft Corporation | Email

Related content

0 Workbooks

1 Queries

20 Analytics rules templates

Data received

Go to log analytics

0 SecurityEvents

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.

Subscriptions

Selected: All

Resource Groups

Selected: All

Resource Types

Selected: All

Locations

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

Windows Security Events via AMA

Disconnected

Microsoft

Provider

Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

Content source

Windows Security Events

Version

1.0.0

Author

Microsoft

Supported by

Microsoft Corporation | Email

Related content

0 Workbooks

1 Queries

20 Analytics rules templates

Data received

Go to log analytics

0 SecurityEvents

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

Windows Security Events via AMA

Disconnected

Microsoft

Provider

Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

Content source

Windows Security Events

Version

1.0.0

Author

Microsoft

Supported by

Microsoft Corporation | Email

Related content

0 Workbooks

1 Queries

20 Analytics rules templates

Data received

Go to log analytics

0 SecurityEvents

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

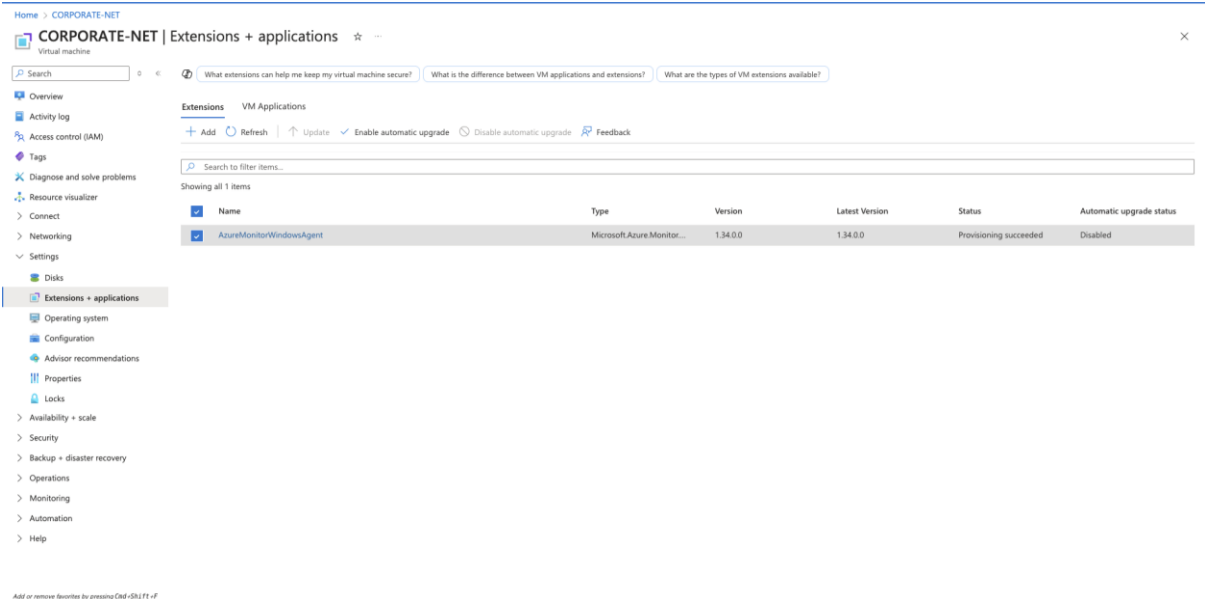
Selected events

AllEvents

Previous

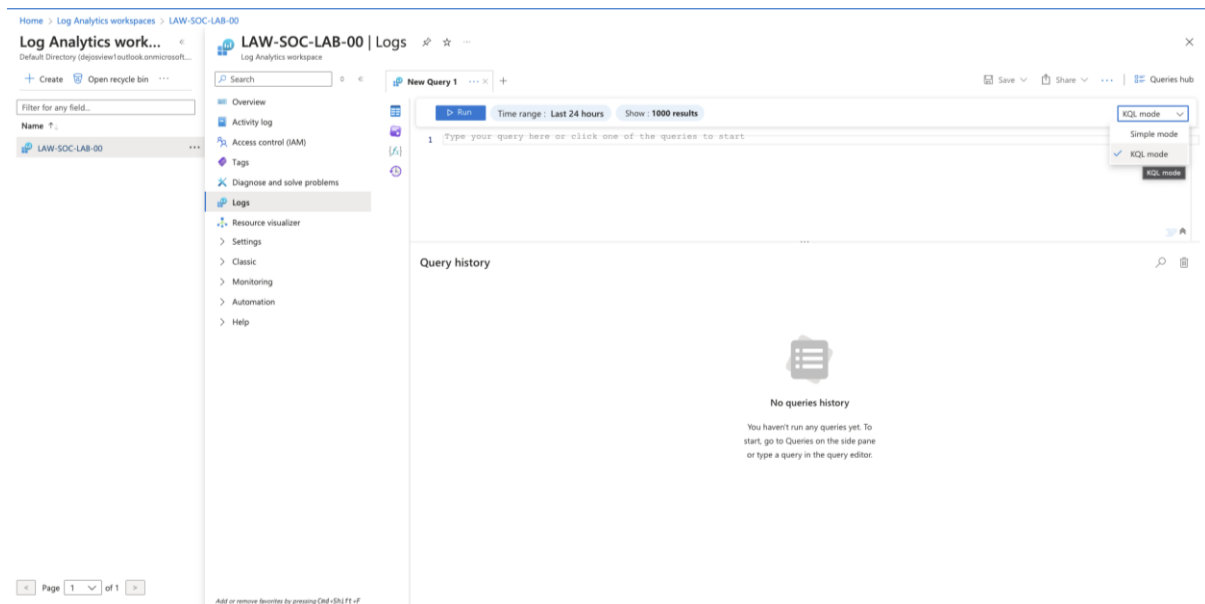
Create

- 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.



## 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.

Home > Log Analytics workspaces > LAW-SOC-LAB-00

Log Analytics work...  
Default Directory (loganalytics.azure.com/microsoft...)

+ Create Open recycle bin ...

Filter for any field...

Name ?

LAW-SOC-LAB-00 ...

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Logs  
Resource visualizer  
Settings  
Classic  
Monitoring  
Automation  
Help

LAW-SOC-LAB-00 | Logs

Log Analytics workspace

Search

