

Cyber Home Lab

By: Keziah Rogers

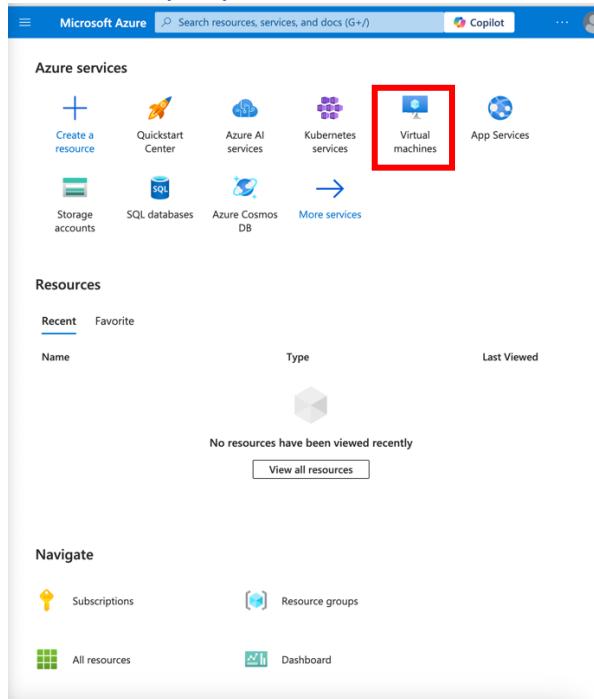
Part 1. Setup Azure Subscription

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

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

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

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



The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo, a search bar, and a Copilot button. Below the navigation bar, the 'Azure services' section is visible, featuring various icons for different services like 'Create a resource', 'Quickstart Center', 'Azure AI services', 'Kubernetes services', 'Virtual machines' (which is highlighted with a red box), and 'App Services'. Below this, the 'Resources' section shows a 'Recent' tab selected, with a table for viewing resources by Name, Type, and Last Viewed. A message indicates 'No resources have been viewed recently' with a 'View all resources' button. At the bottom, the 'Navigate' section includes links for 'Subscriptions', 'Resource groups', 'All resources', and 'Dashboard'.

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

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

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

The screenshot shows the Microsoft Azure Resource Groups page. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and a Copilot icon. Below it is a breadcrumb trail: 'Home > Resource groups'. The main title is 'Resource groups'. There are filter options: 'Subscription equals all' (selected), 'Location equals all', and a 'Create' button. Below the filters, it says 'Showing 0 to 0 of 0 records.' and has sorting options for 'Name ↑', 'Subscription ↑', and 'Location ↑'. In the center, there's a large icon of a cube and the text 'No resource groups to display'. Below that, a descriptive text reads: 'Resource groups provide a logical container to manage and organize Azure resources, simplifying administration and enabling efficient resource management.' A red box highlights the '+ Create' button.

of the actions that I performed.

The screenshot shows the 'Create a resource group' wizard. The top navigation bar includes 'Microsoft Azure', a search bar, and a Copilot icon. The breadcrumb trail is 'Home > Resource groups > Create a resource group'. The main title is 'Create a resource group'. Below it are three tabs: 'Basics' (selected), 'Tags', and 'Review + create' (highlighted with a red box). Under the 'Basics' tab, there's an 'Automation Link' section with a link to 'Automation Link'. The 'Basics' section shows the following configuration:

Subscription	Azure subscription 1
Resource group name	RG-SOC-Lab
Region	East US 2

Under the 'Tags' tab, it says 'None'.

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

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

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 *: RG-SOC-Lab

Instance details

Virtual network name *: Vnet-soc-lab
Region *: (US) East US 2

Deploy to an Azure Extended Zone

and hit next.

I then hit next to keep the

default IP addresses and tags, and then hit create.

