

Azure Home Lab Project: Building a Security Monitoring Environment

By Lucio Rodrigues

Introduction

This project demonstrates the end-to-end setup of a security monitoring environment in Microsoft Azure, designed to simulate real-world attack visibility and incident analysis.

By deploying a honeypot virtual machine, forwarding its logs to a central workspace, and integrating Azure Sentinel for threat detection and visualisation, I created a controlled environment to practice SIEM use cases and threat hunting techniques.

The following documentation provides a structured walkthrough of the setup process, including screenshots of each step. It is written to guide others through reproducing the lab while also showcasing the applied knowledge gained from the project.

Completed Project Overview

The completed lab environment provides a fully functional security monitoring pipeline within Azure. A honeypot virtual machine was deployed, exposed to the internet, and configured to forward security events into a centralised Log Analytics Workspace.

Azure Sentinel was then layered on top to enable correlation, enrichment with a custom geolocation watchlist, and visualisation of global attack patterns.

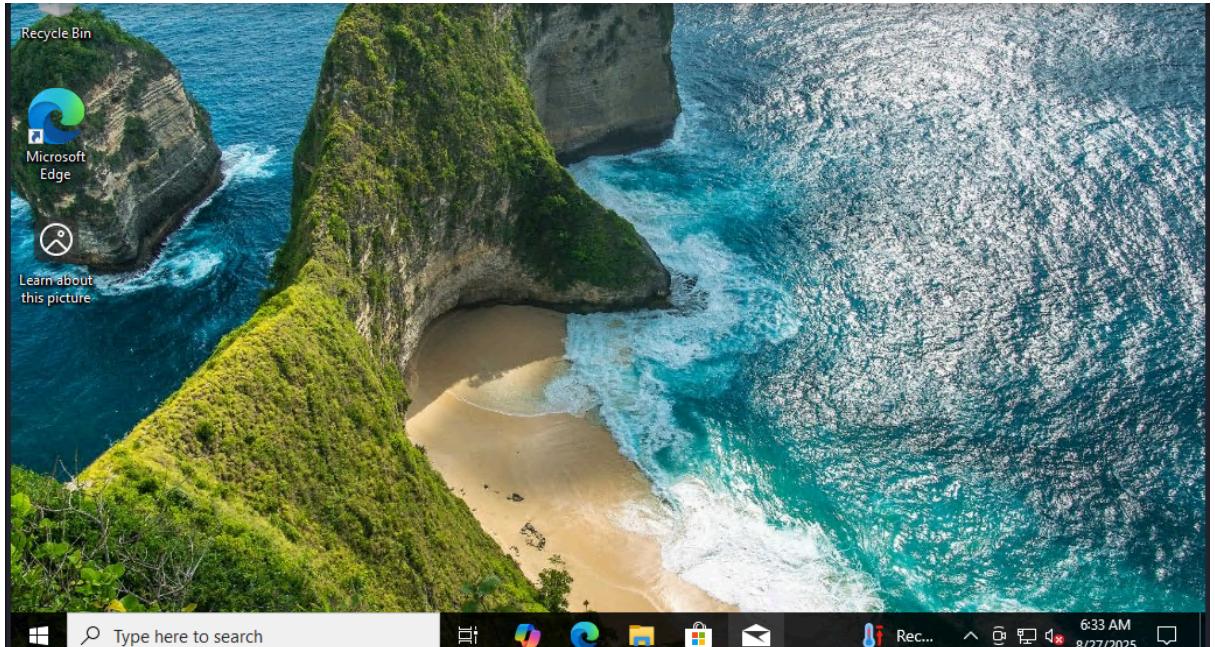
Figures below illustrate the completed setup:

- **Figure 1:** High-level Azure architecture (Resource Group, VM, NSG, Workbook, Log Analytics, Sentinel).

Resource Group with all required resources.

Resources		Recommendations
<input type="button" value="Filter for any field..."/>		Type equals all <input type="button" value="X"/> Location equals all <input type="button" value="X"/> <input type="button" value="Add filter"/>
<input type="checkbox"/>	Name ↑	Type
<input type="checkbox"/>	 4739a7b6-f0bc-480b-a66b-a29ea537d014 (VM Attack)	Azure Workbook
<input type="checkbox"/>	 4f2bd3e1-f43d-4397-a880-d5ba00da689d (VM Attack)	Azure Workbook
<input type="checkbox"/>	 Data-Windows	...
<input type="checkbox"/>	 Logs-SOC-Lab	...
<input type="checkbox"/>	 MAIN-VM-1	...
<input type="checkbox"/>	 MAIN-VM-1-ip	...
<input type="checkbox"/>	 MAIN-VM-1-nsg	...
<input type="checkbox"/>	 main-vm-1959_z1	...
<input type="checkbox"/>	 MAIN-VM-1_OsDisk_1_c5f2ab9721384dd3bff400078df	Disk
<input type="checkbox"/>	 SecurityInsights(logs-soc-lab)	...
<input type="checkbox"/>	 Vnet-SOC-Lab	...

Windows 10 Honeypot VM running on Kali Linux.



Sentinel setup with ingested logs.

The screenshot shows the Microsoft Sentinel Logs interface. On the left, there's a navigation sidebar with sections like General, Threat management, and Logs (which is selected). The main area has a search bar, a 'New Query' button, and a 'User Query' section with a time range of 'Last 24 hours' and a result count of '1000 results'. Below this is a table with columns: TimeGenerated [UTC], Computer, AttackerIp, cityname, and countryname. The table lists 10 rows of log data from August 28, 2025.

TimeGenerated [UTC]	Computer	AttackerIp	cityname	countryname
> 8/28/2025, 4:15:19.531 AM	MAIN-VM-1	80.94.95.215	Maarn	Netherlands
> 8/28/2025, 4:15:12.694 AM	MAIN-VM-1	80.94.95.215	Maarn	Netherlands
> 8/28/2025, 4:15:12.075 AM	MAIN-VM-1	197.210.194.240	Nairobi	Kenya
> 8/28/2025, 4:15:06.011 AM	MAIN-VM-1	80.94.95.215	Maarn	Netherlands
> 8/28/2025, 4:15:05.622 AM	MAIN-VM-1	223.83.34.8	Tura	India
> 8/28/2025, 4:15:05.622 AM	MAIN-VM-1	223.83.34.8	Mumbai	India
> 8/28/2025, 4:15:05.446 AM	MAIN-VM-1	125.142.157.171	Maitland	Australia
> 8/28/2025, 4:14:19.375 AM	MAIN-VM-1	223.83.34.8	Tura	India
> 8/28/2025, 4:14:19.375 AM	MAIN-VM-1	223.83.34.8	Mumbai	India
> 8/28/2025, 4:14:19.309 AM	MAIN-VM-1	125.142.157.171	Maitland	Australia

- **Figure 2:** Sample KQL query results.

Query for failed logons (Code = 4625)

The screenshot shows the Microsoft Sentinel KQL query editor. At the top, there's a 'Run' button, a time range selector ('Time range : Last 24 hours'), a result count selector ('Show : 1000 results'), and a 'KQL mode' dropdown. Below this is a code editor with a numbered script:

```
1 SecurityEvent
2 | where EventID == 4625
3 | project TimeGenerated, Account, IpAddress
4 | order by TimeGenerated desc
5
6
```

At the bottom is a results table with columns: TimeGenerated [UTC], Account, and IpAddress. The table lists 10 rows of log data from August 27, 2025.