New Query 1\* ...

Run Time range: Last 24 hours Show: 1000 results KQL mode

1 SecurityEvent

TimeGenerated (UTC)	Account	AccountType	Computer	EventSourceName	Channel	Task	Level	EventData	EventID	Activity
4/18/2025, 5:47:59.621 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:58.592 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:58.451 AM	User1	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:57.758 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:56.863 AM	User	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:56.847 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:55.983 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:55.253 AM	Admin	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:55.126 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:54.247 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:53.911 AM	Admin2	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:53.388 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:52.484 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:52.451 AM	User1	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:51.613 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A
4/18/2025, 5:47:50.718 AM	Administrator	User	CORPORATE-NET	Microsoft-Windows-Security-Auditing	Security	12544	0		4625	4625 - A

Page 1 of 1

0s 628ms Display time (UTC+00:00)

Query details 1 - 16 of 677

- 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.

Home > Log Analytics workspaces > LAW-SOC-LAB-00

Log Analytics work...  
Default Directory (loganalytics.azure.com/microsoft...)

+ Create Open recycle bin ...

Filter for any field...

Name ?

LAW-SOC-LAB-00 ...

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Logs  
Resource visualizer  
Settings  
Classic  
Monitoring  
Automation  
Help

LAW-SOC-LAB-00 | Logs

Log Analytics workspace

Search

New Query 1\* ...