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

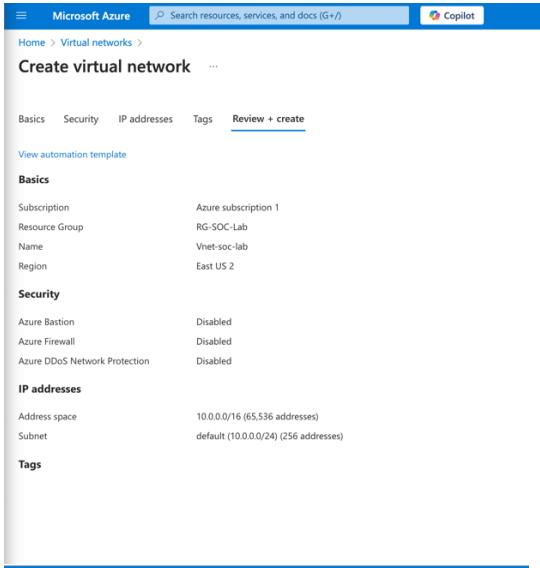
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
default	10.0.0 - 10.0.255	/24 (256 addresses)	-

Add IPv4 address space |

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

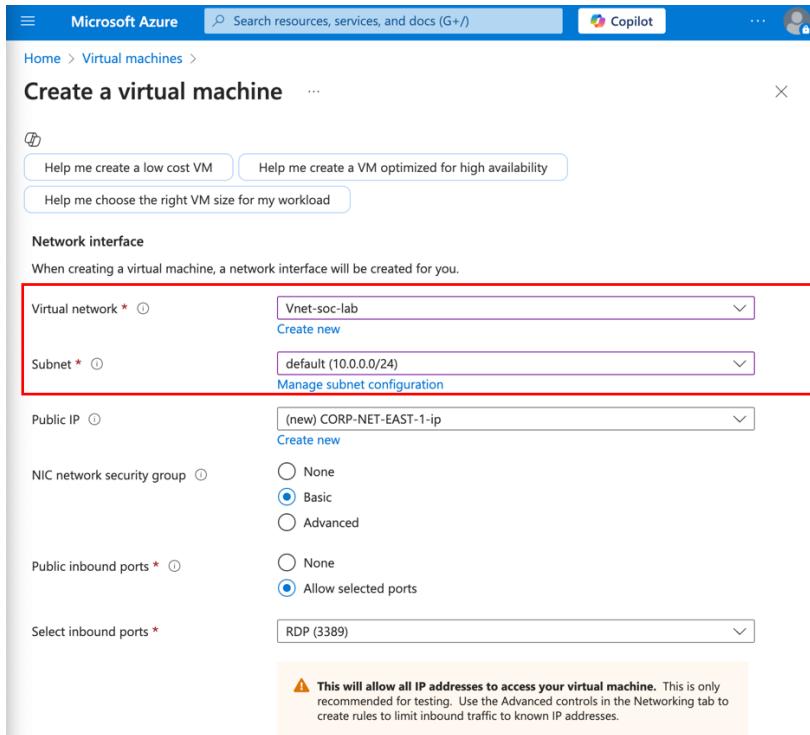


6)

- 7) Next, I created the Virtual Machine.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, 'Copilot' integration, and user account information. Below the header, the 'Virtual machines' section is displayed under 'Default Directory'. A sub-header 'Subscription equals all' is visible. The main content area displays a message: 'No virtual machines to display' with a small icon of a computer monitor. Below this, instructions say: 'Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.' A dropdown menu titled '+ Create' is open, showing four options: 'Azure virtual machine' (which is highlighted with a red box), 'Azure virtual machine with preset configuration', and 'More VMs and related solutions'. At the bottom right of the dropdown is a 'Give feedback' link.