TimeGenerated [UTC]	Account	IpAddress
> 8/27/2025, 1:21:58.734 PM	\ADMINISTRATOR	115.88.154.252
> 8/27/2025, 1:21:52.877 PM	\ADMINISTRATOR	223.83.34.8
> 8/27/2025, 1:21:52.354 PM	\ADMINISTRATOR	115.88.154.252
> 8/27/2025, 1:21:49.160 PM	\DEMO	79.112.47.154
> 8/27/2025, 1:21:46.598 PM	\ADMINISTRATOR	115.88.154.252
> 8/27/2025, 1:21:44.742 PM	\ADMIN	223.83.34.8
> 8/27/2025, 1:21:38.171 PM	\ADMINISTRATOR	115.88.154.252
> 8/27/2025, 1:21:31.438 PM	\ADMINISTRATOR	115.88.154.252
> 8/27/2025, 1:21:29.397 PM	\BACKUP	79.112.47.154

Query to enrich logs with geo-location context.

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

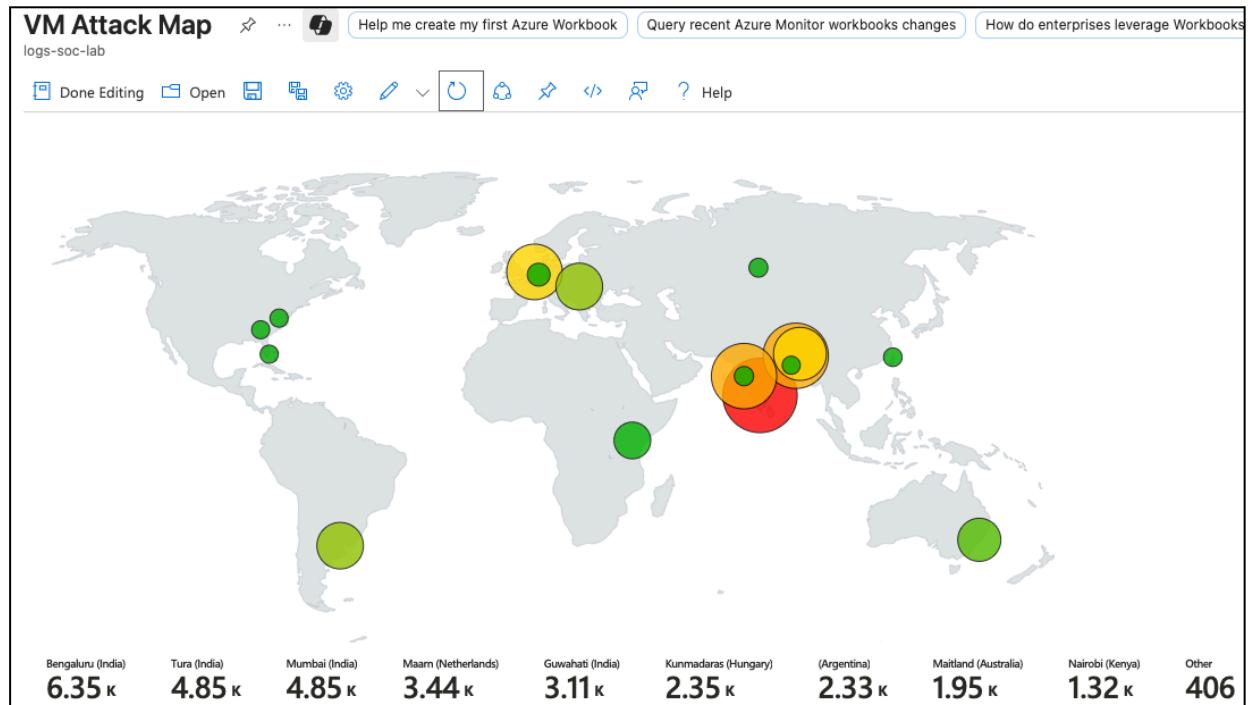
```
1 let GeoIPDB_FULL = _GetWatchlist("geoip");
2 let WindowsEvents = SecurityEvent
3 | where EventID == 4625
4 | order by TimeGenerated desc
5 | evaluate ipv4_lookup(GeoIPDB_FULL, IPAddress, network);
6 WindowsEvents
7 | project TimeGenerated, Computer, AttackerIp = IPAddress, cityname, countryname, latitude, longitude
```

Results Chart Add bookmark

d [UTC] ↑↓	Computer	AttackerIp	...	cityname
5, 1:26:32.452 PM	MAIN-VM-1	115.88.154.252		Bengaluru
5, 1:26:26.230 PM	MAIN-VM-1	115.88.154.252		Bengaluru
5, 1:26:23.501 PM	MAIN-VM-1	79.112.47.154		Kunmadaras
5, 1:26:21.240 PM	MAIN-VM-1	125.142.157.171		Maitland
5, 1:26:20.812 PM	MAIN-VM-1	115.88.154.252		Bengaluru
5, 1:26:15.025 PM	MAIN-VM-1	115.88.154.252		Bengaluru
5, 1:26:09.200 PM	MAIN-VM-1	223.83.34.8		Mumbai
5, 1:26:09.200 PM	MAIN-VM-1	223.83.34.8		Tura
5, 1:26:06.781 PM	MAIN-VM-1	115.88.154.252		Bengaluru

- Figure 3: World map visualisation of attacker IP origins.

12 hours of attack data.



With the completed environment in mind, let's dive into the step-by-step process of building this lab. The lab shows how to configure a security monitoring environment in Azure, delivering practical experience directly applicable to real-world cybersecurity roles.

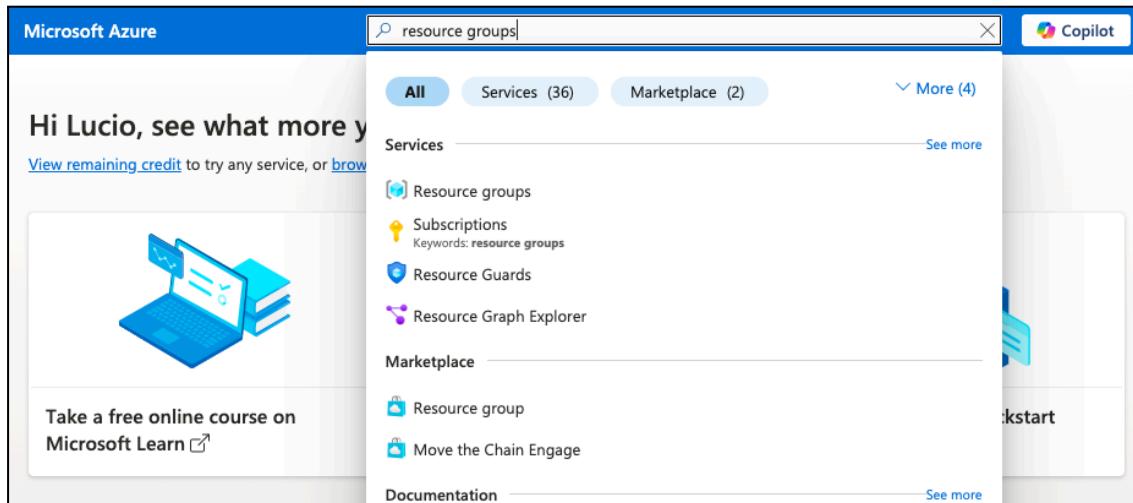
1. Azure Resource Setup

1.1 Resource Group

- Set up a dedicated resource group to logically contain project resources.
- Ensured permissions and policies were properly applied.

Figures:

Create a resource group



Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Subscription * ⓘ

Azure subscription 1

Resource group name * ⓘ

LR-SOC-Lab

Region * ⓘ

(Africa) South Africa North

1.2 Virtual Network and Subnet

- Configured a virtual network (VNet) with an associated subnet.
- This subnet serves as the foundation for connecting the virtual machine honeypot.