Run Time range: Last 24 hours Show: 1000 results KQL mode

```
1 SecurityEvent
2 | where Account == "\Administrator"
3 | project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
```

TimeGenerated (UTC)	Account	Computer	EventID	Activity	IpAddress
4/18/2025, 6:12:39.219 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:12:38.219 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:12:37.294 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:12:36.441 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:12:02.227 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:12:01.359 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:12:00.493 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:59.511 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:58.618 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:57.718 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:56.844 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:55.980 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:55.090 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:54.220 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:53.357 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82
4/18/2025, 6:11:52.514 AM	Administrator	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82

Page 1 of 1

0s 488ms Display time (UTC+00:00)

Query details 1 - 16 of 326

- 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 == 4265

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 Log Analytics workspace interface. On the left, there's a sidebar with navigation options like Overview, Activity log, Access control (IAM), Tags, and Logs. The main area displays a query named 'New Query 1\*' with the following KQL code:

```
1 SecurityEvent
2 | where EventID == 4625
3 | where TimeGenerated > ago(5m)
4 | project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
```

The results table shows a list of failed login attempts. The first row is highlighted:

TimeGenerated [UTC]	Account	Computer	EventID	Activity	IpAddress
4/18/2025, 6:15:59:386 AM	Vfor	CORPORATE-NET	4625	4625 - An account failed to log ...	115.245.191.82

- 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. The search bar contains the IP address '115.245.191.0/24'. The results show the location is in India, specifically in the state of Bihar. The summary table provides details about the IP 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.

Products

Solutions

Why IPinfo?

Pricing

Resources

115.245.191.821/1

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	—	0	⊗	⊗

Explore our IP Address Database Downloads for instant access to our IP address insights

Learn more

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

🖥️ webservers

Search an IP or ASN 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

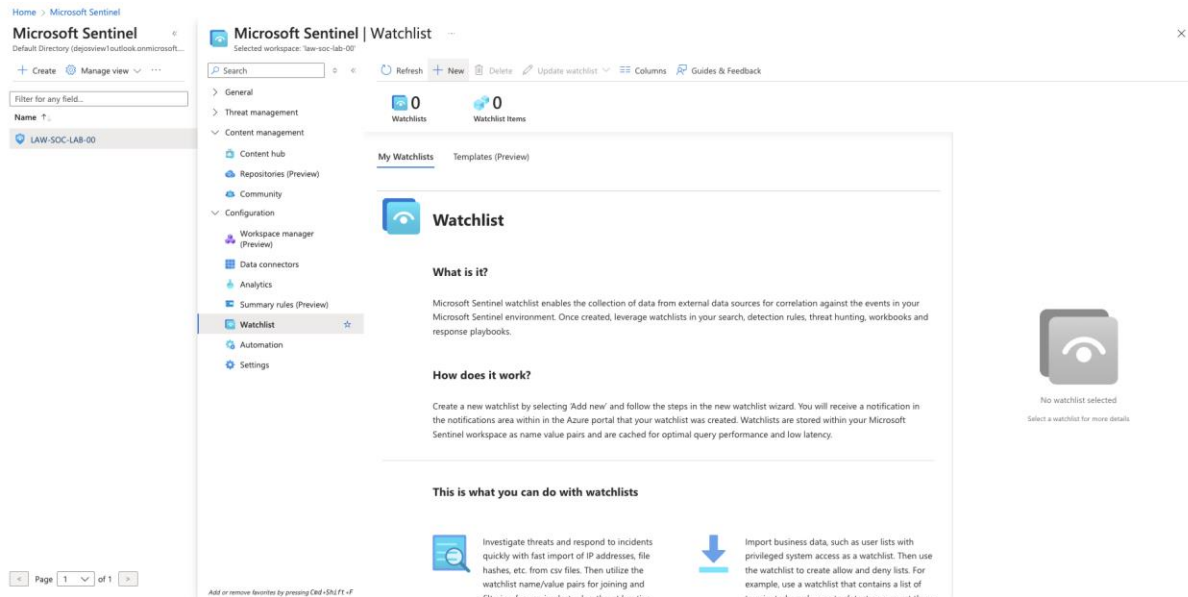
ip.abuse@ril.com

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.

The screenshot shows the 'Watchlist wizard' in Microsoft Sentinel. It has three tabs: 'General', 'Source', and 'Review + create'. The 'General' tab is active, showing input fields for 'Name \*', 'Description', and 'Alias \*'. The 'Name' and 'Alias' fields both contain the text 'geoiip'. At the bottom, there is a 'Next: Source >' button and a 'Give feedback' link.