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



9)

Delete public IP and NIC when VM is

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

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

The screenshot shows the Azure Resource Groups interface for the 'RG-SOC-Lab' group. The 'Resources' tab is active, displaying a list of six resources:

- CORP-NET-EAST-1 (Virtual machine)
- CORP-NET-EAST-1-ip (Public IP address)
- CORP-NET-EAST-1... (Network security group)
- corp-net-east-1788... (Network Interface)
- CORP-NET-EAST-1... (Disk)
- Vnet-soc-lab (Virtual network)

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

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

The screenshot shows the Azure Network Security Group (NSG) interface for 'CORP-NET-EAST-1-nsg'. The 'Inbound Security Rules' section is highlighted with a red box, showing the following rules:

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBou...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

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

The screenshot shows the Microsoft Azure portal interface for managing a Network Security Group (NSG). On the left, the navigation pane is visible with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Inbound security rules (which is selected and highlighted in grey), Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Automation, and Help. The main content area is titled "Add inbound security rule" for the NSG "CORP-NET-EAST-1-nsg". The form fields are as follows:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Service:** Custom
- Destination port ranges:** *
- Protocol:** Any (radio button selected)
- Action:** Allow (radio button selected)
- Priority:** 100
- Name:** DANGER__AllowAnyCustomAnyInbound (this field is highlighted with a red border)
- Description:** (empty)

At the bottom right of the dialog are "Add" and "Cancel" buttons, and a "Give feedback" link.

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

Add inbound security rule

CORP-NET-EAST-1-nsg

Deny

Priority * ⓘ
100

Name *
DANGER__AllowAnyCustomAnyInbound ✓

Description

Warning: 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.

Warning: 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.

Warning: 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.

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

Add **Cancel** [Give feedback](#)

CORP-NET-EAST-1-nsg | Inbound security rules

Network security group

Search

[Add](#) [Hide default rules](#) [Refresh](#) [Delete](#) [Give feedback](#)