Figures:

Create a Vnet.

The screenshot shows the 'Create virtual network' wizard in the Azure portal. It has two main sections: 'Project details' and 'Instance details'. In 'Project details', the 'Subscription' is set to 'Azure subscription 1' and the 'Resource group' is 'LR-SOC-Lab'. In 'Instance details', the 'Virtual network name' is 'Vnet-SOC-Lab' and the 'Region' is '(Africa) South Africa North'. There is also a link to 'Deploy to an Azure Extended Zone'.

Section	Setting
Project details	Subscription
	Azure subscription 1
Resource group	LR-SOC-Lab
	Create new
Instance details	
Virtual network name *	Vnet-SOC-Lab
Region *	(Africa) South Africa North
Deploy to an Azure Extended Zone	

Section Takeaway

This foundational setup ensured all project resources were logically grouped and networked, providing a controlled environment for subsequent monitoring and security configurations.

2. Virtual Machine Honeypot

2.1 Deployment

- Deployed a Windows Virtual Machine (VM) within the subnet.
- Configured basic OS settings and ensured accessibility.

Figures

Create a VM.

The screenshot shows the 'Create a virtual machine' wizard in the 'Basics' tab. It includes sections for 'Project details' (Subscription: Azure subscription 1, Resource group: LR-SOC-Lab), 'Instance details' (Virtual machine name: MAIN-VM-1, Region: (Africa) South Africa North, Availability options: Availability zone, Zone options: Self-selected zone), and a note about deployment eligibility.

Create a virtual machine ... Help me create a VM optimized for high availability Help me create a low cost VM

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more ↗](#)

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

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 * ⓘ LR-SOC-Lab Create new

Instance details

Virtual machine name * ⓘ MAIN-VM-1

Region * ⓘ (Africa) South Africa North Deploy to an Azure Extended Zone

Availability options ⓘ Availability zone

Zone options ⓘ Self-selected zone Choose up to 3 availability zones, one VM per zone

When deploying the virtual machine, Azure provides multiple options for both the operating system image and the VM size.

Depending on the use case, different configurations may be more suitable; however, for this lab I selected Windows 10 Pro, version 22H2 - x64 Gen2 as the image and Standard_B1s as the size to balance cost efficiency with functionality.

Security type ⓘ Trusted launch virtual machines

Image * ⓘ Windows 10 Pro, version 22H2 - x64 Gen2 (free services eligible)

VM architecture ⓘ x64 Arm64

Info Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

Info You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. [Learn more](#)

Size * ⓘ Standard_B1s - 1 vcpu, 1 GiB memory (\$9.93/month) (free services eligible)

Enable Hibernation ⓘ

Info 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](#)

Configure the admin account with a username and password, and allow RDP (Remote Desktop Protocol).

Administrator account

Username * ⓘ azureuser

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 * ⓘ Allow selected ports None

Select inbound ports * RDP (3389)

Warning 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](#)

Input a Vnet name. Subnet & Public IP settings are left at default settings.

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 X

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
[Learn more](#)

Network interface

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

Virtual network * ⓘ Vnet-SOC-Lab Create new

Subnet * ⓘ default (10.0.0.0/24) Manage subnet configuration

Public IP ⓘ (new) MAIN-VM-1-ip Create new

NIC network security group ⓘ None Basic Advanced

Public inbound ports * ⓘ None Allow selected ports

Select inbound ports * RDP (3389)

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to

< Previous Next : Management Review + create Give feedback

Complete.



Your deployment is complete



Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows...

Subscription: [Azure subscription 1](#)

Resource group: [LR-SOC-Lab](#)

Inside of your resource group you'll find all of your new resources.

The screenshot shows the Azure Resource Group Overview page for a group named "LR-SOC-Lab". The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, Help, and Feedback. The main content area displays a table of resources with columns for Name, Type, and Location. The resources listed are:

Name	Type	Location
MAIN-VM-1	Virtual machine	South Africa North
MAIN-VM-1-ip	Public IP address	South Africa North
MAIN-VM-1-nsg	Network security group	South Africa North
main-vm-1959_z1	Network Interface	South Africa North
MAIN-VM-1_OsDisk_1_c5f2ab9721384dd3bff400078df	Disk	South Africa North
Vnet-SOC-Lab	Virtual network	South Africa North

At the bottom, there is a message "Showing 1 - 6 of 6. Display count: auto" and a "Give feedback" link.

2.2 Security Posture (Intentionally Vulnerable)

- Opened the Network Security Group (NSG) and cloud firewall completely to the public internet.
- Disabled internal firewalls inside the VM, ensuring maximum exposure.
- This configuration allowed the VM to attract real-world brute-force and probing attempts.

To intentionally expose the virtual machine as a honeypot, I configured the Network Security Group (NSG) with an inbound rule that allowed unrestricted access from the public internet.

This rule was given the highest priority to ensure it would override any existing restrictions. Instead of leaving only RDP open, I removed the default RDP rule and created a new inbound security rule under the *Settings* → *Inbound security rules* section, effectively making the VM fully accessible for external attack traffic.

Figures:

NSG overview.

The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The main title is "MAIN-VM-1-nsg" under the "Network security group" category. The top navigation bar includes links for "How do I create an alert to track firewall metric failures?", "Diagnose connectivity issues related to this security group", and a "+1" button. Below the title, there's a search bar and standard navigation controls (Move, Delete, Refresh, Give feedback).

The left sidebar contains a navigation menu with items like 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, and Help. A note at the bottom of the sidebar says "Add or remove favorites by pressing Ctrl+Shift+F".

The main content area is titled "Essentials" and displays basic information about the NSG, such as its resource group (LR-SOC-Lab), location (South Africa North), subscription (Azure subscription 1), and tags (Add tags). It also shows custom security rules: 1 inbound, 0 outbound, and associated resources: 0 subnets, 1 network interfaces.

A "JSON View" link is located in the top right corner of the main content area.

The central part of the screen is a table titled "Inbound Security Rules" and "Outbound Security Rules". The Inbound Security Rules table has columns for Priority, Name, Port, Protocol, Source, Destination, and Action. It lists several rules, including one for RDP (Priority 300, Port 3389, TCP, Any, Any, Allow) and others for Azure Load Balancer and DenyAllInBound. The Outbound Security Rules table lists rules for AllowVnetOutBound, AllowInternetOutBound, and DenyAllOutBound, all with Allow actions.

Inbound security rule settings.

Add inbound security rule

MAIN-VM-1-nsg

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
*

Protocol
 Any
 TCP
 UDP
 ICMPv4
 ICMPv6

Action
 Allow
 Deny

Priority * ⓘ
100

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

The inbound security rule was named *CRITICAL* to clearly distinguish it as the intentionally permissive rule. As indicated by the warnings, this configuration is highly insecure and should only be implemented in a controlled lab environment for educational purposes.

