

Cybersecurity Home Lab Project using Microsoft Sentinel 2025

Name: Phanindhar Reddy Karnati

Date: 06/14/2025

Table of Contents

1. Azure Account Creation and Access
2. Resource Group Setup
3. Virtual Network and Subnet Configuration
4. Deploying the Windows Virtual Machine (Honeypot)
5. Configuring Network Security Group (NSG)
6. Disabling Windows Defender Firewall
7. Generating Simulated Attack Logs
8. Verifying Logs Using Event Viewer
9. Creating Log Analytics Workspace (LAW)
10. Deploying Microsoft Sentinel Instance
11. Enabling Log Forwarding with Azure Monitoring Agent (AMA)
12. Confirming Log Ingestion via KQL Queries
13. Uploading GeoIP Watchlist to Sentinel
14. Joining Security Logs with GeoIP Data
15. Visualizing Attacks on World Map (Attack Map Workbook)
16. Conclusion

Introduction

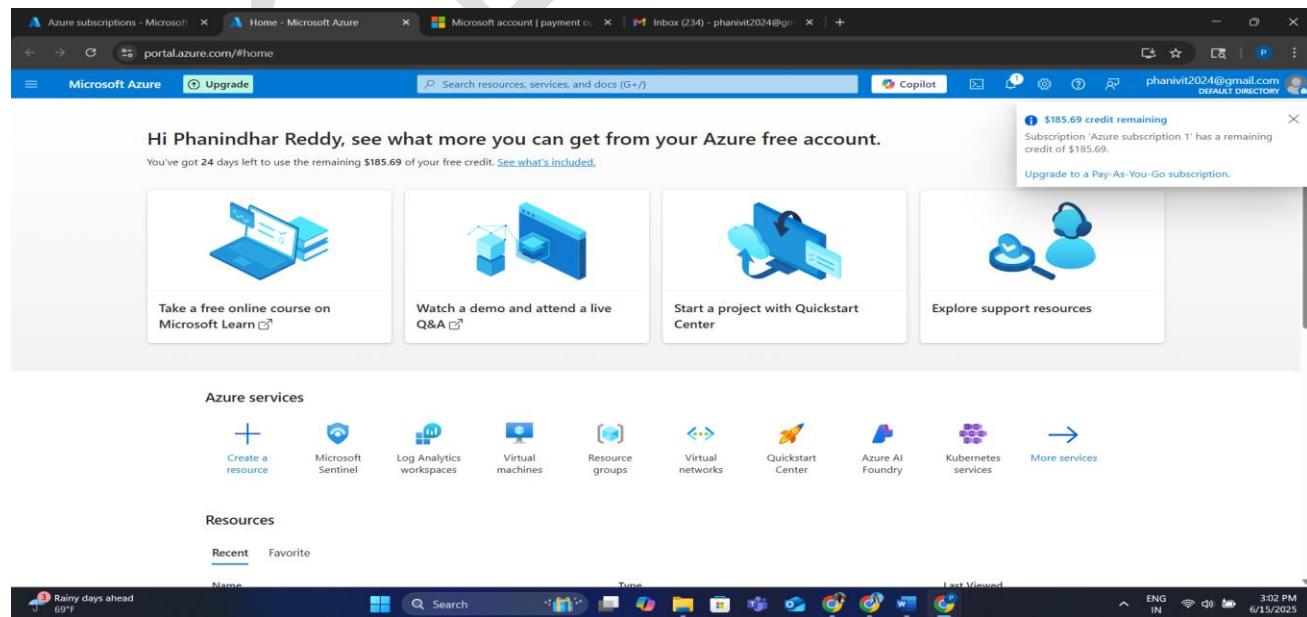
This project outlines the creation and deployment of a cloud-based home Security Operations Center (SOC) using Microsoft Azure and Microsoft Sentinel. The lab provides real-world simulation experience by configuring a honeypot virtual machine (VM) to receive actual malicious traffic from the internet. Through this setup, we demonstrate how to monitor, analyze, and visualize attack patterns using security event logs, Kusto Query Language (KQL), and geographic enrichment via a custom IP-to-location watchlist. This lab is suitable for beginners, professionals, and cybersecurity students seeking hands-on SIEM experience that can be highlighted on resumes.

1. Azure Account Creation and Access

Before deploying any infrastructure, a free Azure subscription is created. Microsoft requires a credit card to verify the user. If a free account is unavailable, users may opt for:

- A pay-as-you-go Azure model (billed like a utility)
- Accessing Azure through the paid "Cyber Range" platform which includes other cybersecurity tools like Tenable

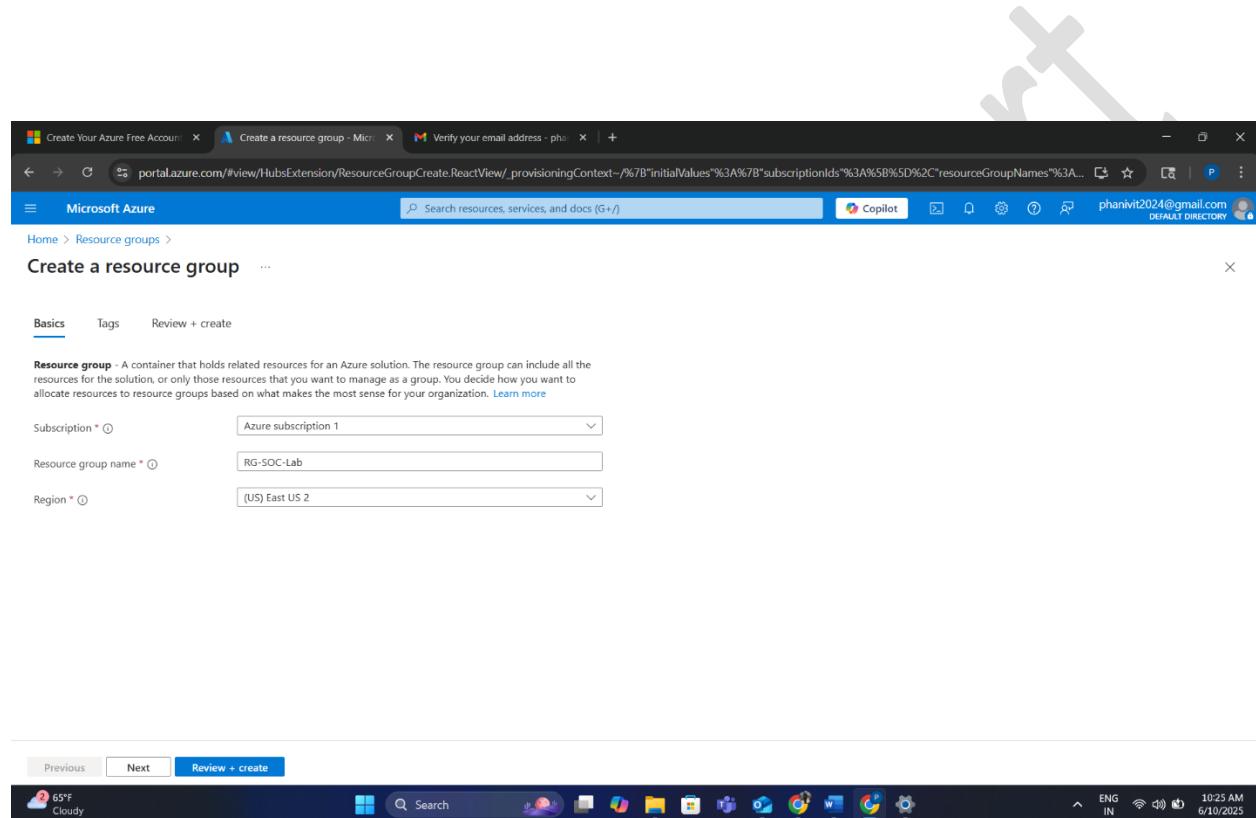
Once an account is active, users can access the Azure dashboard through portal.azure.com.



2. Resource Group Setup

Resource groups in Azure serve as containers for related resources.

- They allow easier management, deletion, and auditing of associated services.



- We created a resource group named rg-socklab in the "East US 2" region to ensure data locality for our VMs and networking resources.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'Create Your Azure Free Account', 'Resource groups - Microsoft Azure', and 'Verify your email address - ph...'. The main title is 'Resource groups' under 'Microsoft Azure'. A search bar at the top right contains the placeholder 'Search resources, services, and docs (G+ /)'. On the far right, the user's email 'phanvit2024@gmail.com' and 'DEFAULT DIRECTORY' are visible. Below the title, there are filter options: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A note says 'You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.' There are also 'Filter for any field...' and 'Subscription equals all' dropdowns, along with a '+ Add filter' button. The main content area shows a table with columns 'Name', 'Subscription', and 'Location'. One entry is listed: 'RG-SOC-Lab' (Subscription: Azure subscription 1, Location: East US 2). At the bottom, it says 'Showing 1 - 1 of 1. Display count: 10' and has a 'Give feedback' link.

3. Virtual Network and Subnet Configuration

A Virtual Network (VNet) simulates a traditional networking environment in the cloud. It functions like a router at home, enabling internal communication and internet exposure:

- A VNet named vnet-soclab was created in the same resource group.
- A default subnet was automatically created within the VNet, enabling internal VM traffic.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'Create Your Azure Free Account', 'Virtual networks - Microsoft Azure', and 'Verify your email address - ph...'. The main title is 'Virtual networks' under 'Microsoft Azure'. A search bar at the top right contains the placeholder 'Search resources, services, and docs (G+ /)'. On the far right, the user's email 'phanvit2024@gmail.com' and 'DEFAULT DIRECTORY' are visible. Below the title, there are filter options: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A note says 'You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.' There are also 'Filter for any field...', 'Subscription equals all', 'Resource Group equals all', 'Location equals all', and a '+ Add filter' button. The main content area features a large 'No virtual networks to display' message with a network icon. Below it, a sub-message reads: 'Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.' It includes a '+ Create' button and a 'Learn more' link. At the bottom, it says 'Showing 1 - 0 of 0. Display count: 10' and has a 'Give feedback' link.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The top navigation bar includes tabs for 'Create Your Azure Free Account', 'Create virtual network - Micro...', and 'Verify your email address - ph...'. The main title is 'Create virtual network ...'. Below it, the 'Project details' section asks for a subscription and resource group, with 'Subscription' set to 'Azure subscription 1' and 'Resource group' set to 'RG-SOC-Lab'. The 'Instance details' section specifies a 'Virtual network name' of 'Vnet-soc-lab' and a 'Region' of '(US) East US 2'. At the bottom, there are 'Previous' and 'Next' buttons, and a prominent 'Review + create' button.