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

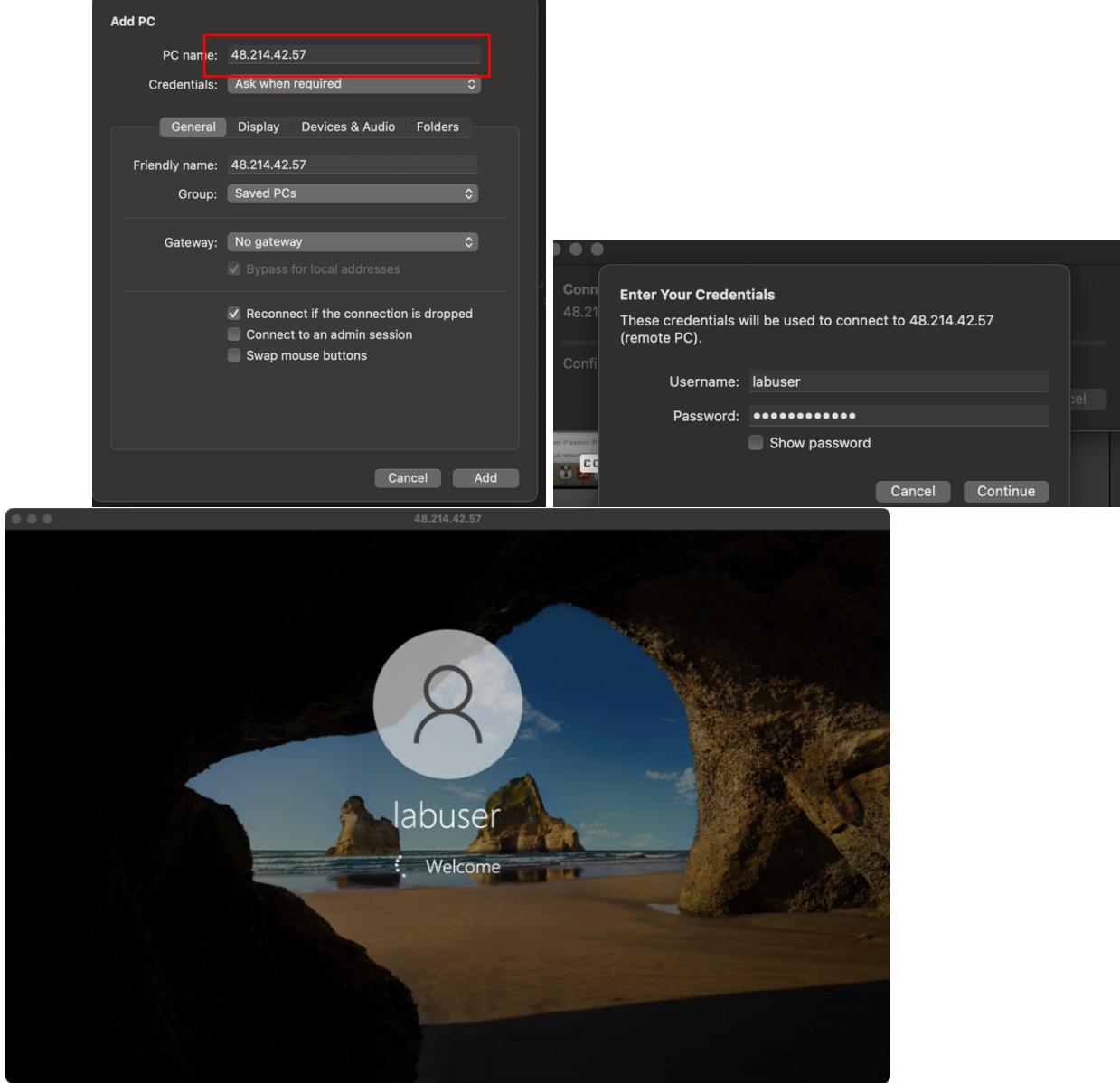
Filter by name

Port == all	Protocol == all	Source == all	Destination == all
Action == all			
Priority ↑↓	Name ↑↓	Port ↑↓	Protocol
<input type="checkbox"/> 100	⚠ DANGER__AllowA...	Any	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any

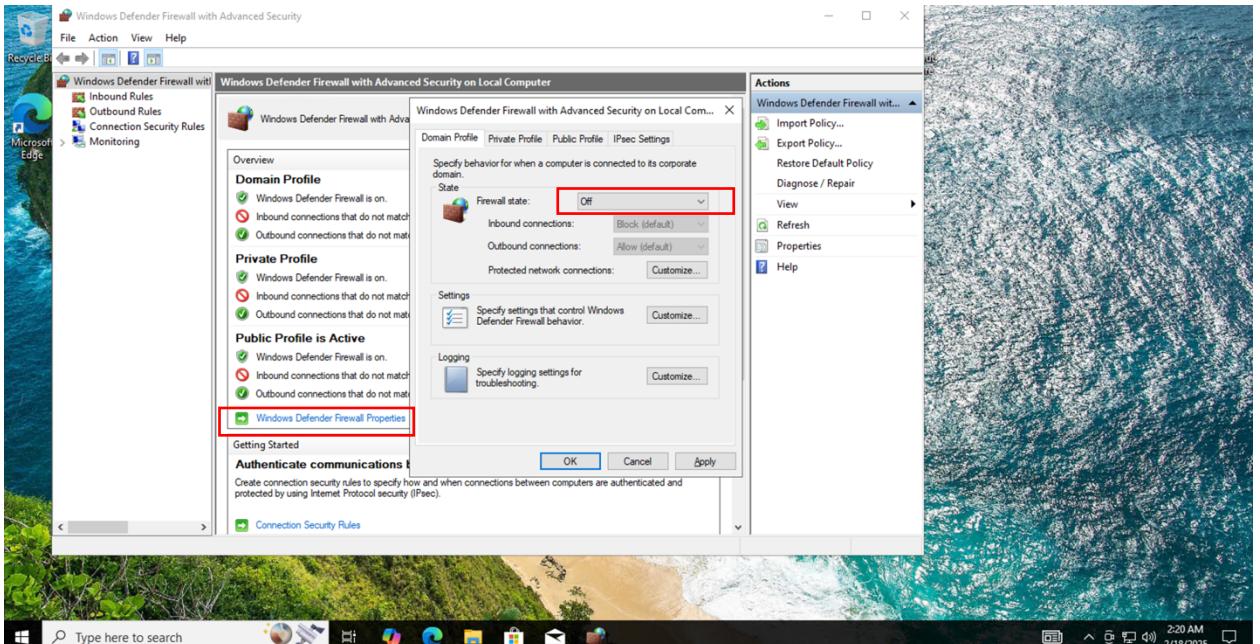
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Inbound security rules
 - Outbound security rules
 - Network interfaces
 - Subnets
 - Properties
 - Locks
- Monitoring
- Automation
- Help