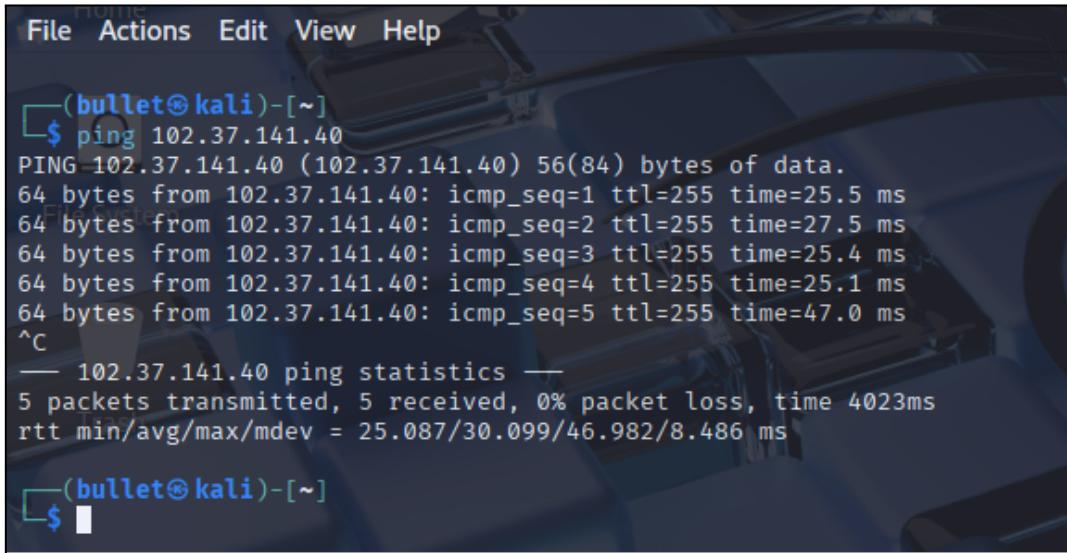
The screenshot shows a web-based configuration interface for a security rule. At the top, there is a field labeled "Name *" with the value "CRITICAL--AllowAnyCustomAnyInbound". A green checkmark icon is positioned to the right of the input field. Below this is a "Description" field which is currently empty. The main body of the interface contains four warning messages, each enclosed in a light orange box with a yellow exclamation mark icon:

- 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.

At the bottom of the interface, there are three buttons: "Add" (blue), "Cancel" (white), and "Give feedback" (blue button with a person icon).

- Next is to establish a connection to the machine. -

Verify connectivity by pinging the VM using its public IP address provided by Azure. This ensures the machine is reachable before proceeding with further configuration.



```
File Actions Edit View Help

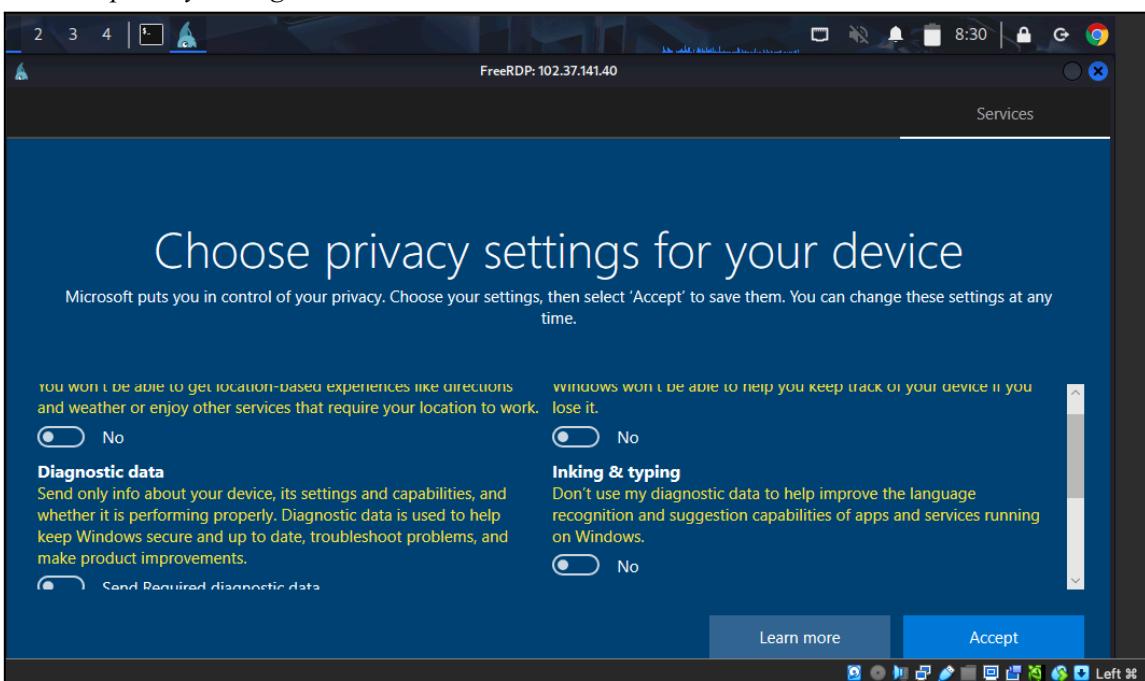
(bullet㉿kali)-[~]
$ ping 102.37.141.40
PING 102.37.141.40 (102.37.141.40) 56(84) bytes of data.
64 bytes from 102.37.141.40: icmp_seq=1 ttl=255 time=25.5 ms
64 bytes from 102.37.141.40: icmp_seq=2 ttl=255 time=27.5 ms
64 bytes from 102.37.141.40: icmp_seq=3 ttl=255 time=25.4 ms
64 bytes from 102.37.141.40: icmp_seq=4 ttl=255 time=25.1 ms
64 bytes from 102.37.141.40: icmp_seq=5 ttl=255 time=47.0 ms
^C
--- 102.37.141.40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4023ms
rtt min/avg/max/mdev = 25.087/30.099/46.982/8.486 ms

(bullet㉿kali)-[~]
$
```

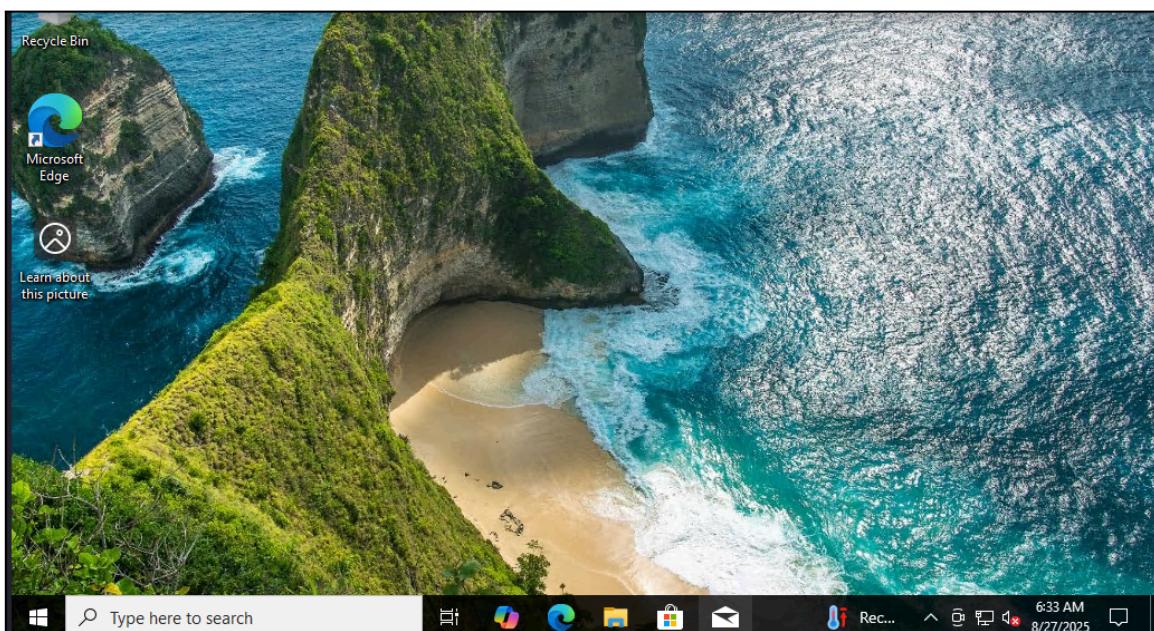
From my Linux virtual machine, I accessed the newly deployed Azure VM using the public IP address and credentials provided by Azure. The connection was established via RDP using the *xfreerdp* client, demonstrating secure remote access to the instance for monitoring and configuration purposes.