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

## Watchlist wizard



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 \*  geoup-summarized.csvDrag and drop the files or [Browse for files](#)

SearchKey \* network

[Reset](#)

File preview | First 50 rows and first 5 columns

network	latitude	longitude	cityname	countryname
1.0.0.0/16	-33.494	143.2104		Australia
1.1.0.0/16	17.8148	103.3386	Ban Chan	Thailand
1.2.0.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
1.3.0.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
1.4.0.0/16	13.6687	100.579	Bangkok	Thailand
1.5.0.0/16	13.6659	100.5882	Bangkok	Thailand
1.6.0.0/16	12.9634	77.5855	Bengaluru	India
1.7.0.0/16	12.9691	77.5902	Bengaluru	India
1.8.0.0/16	12.9557	77.5843	Bengaluru	India
1.9.0.0/16	3.1539	101.7448	Ampang	Malaysia

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

## 4) Click create.

## Watchlist wizard



General Source Review + create

Name \* geoup

Description

Alias \* geoup

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.



Microsoft Sentinel | Watchlist

Selected workspace: law-soc-lab-00

Search: [Search by name, alias and description]

Refresh New Delete Update watchlist Columns Guides & Feedback

0 Watchlists 0 Watchlist items

My Watchlists Templates (Preview)

Name	Alias	Source	Create...	Last u...
geoip	geoip	geoip-sum	4/18/2025	4/18/2025

geoip

Microsoft Provider 0 Rows 4/18/2025, 7:36:47 AM Created time

Description

Source: geoip-summarized.csv

Created by: dejosview1@outlook.com

Last updated: 4/18/2025, 7:36:47 AM

SearchKey: network

Status (Preview): Uploading (25.55%)

View in logs Update watchlist

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.

Log Analytics workspace | LAW-SOC-LAB-00

Log Analytics workspace

Search: [Search]

New Query 1\* Time range: Last 24 hours Show: 1000 results

1 SecurityEvent

2

3 \_GetWatchlist("geoip")

Results Chart

LastUpdatedTime(UTC)	_DfItemid	Searchkey	cityname	countryname	latitude
4/18/2025, 6:36:47.537 AM	6514283a-bb6d-4b1c-ac17-500...	72.149.0.0/16	Grottoes	United States	38.2543
4/18/2025, 6:36:47.537 AM	2ec4e1b2-441e-4b87-9a05-988...	72.154.0.0/16	Grottoes	United States	38.2543
4/18/2025, 6:36:47.537 AM	798a0a3c-a19f-47da-8a0d-04f...	72.158.0.0/16	Grottoes	United States	38.2476
4/18/2025, 6:36:47.537 AM	22c9446-250b-47a9-b0d4-16a...	72.159.0.0/16	Grottoes	United States	38.2444
4/18/2025, 6:36:47.537 AM	19326da-c08b-499b-8764-f0ca...	72.166.0.0/16	Redwater	Canada	53.952
4/18/2025, 6:36:47.537 AM	725990e-3d5b-46b8-a5c7-ca0...	72.169.0.0/16	Thorold	Canada	54.1495
4/18/2025, 6:36:47.537 AM	aa17304a-7a15-4e0d-b5cc-ebc...	72.194.0.0/16	Olmsted Falls	United States	41.3747
4/18/2025, 6:36:47.537 AM	47716bc-a7ec-408f-b92d-3edf...	72.201.0.0/16	Santee	United States	32.8466
4/18/2025, 6:36:47.537 AM	5ab879a9-b5fa-451f-800b-40b...	72.206.0.0/16	Phoenix	United States	33.4512
4/18/2025, 6:36:47.537 AM	f3d5dbec-c1af-4b64-8aaa-db7...	72.208.0.0/16	Mesa	United States	33.3825
4/18/2025, 6:36:47.537 AM	a04c5381-7d45-4477-9a15-889...	72.219.0.0/16	New York	United States	40.7263
4/18/2025, 6:36:47.537 AM	636e4733-4019-4b0c-85b5-a35...	72.225.0.0/16	Kaneohe	United States	21.4254
4/18/2025, 6:36:47.537 AM	239e6d0f-e9ff-4d82-8b4f-9a22...	72.229.0.0/16	Clermont	United States	28.5531
4/18/2025, 6:36:47.537 AM	3749005a-1169-4fca-a53f-8fb1...	72.231.0.0/16	Toledo	United States	41.703
4/18/2025, 6:36:47.537 AM	c7587114-c69f-443a-b01b-343...	72.242.0.0/16	Dolores	United States	37.4587
4/18/2025, 6:36:47.537 AM	7b-d5a5-316-430b-870b-07b...	72.250.0.0/16	Knoxville	United States	37.1444

16 items Display time (UTC+00:00)

Query details 1 - 16 of 1000

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

Home > Log Analytics workspaces > LAW-SOC-LAB-00

Log Analytics work...  
Default Directory

+ Create Open recycle bin ...