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

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



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



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

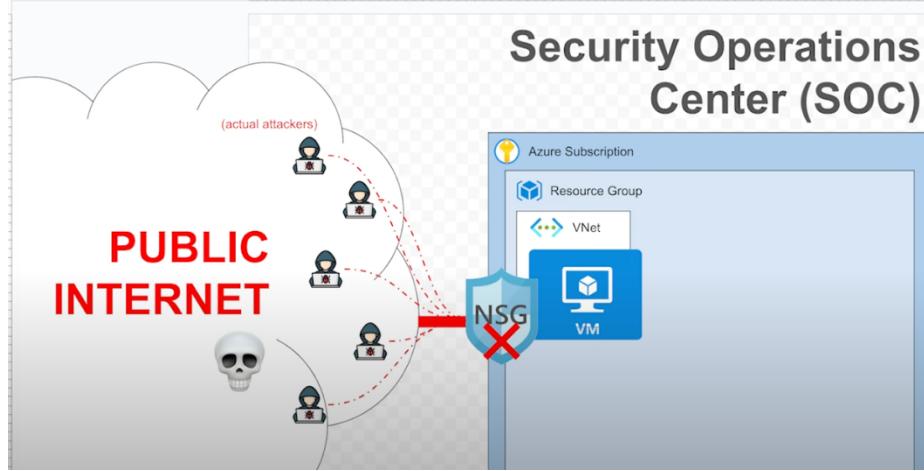
```

keziahrogers@Keziah-MacBook-Air ~ % ping 48.214.42.57
PING 48.214.42.57 (48.214.42.57): 56 data bytes
64 bytes from 48.214.42.57: icmp_seq=0 ttl=111 time=37.143 ms
64 bytes from 48.214.42.57: icmp_seq=1 ttl=111 time=28.103 ms
64 bytes from 48.214.42.57: icmp_seq=2 ttl=111 time=27.660 ms
64 bytes from 48.214.42.57: icmp_seq=3 ttl=111 time=26.232 ms
64 bytes from 48.214.42.57: icmp_seq=4 ttl=111 time=27.648 ms
64 bytes from 48.214.42.57: icmp_seq=5 ttl=111 time=27.484 ms
64 bytes from 48.214.42.57: icmp_seq=6 ttl=111 time=38.196 ms
64 bytes from 48.214.42.57: icmp_seq=7 ttl=111 time=27.253 ms
64 bytes from 48.214.42.57: icmp_seq=8 ttl=111 time=27.603 ms
64 bytes from 48.214.42.57: icmp_seq=9 ttl=111 time=25.256 ms
64 bytes from 48.214.42.57: icmp_seq=10 ttl=111 time=27.547 ms
64 bytes from 48.214.42.57: icmp_seq=11 ttl=111 time=22.074 ms
64 bytes from 48.214.42.57: icmp_seq=12 ttl=111 time=25.490 ms
64 bytes from 48.214.42.57: icmp_seq=13 ttl=111 time=28.379 ms
64 bytes from 48.214.42.57: icmp_seq=14 ttl=111 time=21.736 ms
64 bytes from 48.214.42.57: icmp_seq=15 ttl=111 time=26.205 ms
64 bytes from 48.214.42.57: icmp_seq=16 ttl=111 time=24.725 ms
64 bytes from 48.214.42.57: icmp_seq=17 ttl=111 time=28.667 ms
64 bytes from 48.214.42.57: icmp_seq=18 ttl=111 time=26.812 ms
64 bytes from 48.214.42.57: icmp_seq=19 ttl=111 time=27.612 ms
64 bytes from 48.214.42.57: icmp_seq=20 ttl=111 time=22.758 ms
64 bytes from 48.214.42.57: icmp_seq=21 ttl=111 time=27.465 ms
64 bytes from 48.214.42.57: icmp_seq=22 ttl=111 time=28.231 ms
64 bytes from 48.214.42.57: icmp_seq=23 ttl=111 time=26.946 ms
64 bytes from 48.214.42.57: icmp_seq=24 ttl=111 time=25.223 ms
64 bytes from 48.214.42.57: icmp_seq=25 ttl=111 time=27.421 ms
64 bytes from 48.214.42.57: icmp_seq=26 ttl=111 time=28.127 ms
64 bytes from 48.214.42.57: icmp_seq=27 ttl=111 time=23.937 ms
^C
--- 48.214.42.57 ping statistics ---
28 packets transmitted, 28 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 21.736/26.926/37.143/2.793 ms
keziahrogers@Keziah-MacBook-Air ~ %