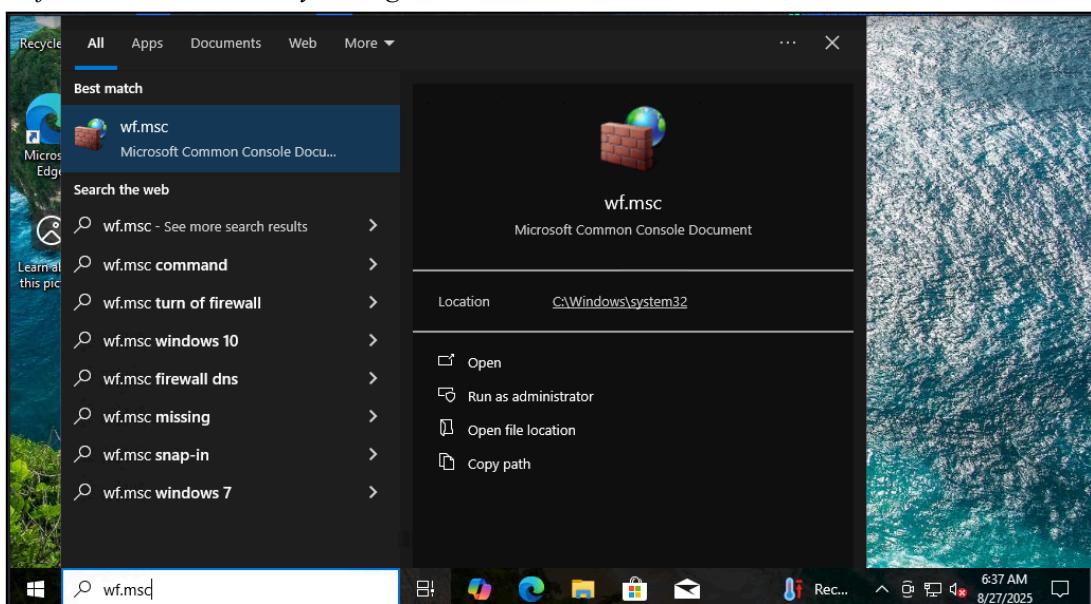
Disable all privacy settings.



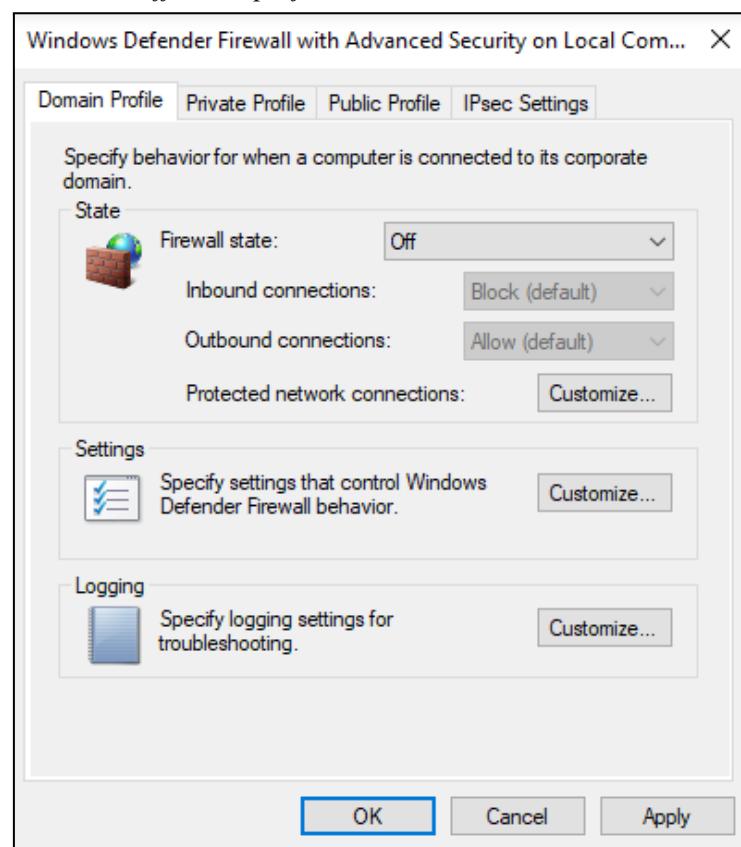
Connected.



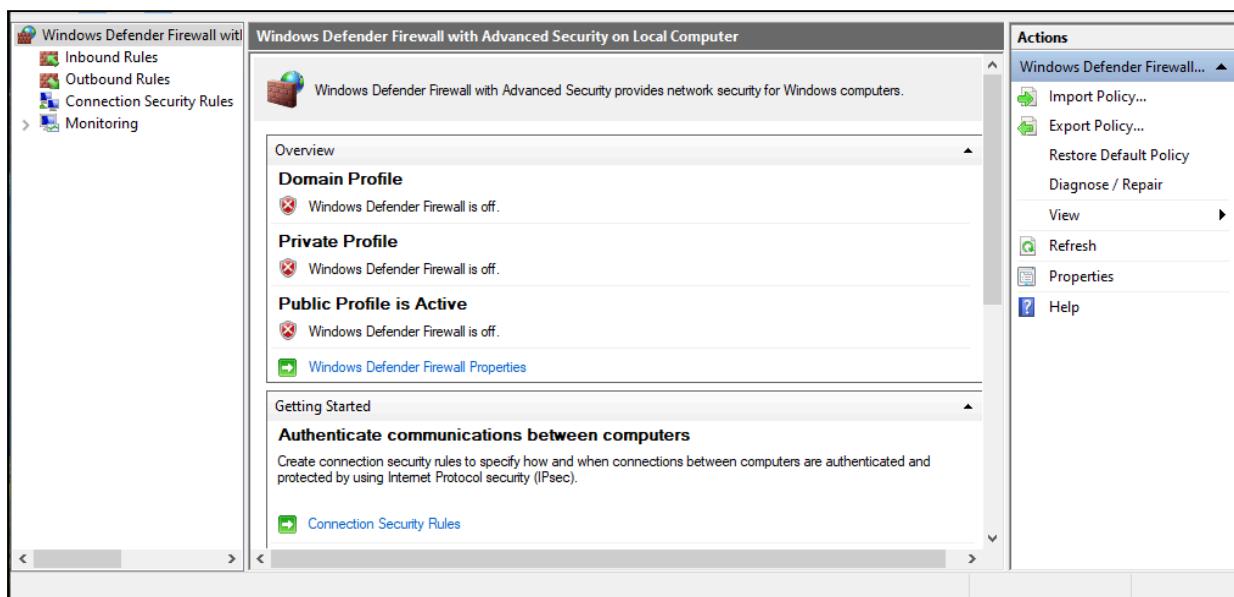
Go to wf.msc to access security settings.



Turn Firewall off on all profiles.



Results.



Section Takeaway

By deliberately exposing the VM to the public internet, it serves as an effective honeypot to attract and log real-world attack traffic for analysis.

3. Log Collection and Centralisation

3.1 Log Analytics Workspace

- Deployed a Log Analytics Workspace to serve as the central log repository.
- Configured retention policies for security-focused log storage.

Figures:

Create Log Analytics workspace.

Create Log Analytics workspace ...

[Basics](#) [Tags](#) [Review + Create](#)

Basics

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](#) X

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 * Azure subscription 1 ▼

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

Instance details

Name * Logs-SOC-Lab1 ✓

Region * South Africa North ▼

[Review + Create](#) [« Previous](#) [Next : Tags >](#)

Results.