The screenshot shows the 'Create virtual network' wizard on the 'Security' step. The top navigation bar and title remain the same. The 'Virtual network encryption' section contains a note about enabling encryption for traffic within the virtual network. The 'Virtual network encryption' checkbox is checked. The 'Azure Bastion' section notes that it provides secure RDP/SSH connectivity over TLS. The 'Enable Azure Bastion' checkbox is checked. The 'Azure Firewall' section is present but not detailed. At the bottom, there are 'Previous' and 'Next' buttons, and a 'Review + create' button.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The top navigation bar includes tabs for 'Create Your Azure Free Account', 'Create virtual network - Micro...', and 'Verify your email address - ph...'. The main title is 'Create virtual network' under 'Virtual networks'. The 'IP addresses' tab is selected. A sub-section titled 'Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need.' has a 'Learn more' link. Below it, a note says '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.' with another 'Learn more' link. A button '+ Add a subnet' is visible. The main area shows an IP address space configuration for '10.0.0.0/16' with a range of '10.0.0.0 - 10.0.255.255' and '65,536 addresses'. A table lists a single subnet named 'default' with an IP address range of '10.0.0.0 - 10.0.0.255' and a size of '/24 (256 addresses)'. At the bottom are 'Previous', 'Next', and 'Review + create' buttons, along with a 'Give feedback' link. The status bar at the bottom right shows 'ENG IN' and the date '6/10/2025'.

The screenshot shows the 'Create virtual network' process on the 'Basics' step. The top navigation bar and title are identical. The 'Review + create' button is now highlighted. The 'Basics' section contains fields for 'Subscription' (Azure subscription 1), 'Resource Group' (RG-SOC-Lab), 'Name' (Vnet-soc-lab), and 'Region' (East US 2). The 'Security' section includes 'Azure Bastion' (Disabled), 'Azure Firewall' (Disabled), and 'Azure DDoS Network Protection' (Disabled). The 'IP addresses' section shows the address space '10.0.0.0/16 (65,536 addresses)' and the default subnet 'default (10.0.0.0/24) (256 addresses)'. At the bottom are 'Previous', 'Next', and 'Create' buttons, along with a 'Give feedback' link. The status bar at the bottom right shows 'Finance headline Fed awaits inflati...' and the date '6/10/2025'.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface. At the top, there are three tabs: "Create Your Azure Free Account", "Vnet-soc-lab-1749566894569", and "Verify your email address - ph...". The main title bar says "Microsoft Azure" and has a search bar. On the right, there's a Copilot icon, a user profile for "phanivit2024@gmail.com", and a "DEFAULT DIRECTORY" button.

The main content area displays the "Overview" of a deployment named "Vnet-soc-lab-1749566894569". It shows a green checkmark indicating the deployment is complete. Deployment details include:

- Deployment name: Vnet-soc-lab-1749566894569
- Subscription: Azure subscription 1
- Resource group: RG-SOC-Lab

Timestamp: Start time : 6/10/2025, 10:48:18 AM
Correlation ID : 3cc5d44-4b69-4224-ab28-b5e9f140c6bf

Below the deployment details, there are sections for "Deployment details" and "Next steps". A "Go to resource" button is available. There are also links for "Give feedback" and "Tell us about your experience with deployment".

On the right side, there are several promotional cards:

- 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 >](#)

At the bottom, the taskbar shows the Windows Start button, a search bar, and icons for various applications like File Explorer, Edge, and Settings. The system tray shows the date and time (10:48 AM, 6/10/2025), battery level (66%), and network status (ENG IN).

Microsoft Sentinel Home Lab

4. Deploying the Windows Virtual Machine (Honeypot)

The core of the honeypot lab is a Windows 10 VM deployed to attract unauthorized access attempts:

This screenshot shows the Microsoft Azure portal's Compute infrastructure - Virtual machines page. The left sidebar is collapsed, and the main area displays a message: "No virtual machines to display". Below this, there is a note: "Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image." A prominent blue "Create" button is centered. At the bottom, there are links to "Learn more about Windows virtual machines" and "Learn more about Linux virtual machines". The top navigation bar includes the Azure logo, account information (phanivit2024@gmail.com), and a search bar.

This screenshot shows the Microsoft Azure portal's Select a VM size - Microsoft A2 page. The search bar at the top contains "D2s". The main content area lists various VM sizes, grouped by availability zone. The table includes columns for VM Size, Type, vCPUs, RAM (GiB), Data disks, Max IOPS, Local storage (GiB), Premium disk, and Cost/month. Some rows are marked with "Request quota". A note at the bottom states: "Prices presented are estimates in USD that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. View Azure pricing calculator." The bottom of the screen shows the Windows taskbar with various pinned icons.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The top navigation bar includes tabs for 'Create Your Azure Free Account', 'Create a virtual machine - Mic...', and 'Verify your email address - ph...'. The main title is 'Create a virtual machine'.

Zone options: The 'Self-selected zone' option is selected, with a note: 'Choose up to 3 availability zones, one VM per zone'. The 'Azure-selected zone (Preview)' option is also available.

Availability zone: 'Zone 1' is selected, with a note: 'You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)'.

Security type: 'Trusted launch virtual machines' is selected, with a link to 'Configure security features'.

Image: 'Windows 11 Pro, version 24H2 - x64 Gen2' is selected, with links to 'See all images' and 'Configure VM generation'.

VM architecture: 'x64' is selected, with a note: 'Arm64 is not supported with the selected image.'

Run with Azure Spot discount: An unchecked checkbox.

Feedback: A 'Give feedback' button is located at the bottom right of the page.

Bottom Taskbar: Shows the Windows taskbar with various pinned icons like File Explorer, Edge, and Settings. The system tray indicates the date and time as '6/10/2025'.

This screenshot shows the continuation of the 'Create a virtual machine' wizard. The title is 'Create a virtual machine'.

VM architecture: 'x64' is selected, with a note: 'Arm64 is not supported with the selected image.'

Run with Azure Spot discount: An unchecked checkbox.

Size: 'Standard_D2ads_v6 - 2 vcpus, 8 GiB memory (\$83.22/month)' is selected, with a link to 'See all sizes'.

Storage: A note states: 'The size you've selected is supported by higher storage performance with NVMe enabled. [Learn more](#)'.

Enable Hibernation: An unchecked checkbox.

Administrator account: A note states: 'Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more](#)'.

Feedback: A 'Give feedback' button is located at the bottom right of the page.

Bottom Taskbar: Shows the Windows taskbar with various pinned icons like File Explorer, Edge, and Settings. The system tray indicates the date and time as '6/10/2025'.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The title bar includes tabs for 'Create Your Azure Free Account', 'Create a virtual machine - Mic...', and 'Verify your email address - ph...'. The main navigation bar has 'Microsoft Azure' and 'Upgrade' options, along with a search bar and various icons.

The current page is titled 'Create a virtual machine' with a sub-section 'Inbound port rules'. It shows fields for 'Username' (labuser), 'Password', and 'Confirm password'. Under 'Inbound port rules', it says '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.' A radio button is selected for 'Allow selected ports', and a dropdown menu shows 'RDP (3389)'. A warning message states: '⚠️ 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.'

At the bottom, there are navigation buttons: '< Previous', 'Next : Disks >', and 'Review + create'. The status bar at the bottom right shows weather (70°F, Mostly cloudy), battery level (ENG IN), time (3:38 PM, 6/10/2025), and signal strength.

This screenshot shows the continuation of the 'Create a virtual machine' wizard. The title bar and top navigation are identical. The current step is 'OS disk'. It includes fields for 'OS disk size' (Image default (127 GiB)), 'OS disk type' (Premium SSD (locally-redundant storage)), and 'Delete with VM' (checkbox checked). Other options like 'Key management' (Platform-managed key) and 'Enable Ultra Disk compatibility' (checkbox unchecked) are also present.

Below this, the 'Data disks for CORP-NET-EAST-1' section is shown, with a note about adding additional data disks. There is a table header for 'LUN', 'Name', 'Size (GiB)', 'Disk type', 'Host caching', and 'Delete with VM'. Buttons for 'Create and attach a new disk' and 'Attach an existing disk' are available.

At the bottom, there is an 'Advanced' section with a dropdown arrow, and navigation buttons: '< Previous', 'Next : Networking >', and 'Review + create'. The status bar at the bottom right shows weather (70°F, Mostly cloudy), battery level (ENG IN), time (3:39 PM, 6/10/2025), and signal strength.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The title bar includes tabs for 'Create Your Azure Free Account', 'Create a virtual machine - Mic...', and 'Verify your email address - ph...'. The main header says 'Microsoft Azure' with an 'Upgrade' button and a search bar. The user is on the 'Networking' tab of the 'Create a virtual machine' wizard. The 'Virtual network' dropdown is set to 'Vnet-soc-lab'. The 'Subnet' dropdown is set to 'default (10.0.0.0/24)'. The 'Public IP' dropdown is set to '(new) CORP-NET-EAST-1-ip'. Under 'NIC network security group', 'Basic' is selected. Under 'Public inbound ports', 'None' is selected. At the bottom, there are buttons for '< Previous', 'Next: Management >', and 'Review + create'.

This screenshot continues the 'Create a virtual machine' wizard. The user has moved to the 'Management' tab. Under 'Select inbound ports', 'Allow selected ports' is selected, and 'RDP (3389)' is chosen. A warning message states: '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.' Under 'Delete public IP and NIC when VM is deleted', the checkbox is checked. Under 'Enable accelerated networking', the checkbox is checked. In the 'Load balancing' section, it says 'You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more'. Under 'Load balancing options', 'None' is selected. At the bottom, there are buttons for '< Previous', 'Next: Management >', and 'Review + create'.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The title bar includes tabs for 'Create Your Azure Free Account', 'Create a virtual machine - Mic...', and 'Verify your email address - ph...'. The main navigation bar has 'Microsoft Azure' and 'Upgrade' buttons, along with a search bar and various icons.