```

the internet)

Snapshot of the blank architecture so far:



Part 3. Logging into the VM and inspecting logs

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

Screenshot of the Windows Event Viewer showing security logs. The main pane displays a list of events under the 'Security' category, with 573 total events. A red box highlights several 'Audit Failure' events on 2/18/2025 at various times between 1:46:41 AM and 2:33:52 AM. The 'Actions' pane on the right shows options like 'Open Saved Log...', 'Create Custom View...', and 'Properties'. A specific event, 'Event 4625, Microsoft Windows security auditing.', is selected and expanded. The 'General' tab shows the message: 'An account failed to log on.' and the subject: 'Log Name: Security'. The 'Details' tab shows the event properties, including the source 'Microsoft Wind...' and task category 'System Integrity'. The status bar at the bottom indicates 'Action: In progress...'. The title bar of the window reads 'Event Viewer'.

Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

Account For Which Logon Failed:

- Security ID: NULL SID
- Account Name: **employee** highlighted
- Account Domain: -

Failure Information:

- Failure Reason: Unknown user name or bad password.
- Status: 0xC000006D
- Sub Status: 0xC0000064

Process Information:

- Caller Process ID: 0x0

Log Name: Security
Source: Microsoft Windows security
Event ID: 4625
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

Sub Status: 0xC0000064

Process Information:

- Caller Process ID: 0x0
- Caller Process Name: -

Network Information:

- Workstation Name: -
- Source Network Address: **60.255.12.230** highlighted
- Source Port: 0

Detailed Authentication Information:

- Logon Process: NtLmSsp
- Authentication Package: NTLM
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most

Log Name: Security
Source: Microsoft Windows security
Event ID: 4625
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

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

Part 4. Log Forwarding and KQL

- I created a Log Analytics Workspace

A screenshot of the Azure portal's 'Create Log Analytics workspace' wizard. The 'Basics' tab is active. A tooltip at the top left says: '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](#)'.