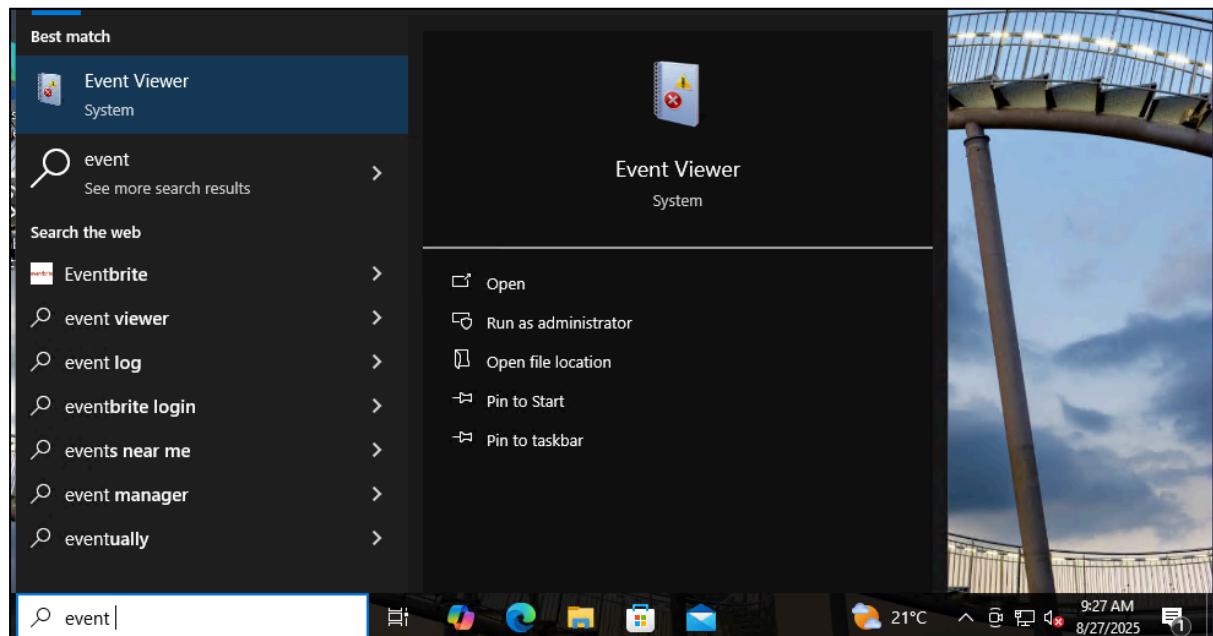
The screenshot shows the Microsoft Log Analytics OMS Overview page. At the top, it displays a deployment status message: "Your deployment is complete". Below this, detailed deployment information is provided, including the deployment name (Microsoft.LogAnalyticsOMS), subscription (Azure subscription 1), resource group (LR-SOC-Lab), start time (8/27/2025, 11:17:34 AM), and correlation ID (cf3569a1-ff0a-4122-a7f3-aff11039f5ba). There are sections for "Deployment details" and "Next steps", with a "Go to resource" button. A "Give feedback" section includes a link to "Tell us about your experience with deployment". On the right side, there is a "Notifications" panel with a single entry: "Deployment succeeded" (Dismiss all). The notification states that the deployment to resource group 'LR-SOC-Lab' was successful. It includes "Go to resource" and "Pin to dashboard" buttons, with a timestamp of "a few seconds ago". Below the main content, there are links for "Cost management" and "Security".

3.2 Azure Monitoring Agent

- Installed and configured the Azure Monitoring Agent on the VM.
- Forwarded all Windows Security Event Logs to the Log Analytics Workspace.

Figures:

Open Event Viewer on your honeypot VM.



Event Viewer displaying security logs that capture various attacker activities.

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists 'Event Viewer (Local)', 'Custom Views', 'Windows Logs' (with 'Security' selected), 'Setup', 'System', 'Forwarded Events', 'Applications and Services Logs', and 'Subscriptions'. The main pane displays a table of events under the 'Security' tab, with 1,729 events available. The table columns are 'Keyword...', 'Date and Time', 'Source', 'Event ID', and 'Task Category'. Several events are listed, all from 'Micros...' source and 'Logon' task category, with event IDs ranging from 4625 to 4799. Below the table, a specific event (Event 4672) is expanded, showing the 'General' tab with the description 'Special privileges assigned to new logon.' and the 'Subject' field. The right pane, titled 'Actions', contains a list of options: 'Open Saved Log...', 'Create Custom Vie...', 'Import Custom Vie...', 'Clear Log...', 'Filter Current Log...', 'Properties', 'Find...', 'Save All Events As...', 'Attach a Task To thi...', 'View', 'Refresh', 'Help', 'Event Properties', 'Attach Task To This ...', and 'Copy'. The 'Event Properties' option is currently selected.

By selecting “Filter Current Log...” under the Actions pane, logs can be refined based on specific parameters for easier analysis.

The screenshot shows the 'Event Viewer' window with the 'Filter Current Log' dialog box open. The dialog has tabs for 'Filter' (selected) and 'XML'. Under 'Logged:', the dropdown is set to 'Any time'. Under 'Event level:', none of the checkboxes ('Critical', 'Warning', 'Verbose', 'Error', 'Information') are checked. There are two radio buttons: 'By log' (selected) with 'Event logs:' dropdown set to 'Security', and 'By source' with 'Event sources:' dropdown. Below these, there is a note: 'Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76'. There are input fields for '4625' (under 'Event IDs'), 'Task category:', 'Keywords:', 'User:<All Users>', and 'Computer(s):<All Computers>'. A 'Clear' button is at the bottom right of the dialog.

Results after filter is applied.

The screenshot shows the Windows Event Viewer interface. The left pane displays navigation options like 'Event Viewer (Local)', 'Custom Views', 'Windows Logs' (selected), and 'Applications and Services'. Under 'Windows Logs', 'Security' is selected. The main pane shows a table of events with columns: Keyword, Date and Time, Source, Event ID, and Task Ca... (Task Category). A filter bar at the top indicates 'Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 998'. Below the table, a specific event is expanded: 'Event 4625, Microsoft Windows security auditing.' The details tab shows the message 'An account failed to log on.' and a subject field. The right pane contains an 'Actions' menu with various options like 'Filter Current Log...', 'Clear Filter', 'Properties', 'Find...', 'Save Filtered Log File...', 'Attach a Task To thi...', 'Save Filter to Custom...', 'View', 'Refresh', 'Help', and a context-specific menu for 'Event 4625, Microsoft W...'. The context menu includes 'Event Properties', 'Attach Task To This ...', 'Copy', 'Save Selected Event...', 'Refresh', and 'Help'.

Windows Security Events ingested into Microsoft Sentinel via the Azure Monitor Agent (Content Hub configuration).

The screenshot shows the Microsoft Sentinel Content Hub interface under the 'Windows Security Events' section. It displays two main counts: 74 installed content items and 22 configuration needed. On the left, there's a summary card for 'Windows Security Events' with provider 'Microsoft' and version '3.0.9'. Below it, a 'Description' section provides instructions for installing the solution, mentioning 'Release Notes' and the fact that 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. It notes that this solution includes two connectors: 'Windows Security Events via AMA' and 'Security Events via Legacy Agent'. A note states that the AMA connector is recommended over the legacy connector. On the right, a detailed view of the 'Windows Security Events via AMA' connector is shown. It includes a search bar, a list of available connectors (with 'Windows Security Events via AMA' selected), and a description of how it streams all security events from Windows machines connected to the Microsoft Sentinel workspace. It also shows the last log received, content source (Windows Security Events), version (1.0.0), author (Microsoft), supported by (Microsoft Corporation | Email), and data received (4). A link to 'Open connector page' is also present.