The page title is 'Create a virtual machine' with a sub-section 'Monitoring'. Below the title, there are three buttons: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. A horizontal navigation bar below these buttons includes 'Basics', 'Disks', 'Networking', 'Management', 'Monitoring' (which is underlined), 'Advanced', 'Tags', and 'Review + create'.

The main content area is titled 'Configure monitoring options for your VM.' It contains sections for 'Alerts' (with a checkbox for 'Enable recommended alert rules'), 'Diagnostics' (with options for 'Boot diagnostics' and 'Enable with managed storage account (recommended)', 'Enable with custom storage account', and 'Disable' (selected)), and 'Health' (with a checkbox for 'Enable application health monitoring').

At the bottom of the page are buttons for '< Previous', 'Next: Advanced >', and 'Review + create'. The status bar at the bottom of the browser window shows the date and time as '6/10/2025 3:42 PM'.

This screenshot shows the 'Review + create' step of the virtual machine creation wizard. The title bar and navigation bar are identical to the previous screenshot.

The main content area displays a green banner with a checkmark icon and the text 'Validation passed'. Below this, there are three buttons: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. The horizontal navigation bar remains the same.

The 'Price' section shows '1 X Standard D2s v3 by Microsoft' and 'Subscription credits apply'. It also lists '0.0960 USD/hr' and 'Pricing for other VM sizes'. A link to 'Terms of use | Privacy policy' is provided.

The 'TERMS' section contains a detailed legal notice about agreeing to terms and privacy statements, authorizing Microsoft to bill the current payment method, and sharing contact, usage, and transactional information with providers of the offering(s).

A warning message in a yellow box states: '⚠ You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.'

At the bottom are buttons for '< Previous', 'Next >', and 'Create'. The status bar at the bottom of the browser window shows the date and time as '6/10/2025 4:18 PM'.

Microsoft Sentinel Home Lab

Validation passed

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

Subscription	Azure subscription 1
Resource group	RG-SOC-Lab
Virtual machine name	CORP-NET-EAST-1
Region	East US 2
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	2
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows 10 Pro, version 22H2 - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No

< Previous | Next > | Create | Download a template for automation | Give feedback

Validation passed

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

Configuration

Enable Hibernation	No
Username	labuser
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Client
Azure Spot	No

Disk

OS disk size	Image default
OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	Vnet-soc-lab
Subnet	default (10.0.0.0/24)

< Previous | Next > | Create | Download a template for automation | Give feedback

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Azure portal with the URL portal.azure.com/#create/Microsoft.VirtualMachine-ARM. The page title is "Create a virtual machine". A green validation bar at the top says "Validation passed". Below it are three help buttons: "Help me create a low cost VM", "Help me create a VM optimized for high availability", and "Help me choose the right VM size for my workload".

Networking

Virtual network	Vnet-soc-lab
Subnet	default (10.0.0.0/24)
Public IP	(new) CORP-NET-EAST-1-ip
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled

Management

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Site Recovery	Disabled
Enable periodic assessment	Off

Buttons at the bottom: < Previous, Next >, Create, Download a template for automation, Give feedback.

The screenshot shows the Microsoft Azure portal with the URL portal.azure.com/#create/Microsoft.VirtualMachine-ARM. The page title is "Create a virtual machine". A green validation bar at the top says "Validation passed". Below it are three help buttons: "Help me create a low cost VM", "Help me create a VM optimized for high availability", and "Help me choose the right VM size for my workload".

Management

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Site Recovery	Disabled
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Monitoring

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

Buttons at the bottom: < Previous, Next >, Create, Download a template for automation, Give feedback.

Microsoft Sentinel Home Lab

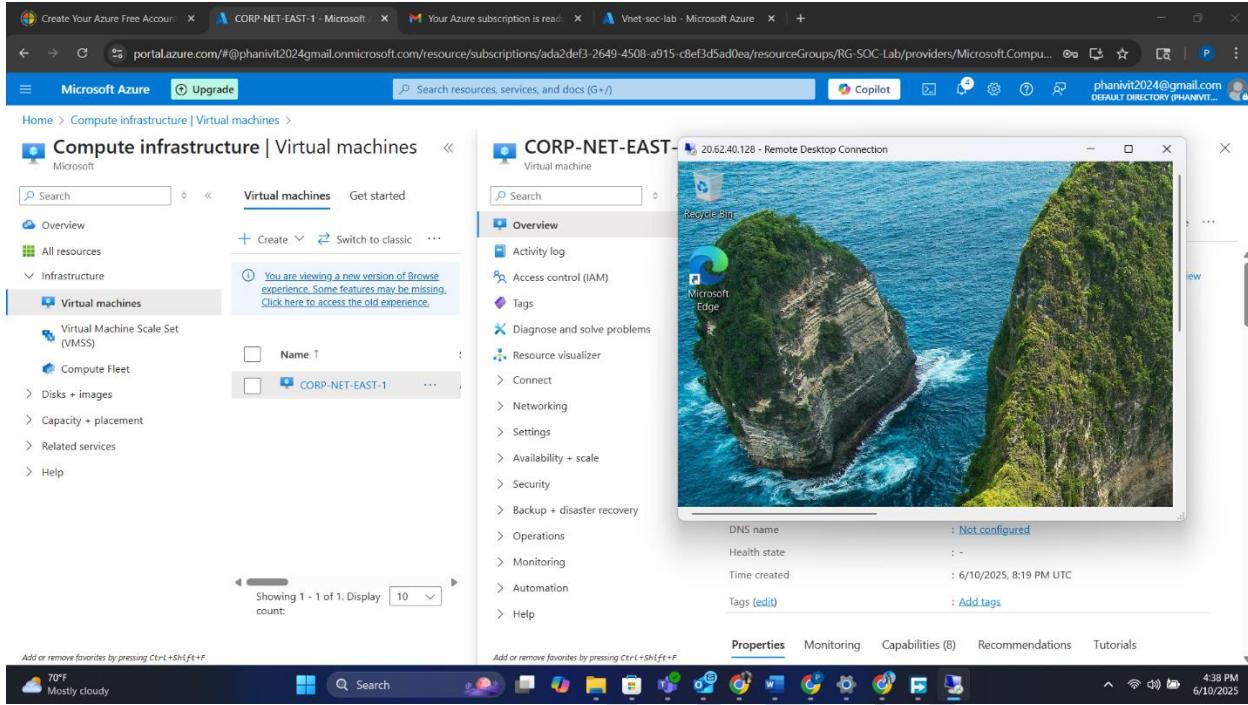
The screenshot shows the Microsoft Azure portal interface. A deployment named "CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20250610161344" has been successfully completed. The deployment details include a subscription from "Azure subscription 1", a start time of 6/10/2025, 4:19:45 PM, and a correlation ID of 6003704a-b75a-45f6-8b9d-a8f4cc493e7d. The resource group is "RG-SOC-Lab". On the right side of the main content area, there are several promotional cards: "Deployment succeeded" (with a green checkmark), "Cost Management" (with a dollar sign icon), "Microsoft Defender for Cloud" (with a lock icon), "Free Microsoft tutorials" (with a book icon), and "Work with an expert" (with a person icon). The bottom of the screen shows a Windows taskbar with various pinned icons.

The screenshot shows the Microsoft Azure portal interface, specifically the "RG-SOC-Lab" resource group overview. The left sidebar lists resource groups: "Name 1", "NetworkWatcherRG", and "RG-SOC-Lab". The main content area displays the "Essentials" section for the "RG-SOC-Lab" group. It includes tabs for "Activity log", "Access control (IAM)", "Tags", "Resource visualizer", "Events", "Settings", "Cost Management", "Monitoring", "Automation", and "Help". The "Resources" tab is selected, showing a table of resources. The table has columns for "Name", "Type", and "Location". The resources listed are:

Name	Type	Location
CORP-NET-EAST-1	Virtual machine	East US 2
CORP-NET-EAST-1-ip	Public IP address	East US 2
CORP-NET-EAST-1-nsg	Network security group	East US 2
corp-net-east-1983_z2	Network Interface	East US 2
CORP-NET-EAST-1_OsDisk_1_40ced9ec7fa141e58973f29847ab349d	Disk	East US 2
Vnet-soc-lab	Virtual network	East US 2

At the bottom of the page, there is a "Give feedback" link. The bottom of the screen shows a Windows taskbar with various pinned icons.

Microsoft Sentinel Home Lab



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\karna> ping 20.62.40.128

Pinging 20.62.40.128 with 32 bytes of data:
Reply from 20.62.40.128: bytes=32 time=57ms TTL=109
Reply from 20.62.40.128: bytes=32 time=69ms TTL=109
Reply from 20.62.40.128: bytes=32 time=52ms TTL=109
Reply from 20.62.40.128: bytes=32 time=50ms TTL=109