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 *: RG-SOC-Lab (dropdown menu, 'Create new' option available)

Instance details
Name *: LAW-soc-lab-0000
Region *: East US 2

Review + Create < Previous Next : Tags >

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

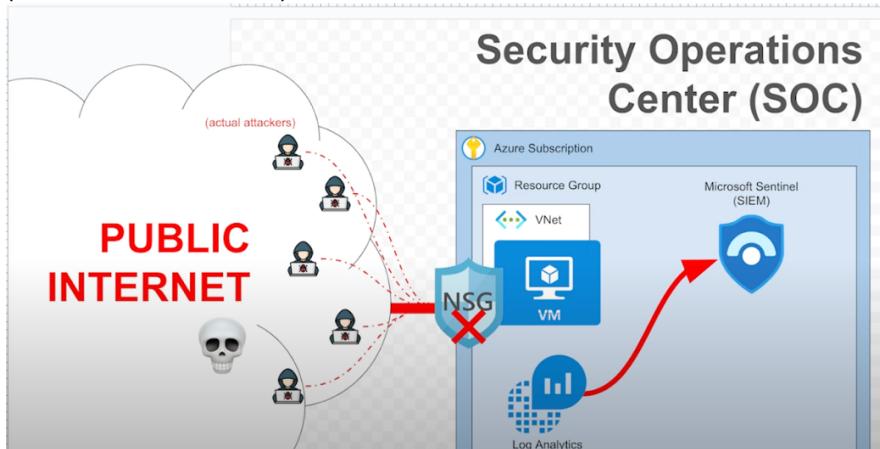
A screenshot of the Azure portal's 'Add Microsoft Sentinel to a workspace' page. It shows a list of workspaces:

Workspace	Location	ResourceGroup	Subscription	Directory
LAW-soc-lab-0000	eastus2	rg-soc-lab	Azure subscription 1	Default Directory

Filter by name...
 + Create a new workspace Refresh

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

- (observe architecture)



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



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

Microsoft Sentinel | Content hub

Selected workspace: 'law-soc-lab-0000'

Content hub

382 Solutions 307 Standalone contents 0 Installed 0 Updates

Didn't find what you were looking for? Refining your search for more specific results.

security event

Status: All Content type: All Content sources: All

Content title

Windows Security

Event Analyzer NRT Security Event log collector New EXE deployed via D

Gain Code Execution on Excessive Windows Logon Starting or Stopping Headless Process Execution F

Content type: 20 Analytics rule: 2 Data connector: 50 Hunting query: 2 Workbooks: 2

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

< Previous Page 1 of 2 Install View details

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

Microsoft Azure Search resources, services, and docs (G+/-) Copilot ...

... > 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. [Learn more](#)

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

- I queried for logs within the LAW

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs (which is selected), Settings, Classic, Monitoring, Automation, and Help. The main area displays a query editor with the following code:

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

The results table shows three rows of data:

TimeGenerated [UTC]	Account	Computer	EventID	Activity	IpAddress
2/18/2025, 3:13:19.922 AM	\CLAUDIA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	92.63.197.9
2/18/2025, 3:11:14.244 AM	\CLAUDIA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	94.102.52.73
2/18/2025, 3:11:09.952 AM	\CLAUDIA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107

Below the results table, there is another table with the same columns and data.

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

ipinfo.io/ips/92.63.197.0/24

STUDENT LOANS SHOWS Wear & Carry TRADING CYBER SECURITY BANKING All Bookmarks

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

IPinfo Products Solutions Why IPinfo? Pricing Resources Docs

92.63.197.0/24 IP Range

All IP Ranges > 92.0.0.0/8 IP Range > 92.63.0.0/16 IP Range > 92.63.197.0/24 IP Range

Summary

ASN	AS210848 Telkom Internet LTD
BGP	92.63.197.0/24
IPs with RDNS	0
Hosted Domains	0
Pingable IPs	8
Router IPs	0

IP ADDRESS	HOSTNAME	DOMAINS	PINGABLE	ROUTER
92.63.197.0	—	0	✗	✗
92.63.197.1	—	0	✓	✗
92.63.197.2	—	0	✗	✗

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

The screenshot shows the Microsoft Log Analytics workspace interface. At the top, there's a navigation bar with 'New Query 1*', a '+' button, 'Try the new Log An...', 'Feedback', 'Queries hub', and other options. Below the bar, a red box highlights the query editor area where the following PowerShell-like query is written:

```

1 SecurityEvent
2 | where EventID == 4625
3 | project TimeGenerated, Account, Computer, EventID, Activity, IpAddress

```

Below the query editor is a table titled 'Results' showing the query results. The table has columns: TimeGenerated [UTC], Account, Computer, and EventID. The data shows multiple entries for EventID 4625 across various accounts and computers. A red box highlights the bottom right corner of the table area, which displays 'Query details' and '1 - 13 of 13773'.