Create Data Collection Rule.

The screenshot shows the Microsoft Sentinel interface. On the left, the 'Windows Security Events via AMA' page is displayed, showing a status of 'Disconnected' with 'Microsoft Provider' and 'Last Log Received'. It includes sections for 'Description', 'Content source' (Windows Security Events, Version 1.0.0), 'Author' (Microsoft), 'Related content' (Workbooks: 0, Queries: 1, Analytics rules templates: 20), and 'Data received' (4). On the right, the 'Create Data Collection Rule' dialog box is open, showing the 'Basic' tab. It has a 'Prerequisites' section with instructions to ensure workspace data sources have read and write permissions and Azure Arc is installed. The 'Configuration' section includes an 'Enable data collection rule' button and a table for managing rules. A 'Rule name' field is set to 'Data-Windows', 'Subscription' to 'Azure subscription 1', and 'Resource group' to 'LR-SOC-Lab'. A 'Next: Resources >' button is at the bottom.

Cont.

This screenshot is identical to the one above, showing the 'Windows Security Events via AMA' page on the left and the 'Create Data Collection Rule' dialog box on the right. The dialog box is on the 'Basic' tab, showing the configuration for the data collection rule, including the selected resource group 'LR-SOC-Lab'. A 'Next: Resources >' button is visible at the bottom of the dialog.

Select required resource group & honeypot VM.

Create Data Collection Rule

Data collection rule management

Basic **Resources** Collect Review + create

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

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

Subscriptions	Resource Groups	Resource Types	Locations
Selected: All	Selected: All	Selected: All	Selected: All

Search to filter items... Show Selected

Scope	Resource Type	Location
Azure subscription 1		
LR-SOC-Lab		
MAIN-VM-1	microsoft.compute/virtualmachines	South Africa North

Choose the appropriate data collection type.

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 >**

Review & Create.

The screenshot shows the 'Create Data Collection Rule' wizard in progress. At the top, a green bar indicates 'Validation passed'. Below it, the 'Review + create' tab is selected. The 'Basic' section shows the rule name 'Data-Windows', subscription 'Azure subscription 1', and resource group 'LR-SOC-Lab'. Under 'Selected resources', a single VM named 'main-vm-1' is listed as a 'microsoft.compute/virtualmachines'. In the 'Selected events' section, 'AllEvents' is chosen. At the bottom, there are 'Create' and 'Cancel' buttons.

Within the VM dashboard, navigate to Settings → Extensions + Applications to verify that the Azure Monitor Windows Agent has been successfully installed.

The screenshot shows the 'Extensions + applications' blade for the VM 'MAIN-VM-1'. It lists one extension: 'AzureMonitorWindowsA...' of type 'Microsoft.Azure.Monitor...' and version '1.37.0'. The blade includes tabs for 'Extensions' and 'VM Applications', and a search bar at the top right.

Azure Monitor Agent installed.

The screenshot shows the Azure portal interface for a virtual machine named "MAIN-VM-1". The left sidebar has sections for Resource visualizer, Networking (Network settings, Load balancing, Application security groups, Network manager), Settings (Disks), and Extensions + applications (selected). The main content area is titled "Extensions" and shows one item: "AzureMonitorWindowsAgent". The details pane on the right provides the following information:

Setting	Value
Type	Microsoft.Azure.Monitor.AzureMonitorWindow
Version	1.37.0.0
Status	Provisioning succeeded
Status level	(not explicitly listed)

Section Takeaway

Centralising logs in the workspace provided a single source of truth, simplifying monitoring and enabling more effective detection and analysis.

4. Sentinel SIEM Configuration

4.1 Sentinel Deployment

- Created an Azure Sentinel instance connected to the Log Analytics Workspace.
- Verified log ingestion from the honeypot VM.

Figures:

Deploy an Azure Sentinel instance and connect it to the existing Log Analytics workspace to enable centralised security monitoring and threat detection.

The screenshot shows the 'Add Microsoft Sentinel to a workspace' page. At the top, there are two buttons: '+ Create a new workspace' and 'Refresh'. Below them are two informational messages: one about a 31-day free trial and another about automatically onboarded users redirected to the Defender portal. A search bar labeled 'Filter by name...' is followed by a table with columns: Workspace, Location, ResourceGroup, Subscription, and Directory. One row is visible, showing 'Logs-SOC-Lab' under Workspace, 'southernaficanorth' under Location, 'lr-soc-lab' under ResourceGroup, 'Azure subscription 1' under Subscription, and 'Default Directory' under Directory. At the bottom are 'Add' and 'Cancel' buttons.

In the Content Hub, filter the search by 'security events' and install the Windows Security Events solution to enable ingestion of relevant security logs.

The screenshot shows the Microsoft Sentinel Content hub. The left sidebar includes 'General', 'Threat management', 'Content management' (which is selected), 'Repositories', 'Community', and 'Configuration'. The main area has sections for 'Solutions' (419), 'Standalone contents' (319), 'Installed' (0), and 'Updates' (0). A search bar at the top right shows 'security events'. A detailed view of the 'Windows Security Events' solution is shown on the right, including its provider (Microsoft Provider), support (Microsoft Support), and version (3.0.9). It also includes a note about installing before using it with Azure Monitor Agent, a 'Release Notes' link, and a 'View details' button.

Installation complete.

The screenshot shows the Microsoft Sentinel Content hub interface. At the top, there are statistics: 419 Solutions, 319 Standalone contents, 1 Installed, and 0 Updates. A search bar shows the query "security events". The main area displays a table of content items, with one item, "Windows Security Events", highlighted and marked as "Installed". The right side of the screen provides a detailed view of the "Windows Security Events" solution, including its provider (Microsoft), support (Microsoft Support), and version (3.0.9). It also includes a note about the solution's purpose and a link to the Release Notes.

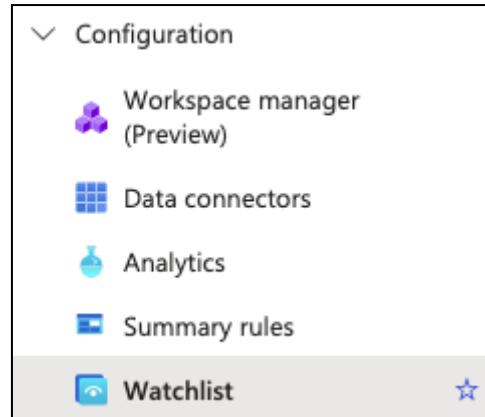
4.2 Threat Detection with Watchlists

- Uploaded a custom watchlist (spreadsheet containing IP ranges and geographic info).
- Correlated attacker IP addresses from failed logon events (4625) with the watchlist data.
- Enriched logs with geo-location context.

Figures:

Within Sentinel, navigate to Configuration → Watchlist and create a new watchlist instance to enrich log data with external context.

The screenshot shows the Microsoft Sentinel Watchlist configuration page. The left sidebar lists various configuration options, with "Watchlist" selected. The main area is titled "Watchlist" and contains sections for "What is it?" and "How does it work?". It explains that Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against events in the Microsoft Sentinel environment. The "How does it work?" section provides instructions on creating a new watchlist using the "Add new" button.



Provide a suitable name & alias.