Filter for any field...

Name ↑

LAW-SOC-LAB-00 ...

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Logs  
Resource visualizer  
Settings  
Classic  
Monitoring  
Automation  
Help

LAW-SOC-LAB-00 | Logs

New Query 1\* ...  
D. Run Time range: Last 24 hours Show: 1000 results KQL mode

```
1 SecurityEvent
2 | where EventID == "4625"
```

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task
4/18/2025, 1:16:31.581 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:30.551 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:30.268 PM	\ADMIN	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:30.232 PM	\ADMINISTRATOR	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:29.537 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:28.512 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:27.646 PM	\ADMIN	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:27.598 PM	\ADMINISTRATOR	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:27.494 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:26.479 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:25.455 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:24.433 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:23.521 PM	\ADMINISTRATOR	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:23.437 PM	\ADMIN	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:23.417 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12
4/18/2025, 1:16:22.405 PM	\minimal	User	CORPORATE-NET	Microsoft-Windows-Security-A...	Security	12

Page 1 of 1

0s 62ms Display time (UTC+00:00)

Query details 1 - 16 of 1000

- 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.

Home > Log Analytics workspaces > LAW-SOC-LAB-00

Log Analytics work...  
Default Directory

+ Create Open recycle bin ...

Filter for any field...

Name ↑

LAW-SOC-LAB-00 ...

LAW-SOC-LAB-00 | Logs

New Query 1\* ...  
D. Run Time range: Last 24 hours Show: 1000 results KQL mode

```
1 let GeoIPDB_FULL = _getMatchlist("geoip");
2 let WindowsEvents = SecurityEvent
3 | where IpAddress == "201.187.98.150"
4 | where EventID == 4625
5 | order by TimeGenerated desc
6 | evaluate ipn_lookup(GeoIPDB_FULL, IpAddress, network);
7 WindowsEvents
8 | project TimeGenerated, Computer, AttackerIP = IpAddress, cityname, countryname, latitude, longitude
```

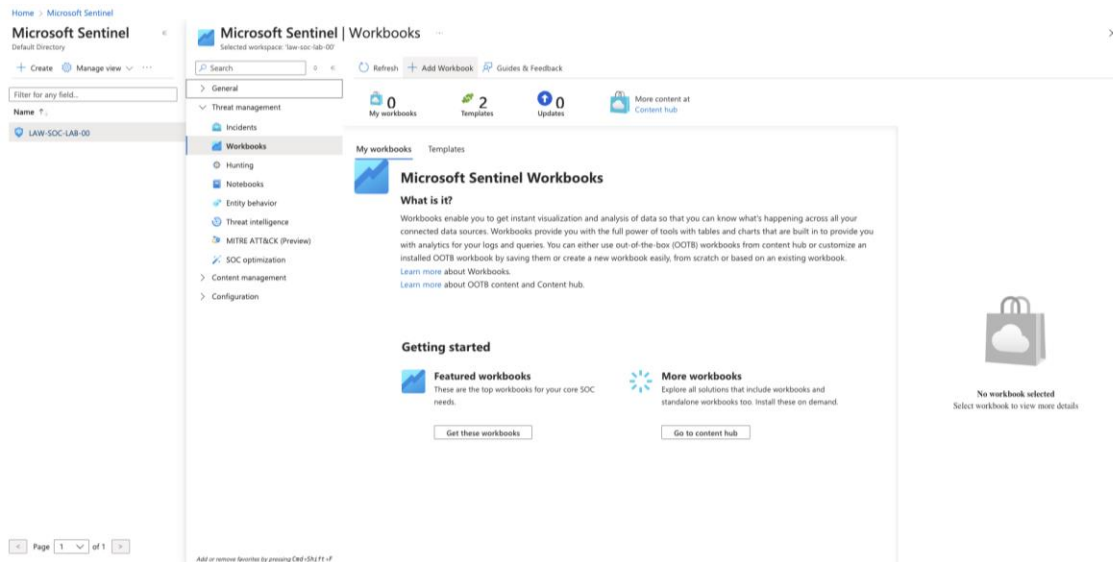
TimeGenerated [UTC]	Computer	AttackerIP	cityname	countryname	latitude	longitude
4/18/2025, 1:25:33.188 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:32.175 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:31.154 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:30.139 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:29.125 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:28.106 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:27.083 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:26.056 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:25.047 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:24.031 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:23.017 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:21.992 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:20.967 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:19.948 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:18.935 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984
4/18/2025, 1:25:17.911 PM	CORPORATE-NET	201.187.98.150	Valparaiso	Chile	-33.0447	-71.5984