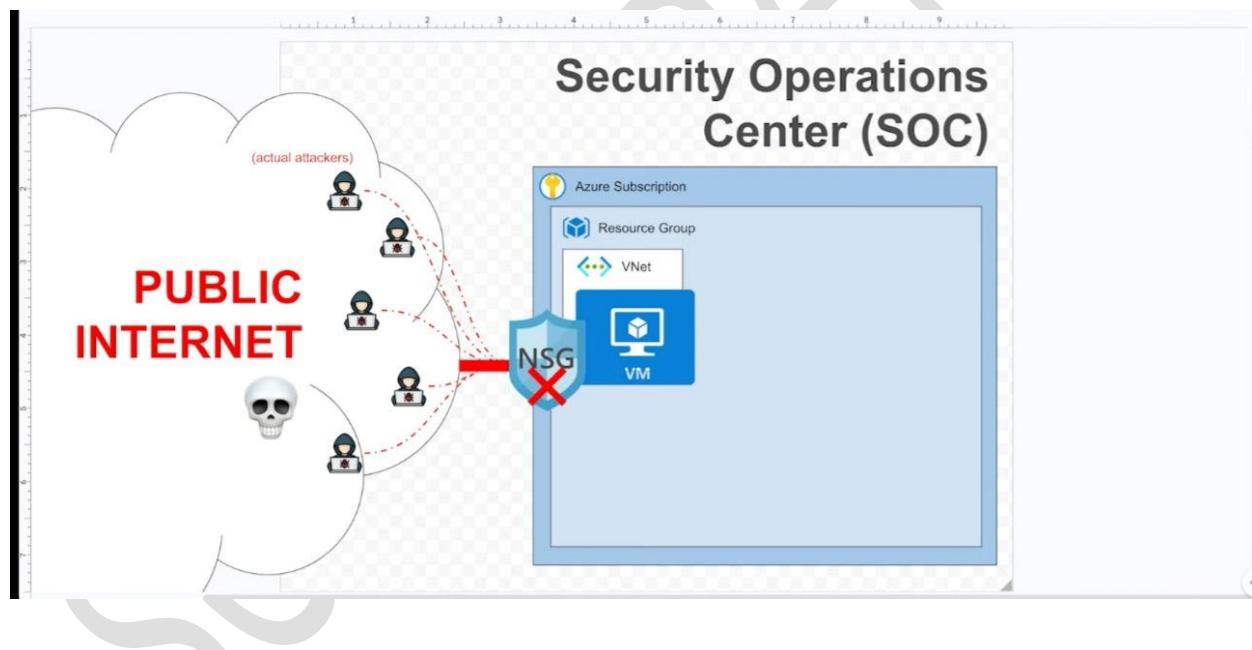
Ping statistics for 20.62.40.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 69ms, Average = 57ms
PS C:\Users\karna>
```

5. Configuring Network Security Group (NSG)

To allow attacker interaction:

- The default RDP-only inbound rule was deleted.
- A new inbound rule was added:
 - Source: Any
 - Destination: Any
 - Protocol: Any
 - Port Range: *
 - Action: Allow

This effectively opens the VM to all inbound traffic, simulating an exposed public system.



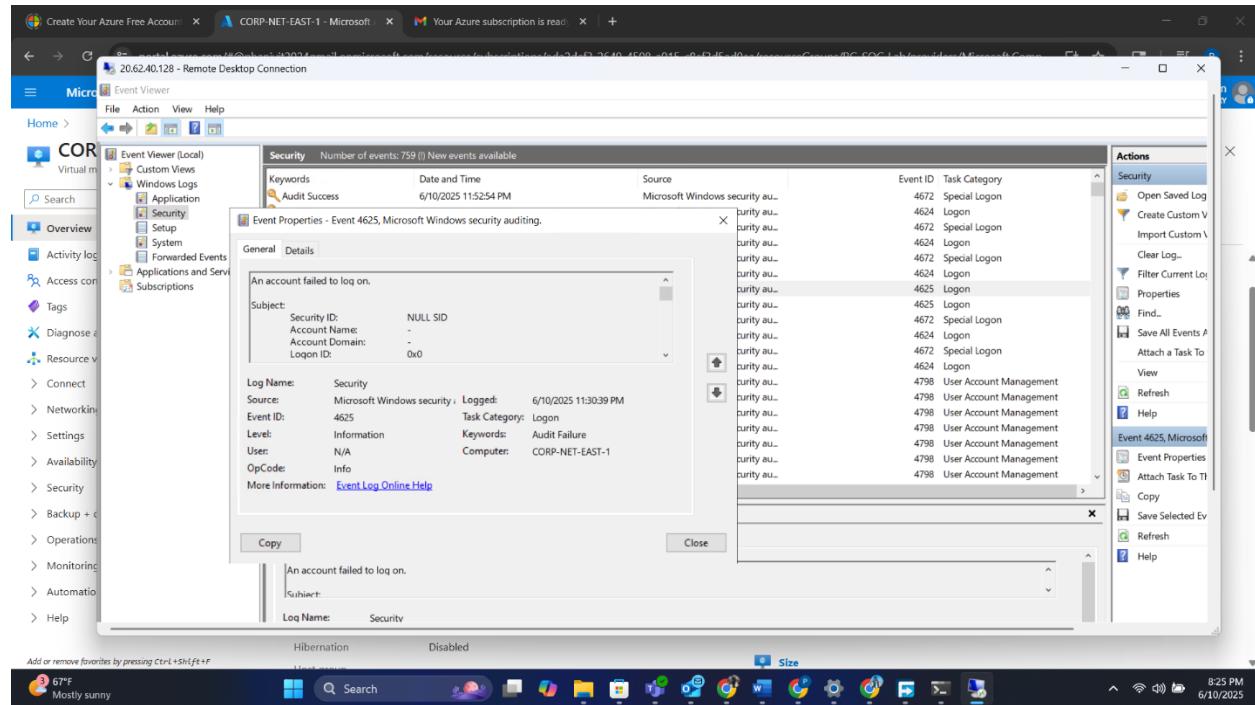
6. Disabling Windows Defender Firewall

To ensure all incoming traffic is logged:

- Remote Desktop Protocol (RDP) was used to log into the VM.
- Windows Firewall was accessed via wf.msc.
- The firewall was turned off for Domain, Private, and Public profiles.

Microsoft Sentinel Home Lab

This further simulates a vulnerable system and guarantees event logging.



7. Generating Simulated Attack Logs

To simulate brute-force attempts:

- Several failed login attempts were made using fake usernames like employee.
- These actions triggered Windows Security Event ID 4625 (failed logon attempt).

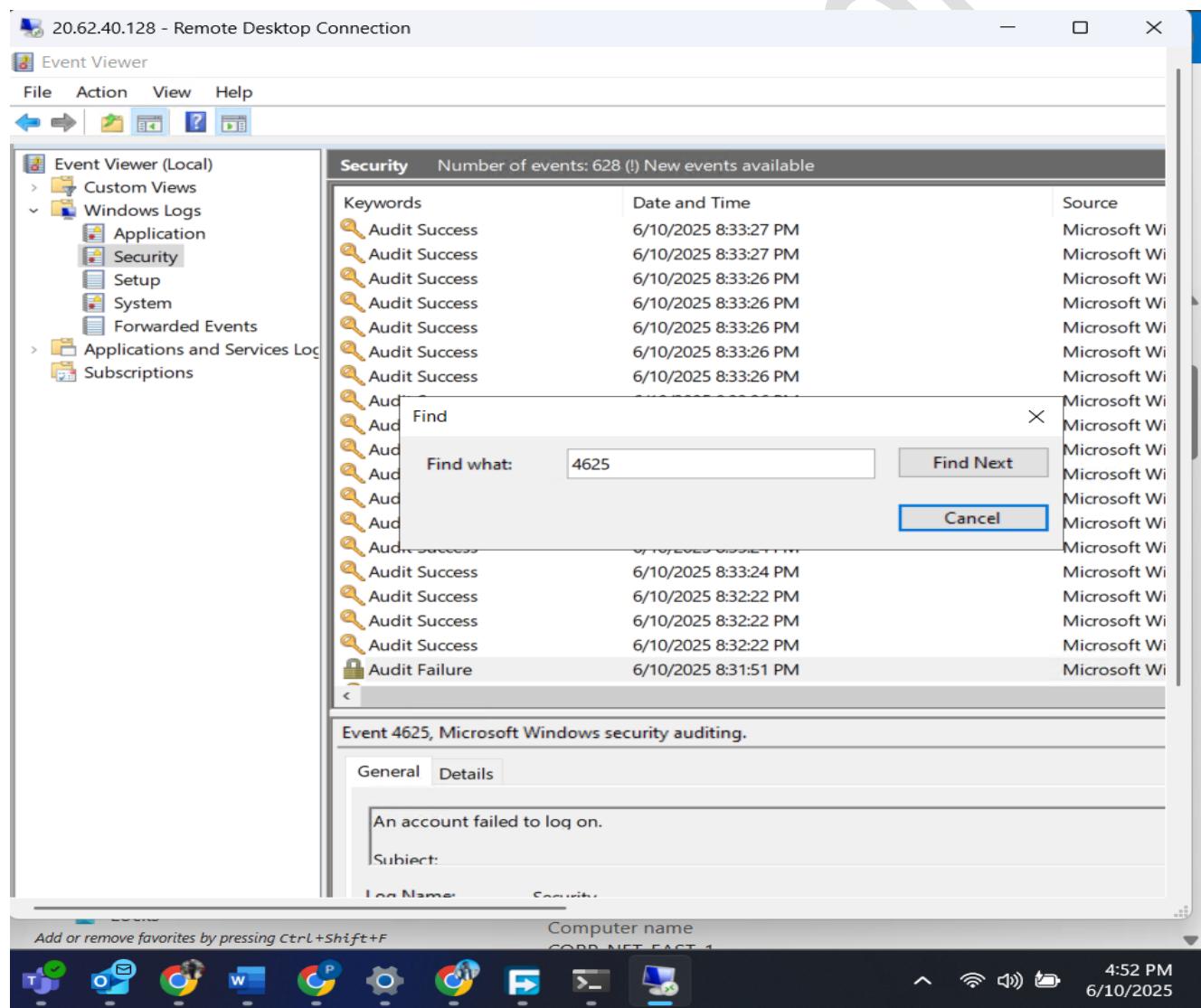
A screenshot of a web browser showing the Azure Log Analytics workspace creation page. The URL is portal.azure.com/#browse/Microsoft.OperationalInsights%2Fworkspaces. The page displays a message: "No log analytics workspaces to display". It includes a note about leveraging unique environments for log data from Azure Monitor and other Azure services. There is a prominent blue "+ Create" button. At the bottom, there is a search bar, a toolbar with various icons, and a status bar showing the date and time.

8. Verifying Logs Using Event Viewer

Within the VM:

- Event Viewer was opened.
- Navigated to: Windows Logs > Security
- Filtered logs by Event ID 4625.

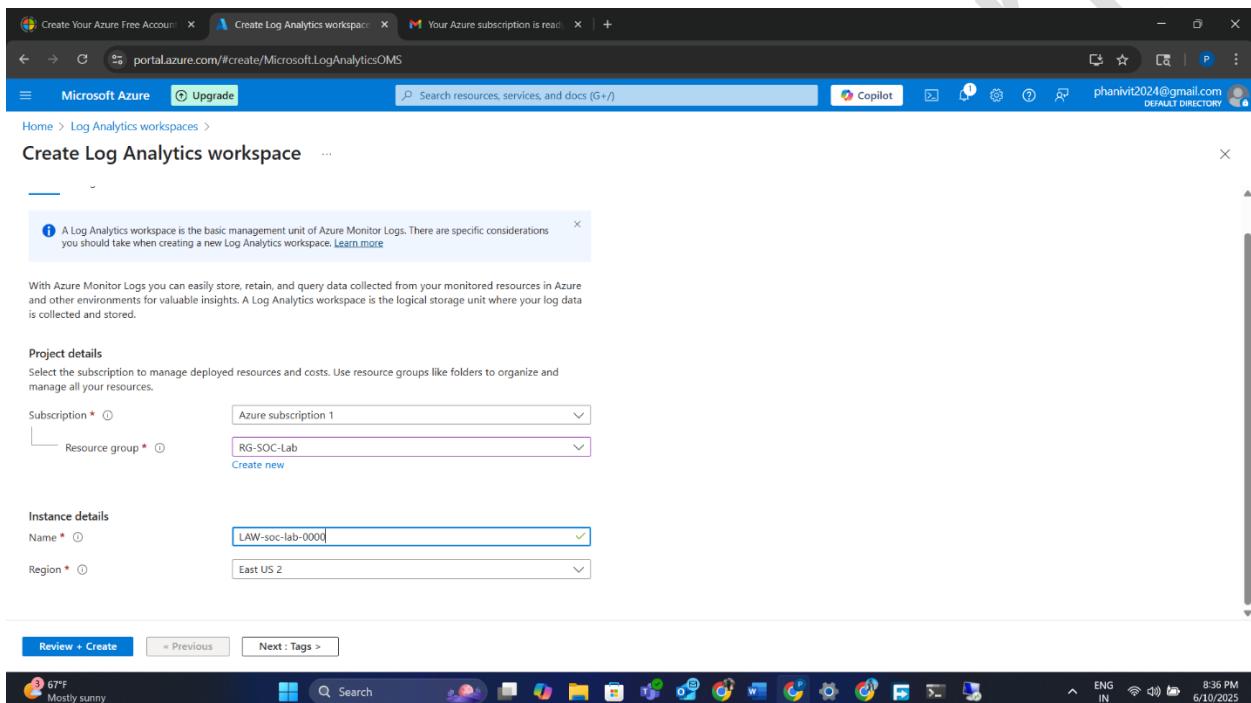
Details such as the attempted username, source IP, and failure reasons were verified.



9. Creating Log Analytics Workspace (LAW)

A Log Analytics Workspace acts as a centralized repository:

- Created within **rg-socklab**
- Named **law-socklab-east2**
- Used to ingest logs forwarded from Azure resources, including VMs.



Microsoft Sentinel Home Lab

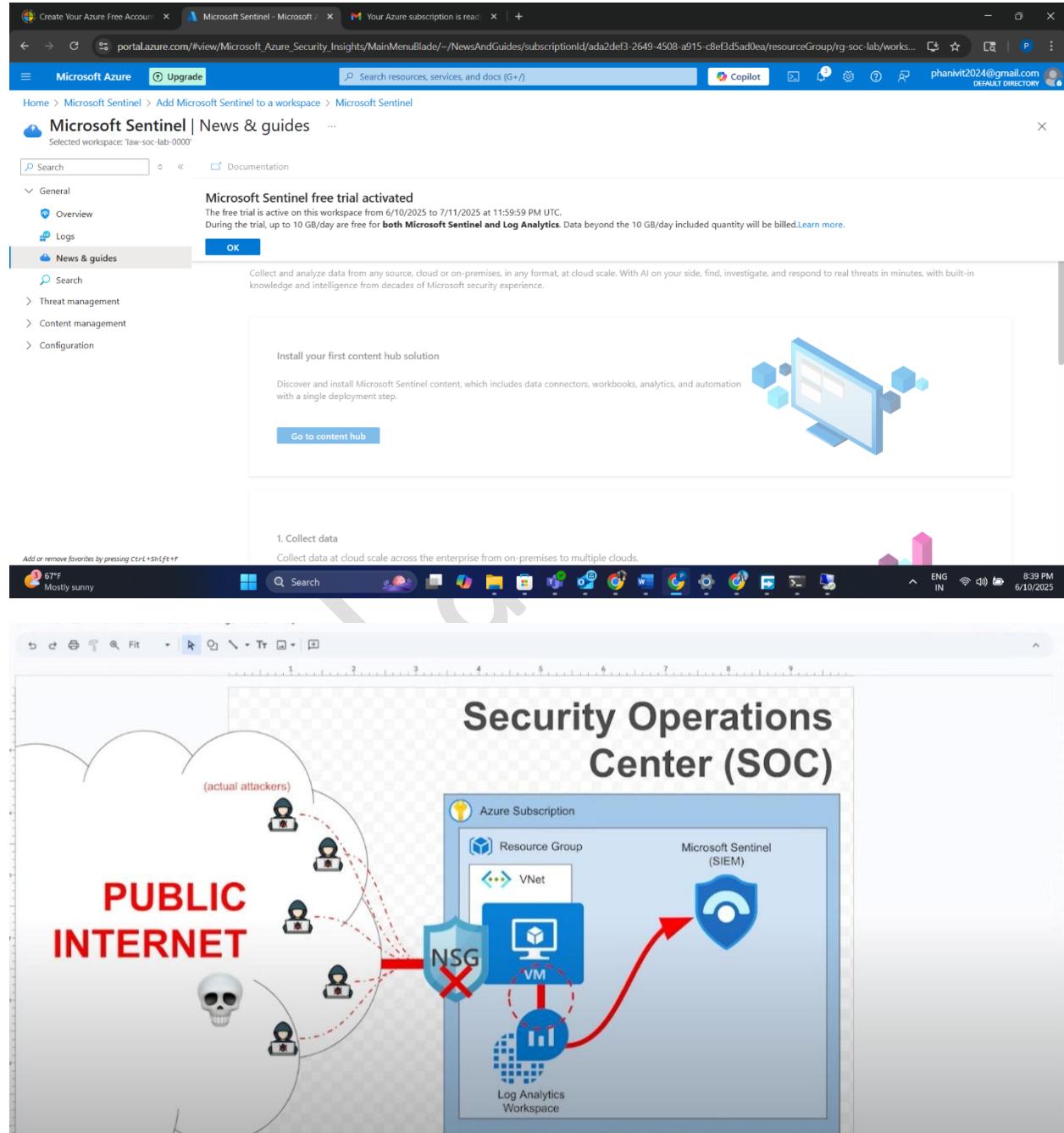
The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'Create Your Azure Free Account', 'Create Log Analytics workspace', and 'Your Azure subscription is ready'. The main title is 'Create Log Analytics workspace'. A green validation message 'Validation passed' is displayed. The 'Review + Create' tab is selected. The 'Log Analytics workspace' section shows details: Subscription (Azure subscription 1), Resource group (RG-SOC-Lab), Name (LAW-soc-lab-0000), and Region (East US 2). The 'Pricing' section indicates a 'Pay-as-you-go (Per GB 2018)' tier. Below this, a note states that the cost depends on data volume and retention, with regional pricing details available on the Azure Monitor pricing page. A link to learn more about Log Analytics pricing models is provided. The 'Tags' section is present but empty. At the bottom, there are 'Create', 'Previous', and 'Download a template for automation' buttons.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'Create Your Azure Free Account', 'Microsoft.LogAnalyticsOMS - M', and 'Your Azure subscription is ready'. The main title is 'Microsoft.LogAnalyticsOMS | Overview'. A green success message 'Deployment succeeded' is displayed, stating that deployment to resource group 'RG-SOC-Lab' was successful. The 'Overview' section shows deployment details: Deployment name (Microsoft.LogAnalyticsOMS), Subscription (Azure subscription 1), and Resource group (RG-SOC-Lab). It also shows deployment status: Start time (6/10/2025, 8:37:14 PM) and Correlation ID (25a4408f-779c-4f1a-89c3-5dcc3d9f286). The 'Deployment details' section is expanded, showing deployment steps: 'Inputs', 'Outputs', and 'Template'. The 'Next steps' section contains a 'Go to resource' button. On the right side, there are links for 'Cost management', 'Microsoft Defender for Cloud', 'Free Microsoft tutorials', and 'Work with an expert'. The bottom of the screen shows a taskbar with various pinned icons and system status indicators.

10. Deploying Microsoft Sentinel Instance

Microsoft Sentinel, a cloud-native SIEM/SOAR platform, was added to the LAW:

- The LAW created earlier was selected.
- Sentinel connects to LAW to run detection queries, dashboards, and incidents.



11. Enabling Log Forwarding with Azure Monitoring Agent (AMA)