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

Part 5. Log Enrichment and Finding Location Data

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

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

Downloaded from: [geoip-summarized.csv](#)

Within Sentinel, I create the watchlist:

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

Microsoft Azure Search resources, services, and docs (G+) Copilot ...

Home > Microsoft Sentinel | Watchlist >

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 * geoip-summarized.csv

Drag 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

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

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

The screenshot shows the Microsoft Sentinel Watchlist interface. On the left, a sidebar lists categories like General, Threat management, Content management, Configuration, and Watchlist (which is selected). The main area displays a summary: 1 Watchlists and 55K Watchlist Items. A detailed view of the 'geoip' watchlist is shown, including its provider (Microsoft), rows (55K), and creation time (2/17/2025). The watchlist description is 'geoip-summarized.csv', created by keziahrogers@outlook.com, last updated on 2/17/2025 at 10:35:46 PM, with a search key 'network'. The status is 'Succeeded'. Navigation controls at the bottom include 'View in logs' and 'Update watchlist'.

(observe architecture)

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

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

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

(observe architecture)

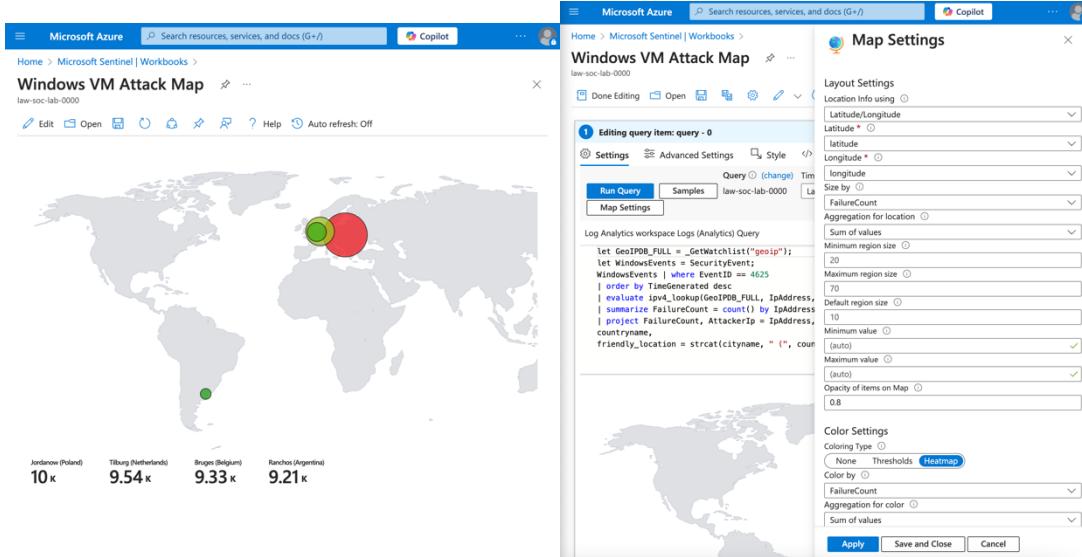
Part 6. Attack Map Creation

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

Workbook (Attack map):

[map.json](#)

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



Home > Microsoft Sentinel | Workbooks >

Windows VM Attack Map

law-soc-lab-0000

Editing query item: query - 0

Advanced Editor

Query (change) Time Range Visualization Size

Run Query

Samples

law-soc-lab-0000

Last 30 days

Map

Full

Log Analytics workspace Logs (Analytics) Query

Query help

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