Page 1 of 1

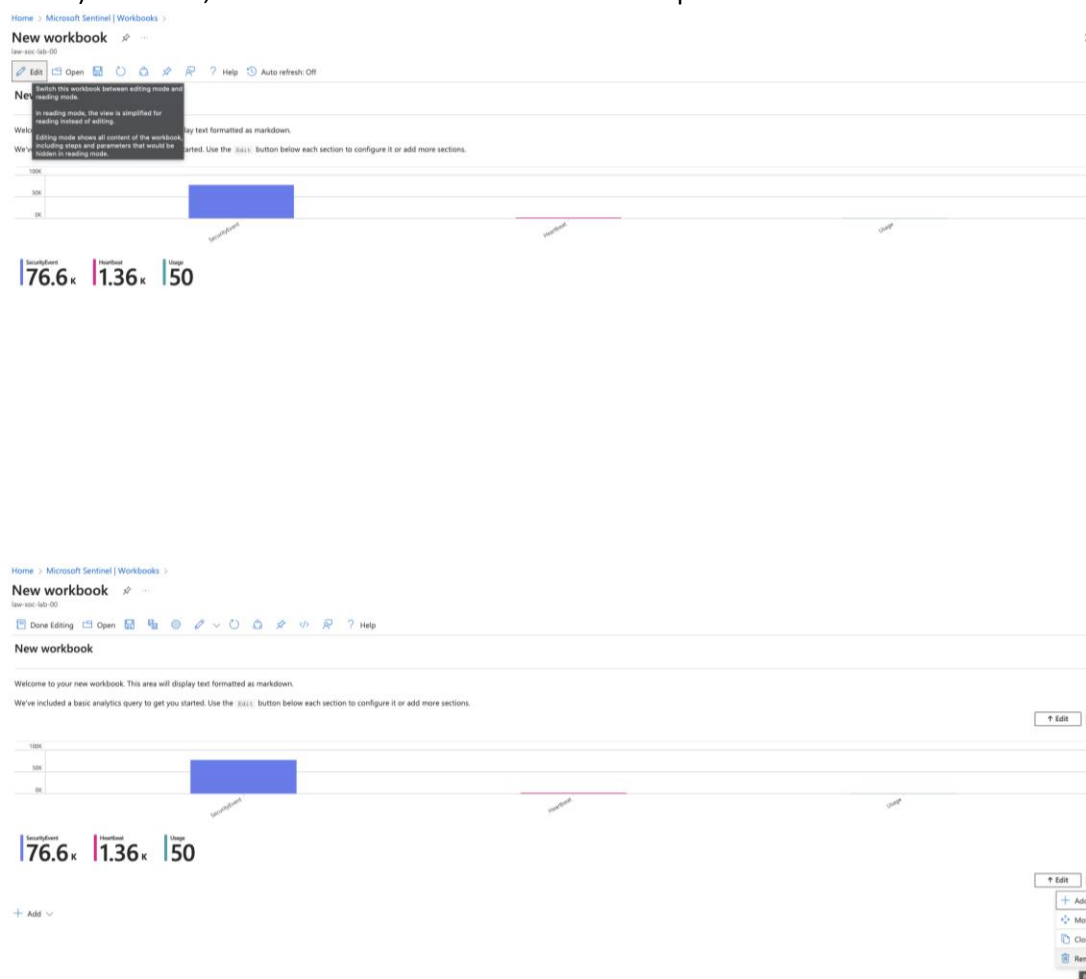
0s 567ms Display time (UTC+00:00)