The screenshot shows the Microsoft Sentinel Content hub interface. On the left, there's a sidebar with options like 'Create', 'Logs', 'Search', 'Threat management', and 'Content management'. Under 'Content management', 'Content hub' is selected. The main area displays a search bar with 'security events' and a results table. The table has columns for 'Content title', 'Status', and 'Content source'. One row is expanded to show 'Windows Security Events' with status 'Not installed'. To the right, there's a sidebar for 'Windows Security Events' with sections for 'Provider', 'Support', 'Category', and 'Pricing'. At the bottom, there's a toolbar with icons for 'Install' and 'View details'.

The screenshot shows the 'Windows Security Events via AMA' configuration page. It starts with a 'Prerequisites' section listing 'Workspace data sources' and 'Data connectors'. Below that is a 'Configuration' section with a 'Data collection rule' table. The table has columns for 'Rule name', 'Created by', and 'Filter name'. A note says 'Security Events logs are collected only from Windows agents.' At the bottom, there's a button '+Create data collection rule'.

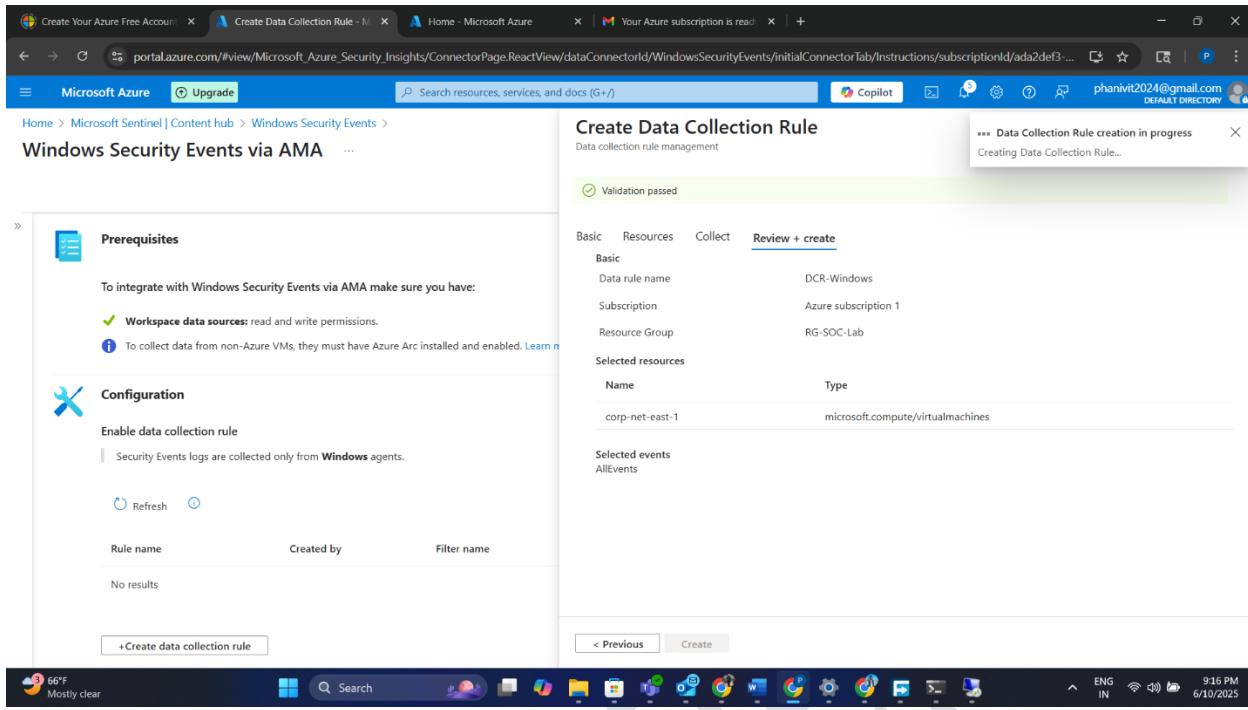
Microsoft Sentinel Home Lab

To connect VM logs to LAW:

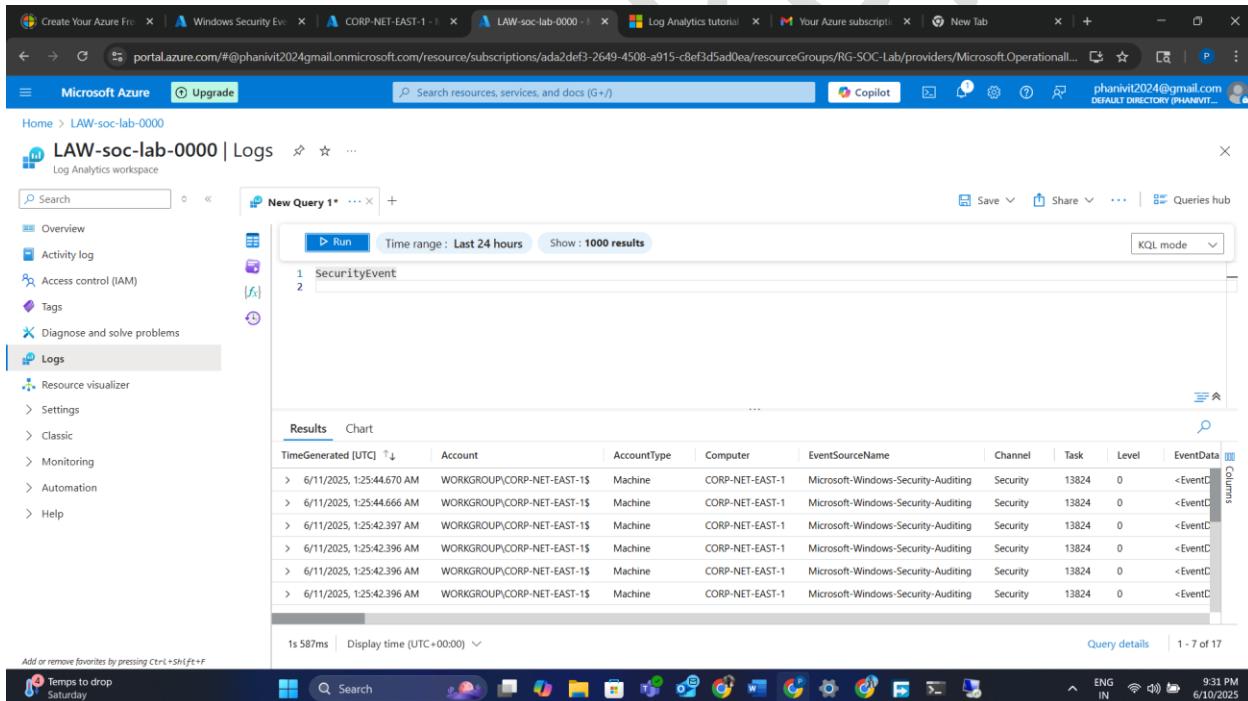
- Windows Security Events Data Connector (Windows Security Events via AMA) was installed.

The screenshot shows two side-by-side windows of the Microsoft Azure portal. Both windows are titled 'Create Data Collection Rule' under 'Data collection rule management'.
The top window shows the 'Basic' tab selected. It has fields for 'Rule name' (set to 'DCR-Windows'), 'Subscription' (set to 'Azure subscription 1'), and 'Resource group' (set to 'RG-SOC-Lab').
The bottom window shows the 'Resources' tab selected. It displays a table with columns 'Subscriptions', 'Resource Groups', 'Resource Types', and 'Locations'. Under 'Subscriptions', 'Selected: All' is chosen. Under 'Resource Groups', 'Selected: All' is chosen. Under 'Resource Types', 'Selected: All' is chosen. Under 'Locations', 'Selected: All' is chosen. A note at the top of this section states: '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.'
Both windows have a sidebar on the left with sections for 'Prerequisites' and 'Configuration'. The 'Prerequisites' section lists requirements for integrating with Windows Security Events via AMA, including workspace data sources and Azure Arc. The 'Configuration' section shows a table for enabling data collection rules, with one row listed: 'Security Events logs are collected only from Windows agents'.
At the bottom of both windows, there are navigation buttons: '< Previous' and 'Next: Collect >' on the left, and '< Previous' and 'Next: Resources >' on the right. The status bar at the bottom of the screen shows system information: 66°F, Mostly clear, ENG IN, 9:15 PM, 6/10/2025.

Microsoft Sentinel Home Lab



The screenshot shows the Microsoft Azure portal interface. A progress bar at the top right indicates "Data Collection Rule creation in progress" and "Creating Data Collection Rule...". The main area displays the "Create Data Collection Rule" wizard, specifically the "Review + create" step. The rule is named "DCR-Windows", associated with "Subscription: Azure subscription 1" and "Resource Group: RG-SOC-Lab". Under "Selected resources", there is one entry: "Name: corp-net-east-1" and "Type: microsoft.compute/virtualmachines". Below this, under "Selected events", is "AllEvents". On the left sidebar, sections like "Prerequisites" and "Configuration" are visible, along with a table showing no results for data collection rules.



The screenshot shows the Microsoft Log Analytics workspace for the "LAW-soc-lab-0000" workspace. A search bar at the top has the query "SecurityEvent". The results table shows 1000 results from the last 24 hours. The columns include TimeGenerated [UTC], Account, AccountType, Computer, EventSourceName, Channel, Task, Level, and EventData. The table lists multiple entries for "SecurityEvent" from "CORP-NET-EAST-1\$". At the bottom, it says "1s 587ms | Display time (UTC+00:00)" and "Query details | 1 - 7 of 17".

Microsoft Sentinel Home Lab

- A Data Collection Rule (**DCR**) was created to:
 - Link the VM to the LAW
 - Forward all security events

Confirmation of success was verified in the VM's Extensions tab.

The screenshot shows the Microsoft Azure Log Analytics workspace interface. On the left, there is a navigation pane with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Logs. The Logs section is selected. In the center, a search bar and a 'New Query' button are at the top. Below that, a query editor shows the following KQL code:

```
1 SecurityEvent  
2 | where Account == "\\\Test"
```

The results pane displays a single event row:

TimeGenerated [UTC]	Account	AccountType	Computer
0	4625	NTLM	194.165.16.166
	4625 - An account failed to log on.		
	FailureReason		
	%2313		
	IpAddress		
	194.165.16.166		

At the bottom of the results pane, it says "3s 256ms | Display time (UTC+00:00) | Query details | 1 - of 2".

The screenshot shows the IPinfo.io website. The URL in the address bar is https://ipinfo.io/194.165.16.164. The main content area has tabs for Summary, Geolocation, Privacy, ASN, Company, and Abuse. The Summary tab is active. It shows the following information:

Hosted domains	0
Privacy	True

Below this, there is a section for IP Geolocation:

City	Vilnius
State	Vilnius
Country	Lithuania
Postal	01001
Local time	06:09 AM, Wednesday, June 11, 2025
Timezone	Europe/Vilnius
Coordinates	54.6892,25.2798

A map of Vilnius, Lithuania, is displayed with the coordinates 54.6892,25.2798 marked. The map includes labels for Avižieniai, Zujūnai, Turniškės, Galgiai, Igališkės, Rokantiškės, and Nemėžis.

At the bottom of the page, there is a section for IP Geolocation data with the text: "IP geolocation lookup is the identification of an IP address' geographic location in the real world." and a link to "IP Geolocation API >".

12. Confirming Log Ingestion via KQL Queries

In the LAW > Logs tab:

- Queried SecurityEvent table using KQL
- Verified presence of Event ID **4625**

Example query:

```
# SecurityEvent
```

```
| where EventID == 4625
```

```
| project TimeGenerated, Account, Computer, IPAddress #
```

Thousands of failed login attempts from global IPs appeared within minutes.

The screenshot shows the IPinfo.io interface. The URL in the browser bar is <https://ipinfo.io/194.165.16.164>. The main content area displays the following geolocation information:

Category	Value
City	Vilnius
State	Vilnius
Country	Lithuania
Postal	01001
Local time	06:09 AM, Wednesday, June 11, 2025
Timezone	Europe/Vilnius
Coordinates	54.6892, 25.2798

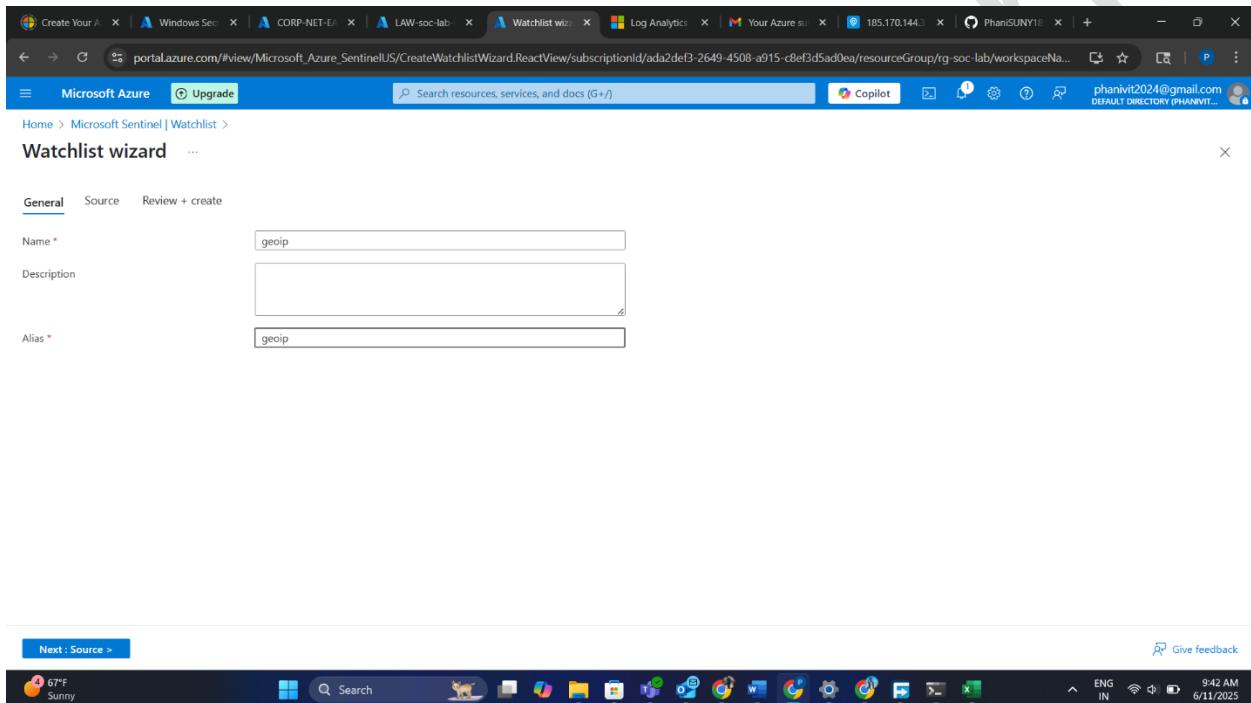
Below this, there is a map of Vilnius with the coordinates 54.6892, 25.2798 marked. The map shows various streets and neighborhoods. A green box highlights the coordinates with the text "54.6892, 25.2798".

On the left sidebar, there are navigation links for Summary, Geolocation, Privacy, ASN, Company, and Abuse. The "Summary" link is currently selected. At the top of the page, there are sections for Privacy (True), Anycast (False), and a sign-up button for free access.

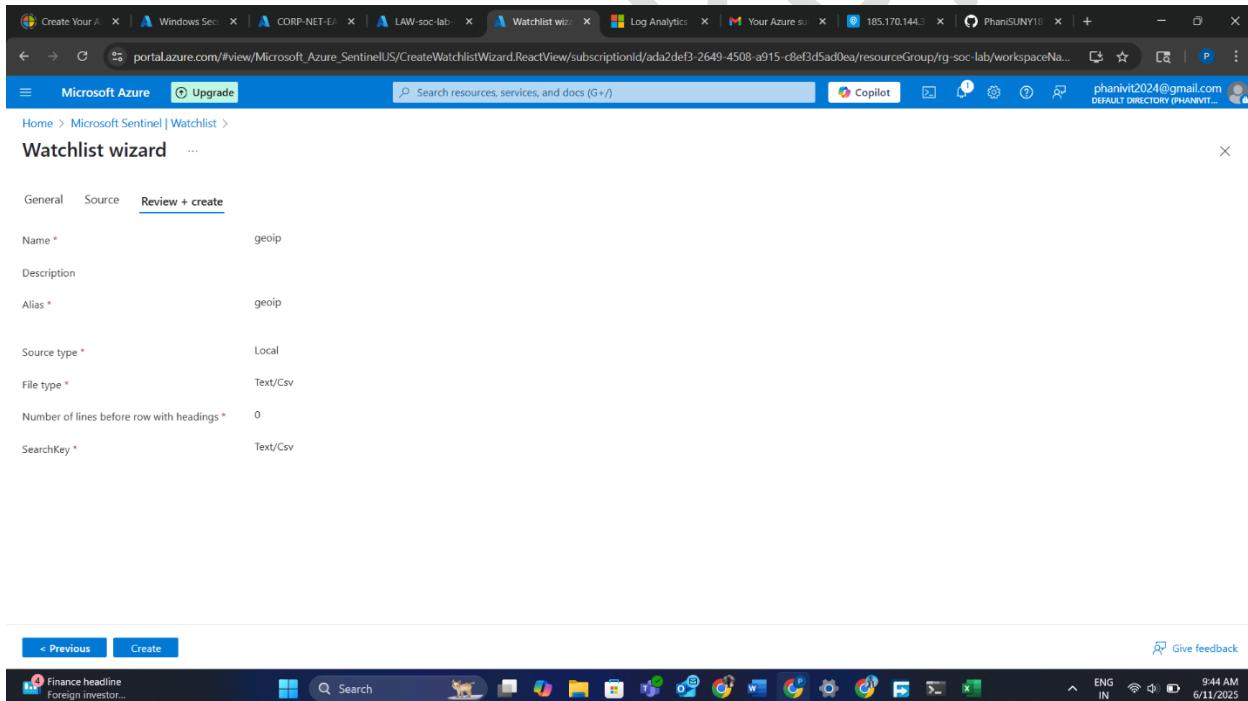
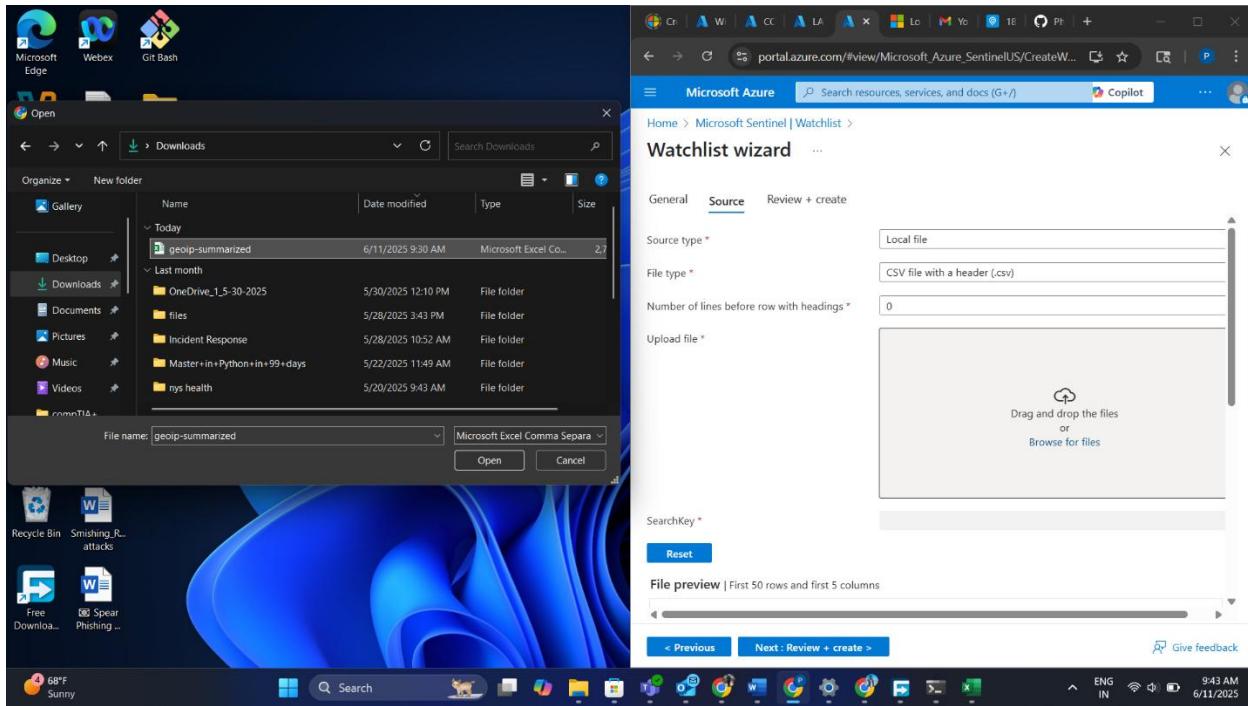
13. Uploading Geolocated Watchlist to Sentinel

To enrich IPs with location data:

- A CSV file (geoip-summarized.csv) was uploaded as a Watchlist in Sentinel
- Watchlist fields included: IP range, latitude, longitude, city, country
- Name and alias: Geolocated and geoip



Microsoft Sentinel Home Lab



Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Sentinel Watchlist creation interface. The user has created three watchlists: 'geoip', 'geoip', and 'geoip'. Each creation is accompanied by a success message: 'Successfully submitted watchlist [geoip]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.'

Watchlist Creation Log:

- Created watchlist [geoip]
- Successfully submitted watchlist [geoip]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.
- Created watchlist [geoip]
- Successfully submitted watchlist [geoip]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.
- Created watchlist [geoip]
- Successfully submitted watchlist [geoip]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.

14. Joining Security Logs with GeoIP Data

Using KQL, logs were joined with the Watchlist to extract attacker locations:

```
let geo = _GetWatchlist("geoip");
```

```
SecurityEvent
```

```
| where EventID == 4625
```

```
| lookup kind=leftouter geo on $left.IPAddress == $right.Network
```

```
| project TimeGenerated, Account, IPAddress, CityName, CountryName, Latitude,  
Longitude
```

The screenshot shows the Microsoft Azure Log Analytics interface. The browser address bar displays a URL related to Microsoft Operations Management Suite. The main window shows a 'Logs' blade for a workspace named 'LAW-soc-lab-0000'. A 'New Query' button is visible. The query editor contains the following KQL:

```
let geo = _GetWatchlist("geoip");
SecurityEvent
| where EventID == 4625
| lookup kind=leftouter geo on $left.IPAddress == $right.Network
| project TimeGenerated, Account, IPAddress, CityName, CountryName, Latitude, Longitude
```

The results table displays the following data:

	LastUpdatedTimeUTC [U... ↑]	_DTItemid	SearchKey	cityname	countryname	latitude	longitude	network
□	> 6/11/2025, 1:44:41.823 PM	771eeef8-ca50-40a0-bf05-8812de9fb895	178.34.0.0/16	Surgut	Russia	61.2431	73.4139	178.34.0.0/16
□	> 6/11/2025, 1:44:41.823 PM	db5376e6-37f5-4615-9143-71790b4ea09b	178.44.0.0/16	Korinos	Greece	40.3188	22.584	178.44.0.0/16
□	> 6/11/2025, 1:44:41.823 PM	a6ad75ba-f7b7-4bf7-93e9-e718b5ab3fe	178.47.0.0/16	Kuwait City	Kuwait	29.3645	47.9889	178.47.0.0/16
□	> 6/11/2025, 1:44:41.823 PM	abff7214-6817-4616-b4b2-656fd0484cb	178.48.0.0/16	Amsterdam	Netherlands	52.352	4.9392	178.48.0.0/16
□	> 6/11/2025, 1:44:41.823 PM	1b401210-37a5-4c51-9644-91853875f213	178.49.0.0/16	Morschen	Germany	51.05	9.6	178.49.0.0/16
□	> 6/11/2025, 1:44:41.823 PM	a8714ada-cafa-46ab-b340-021a18ae0f2c	178.68.0.0/16	Amsterdam	Netherlands	52.352	4.8384	178.68.0.0/16

Below the table, it says '7s 813ms | Display time (UTC+0:00)'. On the right, there are 'Query details' and '1 - 7 of 51000'.

Microsoft Sentinel Home Lab

The screenshot shows the Microsoft Sentinel Workbooks interface. At the top, there's a navigation bar with links for 'Create You', 'Windows', 'CORP-NET', 'LAW-soc...', 'Microsoft', 'Microsoft', 'Log Analy...', 'Your Azure', '185.170.14...', 'PhanvitSUN', and a plus sign. The main title is 'Microsoft Sentinel | Workbooks' with the subtitle 'Selected workspace: "law-soc-lab-0000"'. A search bar says 'Search resources, services, and docs (G+)'. On the left, a sidebar has a 'Create' button and a message about viewing a new version of the browser. It lists categories like General, Threat management, Incidents, Workbooks (selected), Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, Configuration, Workspace manager (Preview), Data connectors, Analytics, and Summary rules (Preview). Below the sidebar, it says 'Showing 1 - 1 of 1. Display count: auto'. The main area shows 'My workbooks' with 0 items, 'Templates' with 2 items, and 'Updates' with 0 items. It features a large 'Microsoft Sentinel Workbooks' section with a 'What is it?' summary, 'Learn more' links for workbooks and OOTB content, and a 'Getting started' section. To the right, there's a 'Featured workbooks' section with a 'Cloud Bag' icon and a message 'No workbook selected. Select workbook to view more details'. The bottom navigation bar includes icons for Home, Search, Refresh, Add Workbook, Guides & Feedback, and Copilot, along with system status indicators for ENG IN, 1110 AM, and 6/11/2025.

Welcome to your new workbook. This area will display text formatted as markdown.

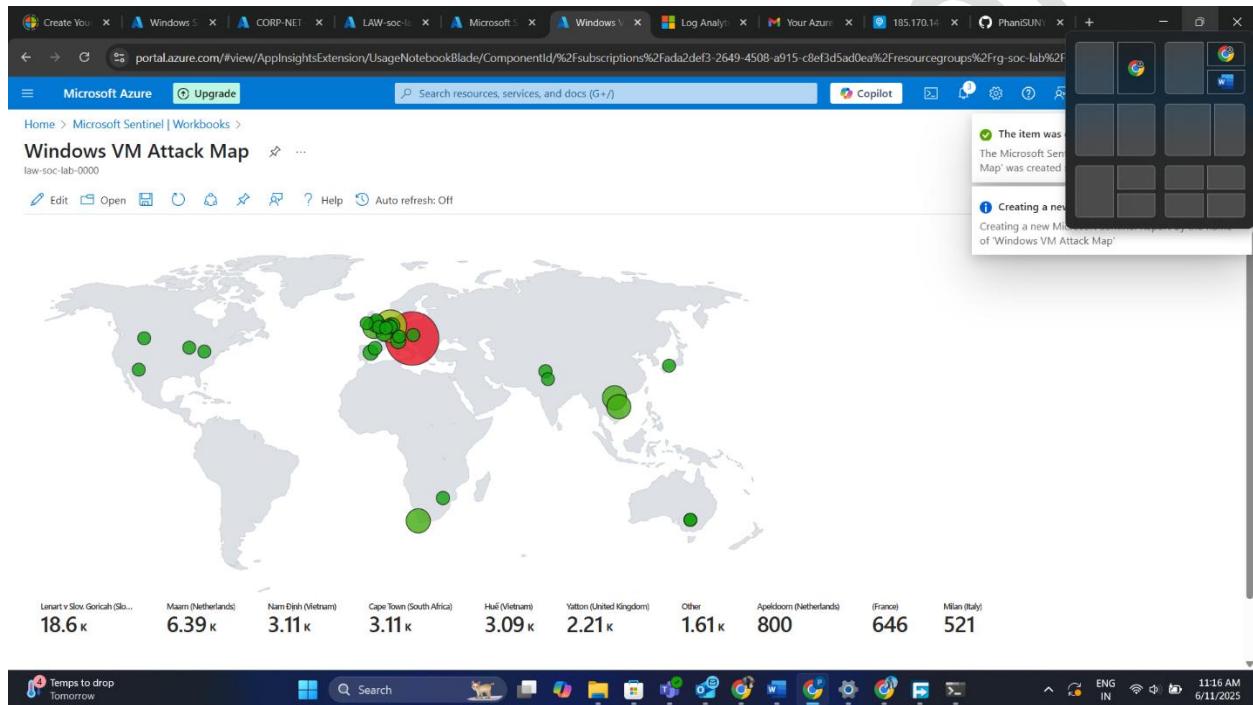
We've included a basic analytics query to get you started. Use the **Edit** button below each section to configure it or add more sections.

The screenshot shows the Microsoft Sentinel 'New workbook' page. At the top, there's a navigation bar with 'Microsoft Azure' and 'Upgrade' buttons, a search bar, and a Copilot icon. The main content area has a title 'New workbook' and a subtitle 'law-soc-lab-0000'. Below this is a toolbar with icons for Edit, Open, Refresh, Help, and Auto refresh: Off. The main body contains a heading 'New workbook' and a welcome message. Below the message is a chart with a blue bar labeled 'SecurityEvent' at 41.7k, a pink line labeled 'Heartbeat' at 829, and a green line labeled 'Usage' at 27. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

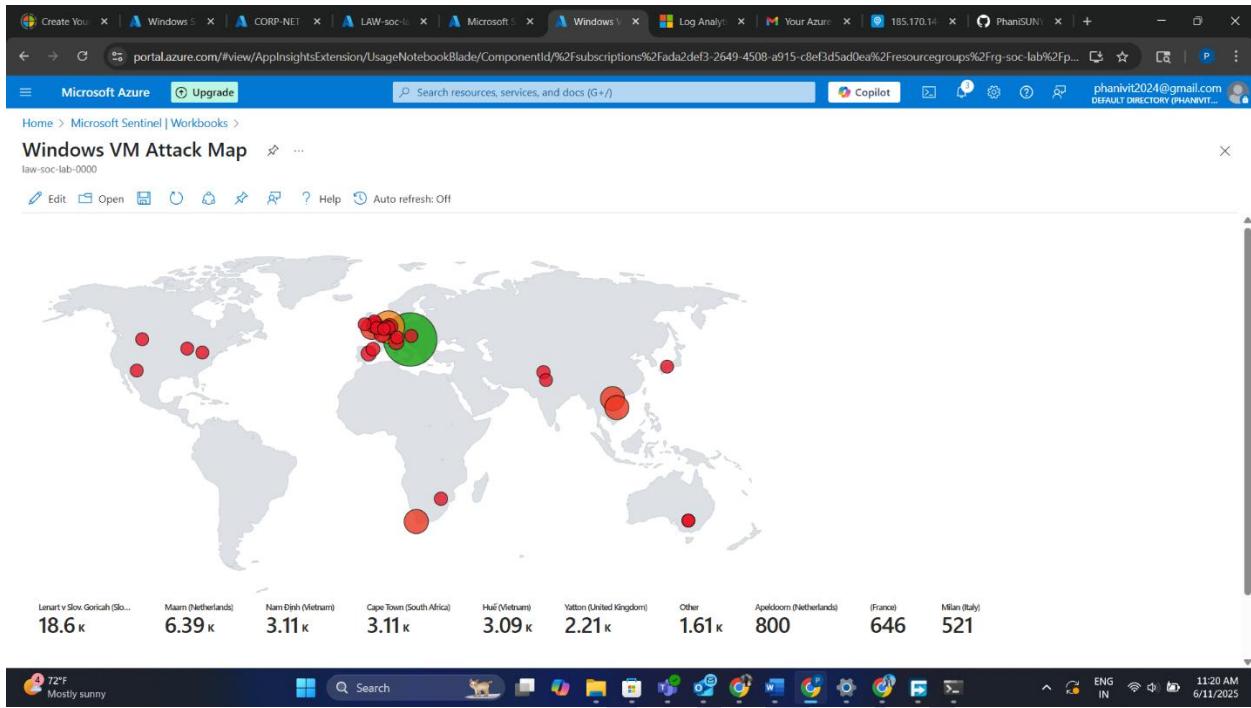
15. Visualizing Attacks on World Map (Attack Map Workbook)

A custom Sentinel Workbook was created:

- Visualized attacker locations using a heatmap
- JSON template from the lab was imported
- Map labeled by city + country
- Updated in real time as logs increased



Microsoft Sentinel Home Lab



Conclusion

This lab simulates how real-world systems are probed and attacked almost instantly when exposed online. It teaches:

- Cloud infrastructure setup
- Vulnerability simulation
- Log ingestion and enrichment
- Security analytics with KQL
- Building geographic visualizations

Completing this lab is a strong portfolio item for aspiring SOC analysts, threat hunters, and cybersecurity engineers.