Query details 1 - 16 of 1000

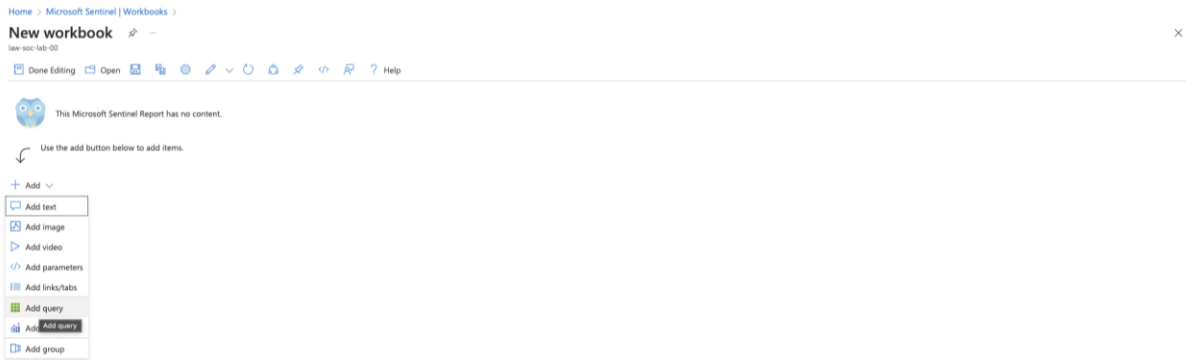
- 9) Go to Sentinel and select Workbooks



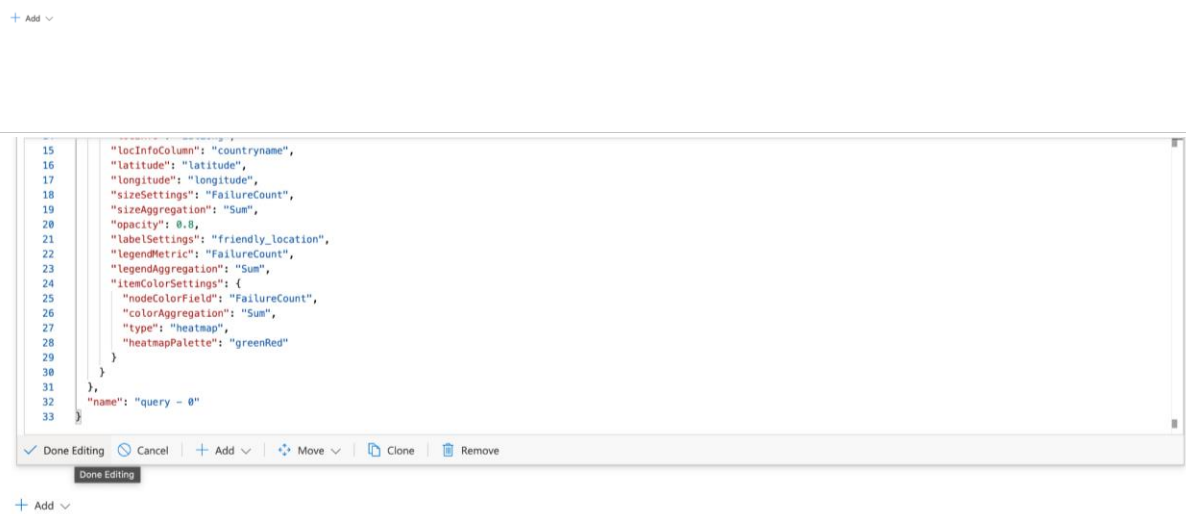
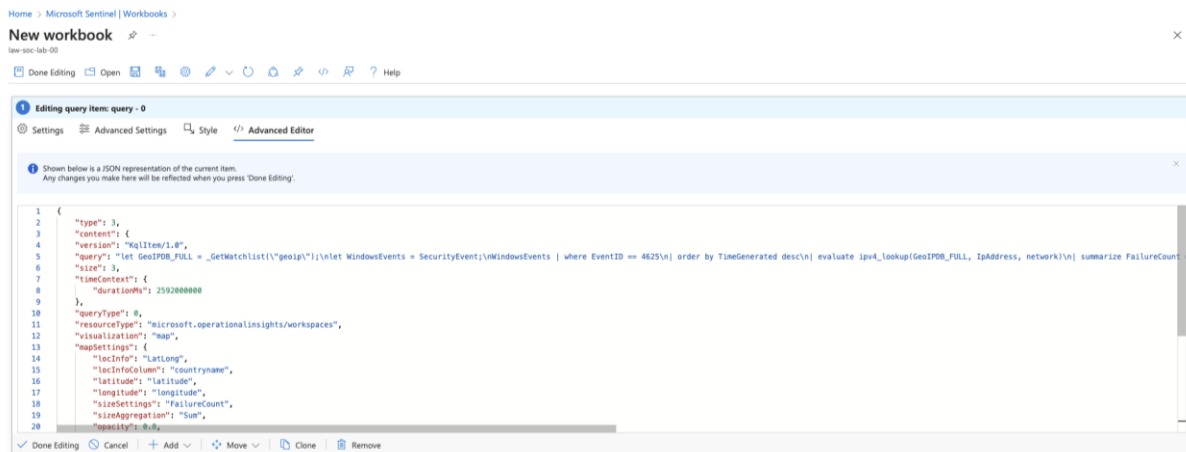
10) Click edit, then remove all the elements that are preset in the workbook.



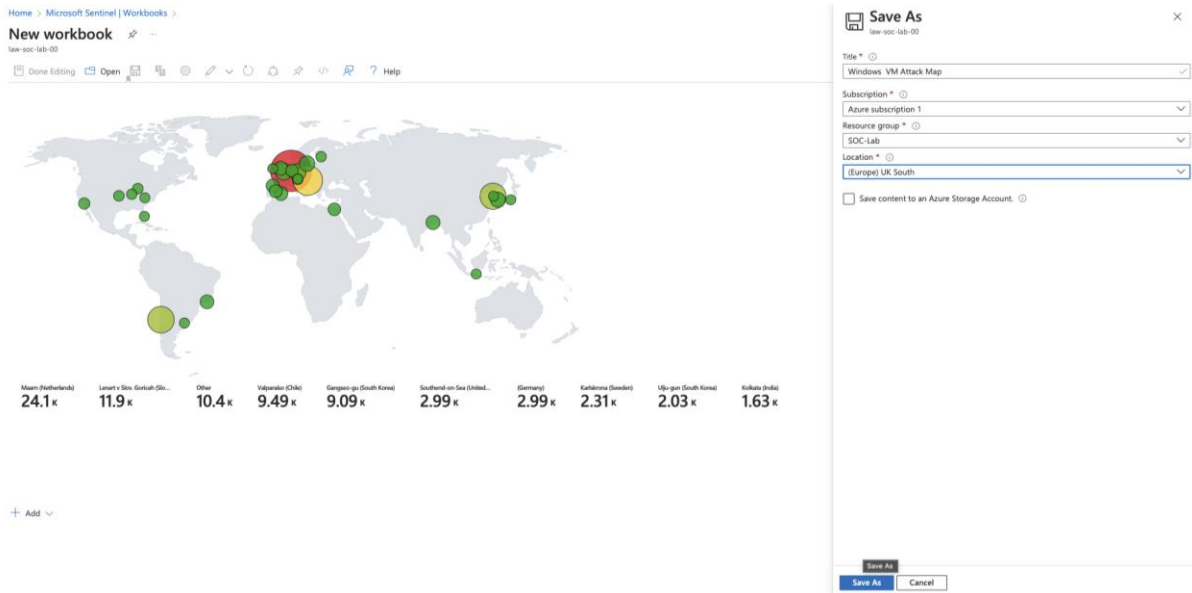
11) Select add, then click add query.



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.