Watchlist wizard

General Source Review + create

Name *

Description

Alias *

Prepare the watchlist file for upload; in this example, a pre-configured file provided by Josh Madakor is used.

geoip-summarized.csv

Open with ▾

geoip-summarized.csv
2.7 MB • 3 minutes ago

	A	B	C	D	E
1	network	latitude	longitude	cityname	countryname
2	1.0.0.0/16	-33.494	143.2104		Australia
3	1.1.0.0/16	17.8148	103.3386	Ban Chan	Thailand
4	1.2.0.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
5	1.3.0.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
6	1.4.0.0/16	13.8687	100.579	Bangkok	Thailand
7	1.5.0.0/16	13.6659	100.588	Bangkok	Thailand
8	1.6.0.0/16	12.9834	77.5855	Bengaluru	India
9	1.7.0.0/16	12.9691	77.5902	Bengaluru	India
10	1.8.0.0/16	12.9557	77.5843	Bengaluru	India
11	1.9.0.0/16	3.1539	101.7448	Ampang	Malaysia
12	1.10.0.0/16	17.8842	102.7394	Nong Khai	Thailand

Select “network” as the SearchKey.

The screenshot shows the Microsoft Sentinel Watchlist wizard interface. On the left, the 'Source' tab is selected, displaying fields for 'Source type' (Local file), 'File type' (CSV file with a header), 'Number of lines before row with headings' (0), and an uploaded file named 'geoip-summarized.csv'. A 'SearchKey' dropdown is set to 'network'. Below these are buttons for 'Reset' and 'Next : Review + create >'. On the right, a 'File preview' section shows the first 5 columns of the CSV file, which include 'network', 'latitude', 'longitude', 'cityname', and 'countryname'. The preview data includes rows from 1.0.0/16 to 1.9.0/16, with various geographical coordinates and country names.

Wait for the selected file to upload fully.

The screenshot shows the Microsoft Sentinel Watchlist Items page. It displays two sections: 'Watchlists' (0 items) and 'Watchlist Items' (0 items). The 'My Watchlists' section on the left shows a search bar and a table with a single row named 'geoip' under the 'Name' column and 'geoip' under the 'Alias' column. The 'Templates (Preview)' section on the right shows a detailed view of the 'geoip' watchlist. It includes fields for 'Provider' (Microsoft), 'Rows' (0), 'Created ti...' (8/27/2020), 'Description' (empty), 'Source' ('geoip-summarized.csv'), 'Created by' ('lucio11303@gmail.com'), 'Last updated' ('8/27/2025, 12:23:06 PM'), 'SearchKey' ('network'), and 'Status (Preview)' ('Uploading (7.3%)'). At the bottom, there are buttons for 'View in logs' and 'Update watchlist'.

Upload complete.

The screenshot shows the Microsoft Sentinel Watchlists interface. At the top, it displays '1 Watchlists' and '55K Watchlist Items'. On the left, the 'My Watchlists' section is shown with a 'New' button, a search bar, and a table header with columns: Name, Alias, Source, Created..., Last up... A row for 'geoip' is selected. On the right, a detailed view of the 'geoip' watchlist is displayed, including its provider (Microsoft), rows (55K), creation time (8/27/2025, 12:23...), description ('geoip-summarized.csv'), source ('geoip-summarized.csv'), created by ('lucio11303@gmail.com'), last updated ('8/27/2025, 12:23:06 PM'), search key ('network'), and status ('Succeeded').

Section Takeaway

Integrating Sentinel with the workspace transformed raw event data into actionable intelligence, laying the foundation for meaningful threat hunting.

5. Threat Hunting and Visualization

5.1 KQL Queries

- Executed KQL queries to identify failed login attempts against the VM.
- Mapped source IP addresses to geographic locations using the watchlist.

Figures:

This query identifies failed Remote Desktop logon attempts (Event ID 4625) on the honeypot VM. Monitoring these attempts is important because attackers often brute-force credentials, and repeated failures from the same IP can indicate malicious behavior.

The screenshot shows a KQL query interface with the following details:

Query:

```
1 SecurityEvent
2 | where EventID == 4625
3 | project TimeGenerated, Account, IpAddress
4 | order by TimeGenerated desc
5
6
```

Run button, Time range: Last 24 hours, Show: 1000 results, KQL mode dropdown.

Results table:

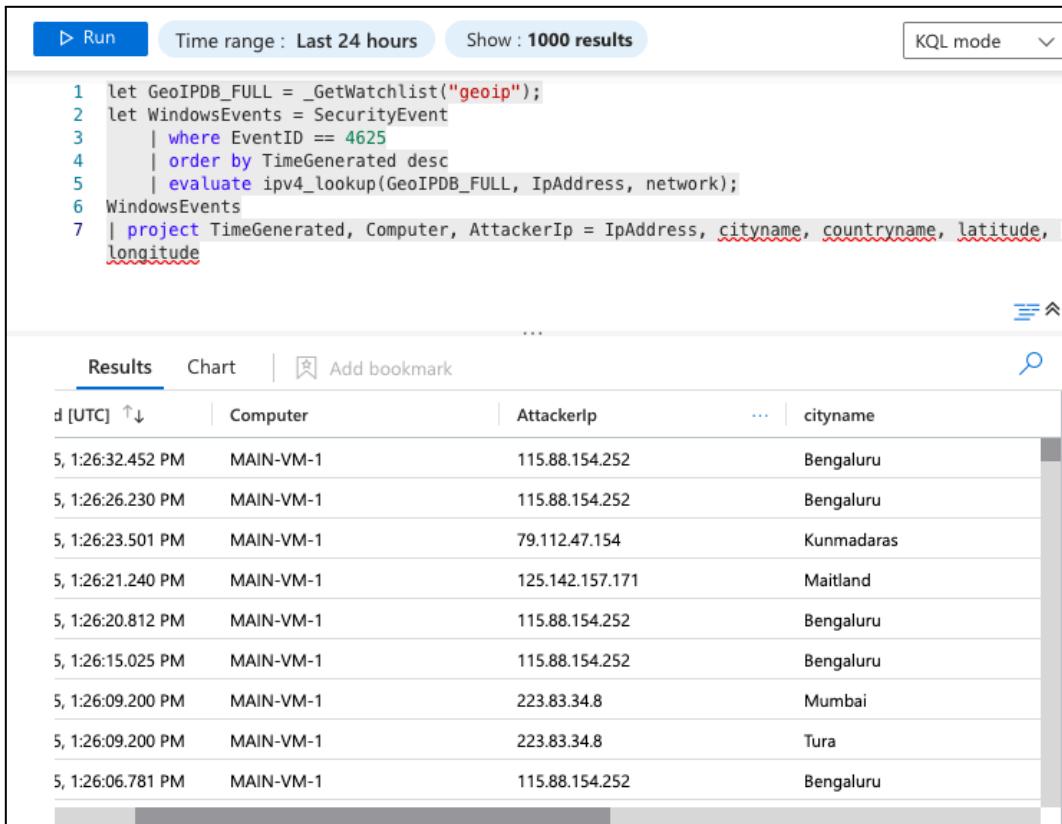
TimeGenerated [UTC]	Account	IpAddress
8/27/2025, 1:21:58.734 PM	\ADMINISTRATOR	115.88.154.252
8/27/2025, 1:21:52.877 PM	\ADMINISTRATOR	223.83.34.8
8/27/2025, 1:21:52.354 PM	\ADMINISTRATOR	115.88.154.252
8/27/2025, 1:21:49.160 PM	\DEMO	79.112.47.154
8/27/2025, 1:21:46.598 PM	\ADMINISTRATOR	115.88.154.252
8/27/2025, 1:21:44.742 PM	\ADMIN	223.83.34.8
8/27/2025, 1:21:38.171 PM	\ADMINISTRATOR	115.88.154.252
8/27/2025, 1:21:31.438 PM	\ADMINISTRATOR	115.88.154.252
8/27/2025, 1:21:29.397 PM	\BACKUP	79.112.47.154

This query tracks successful logons (Event ID 4624). By comparing these with failed logons, we can determine if brute-force attempts eventually succeeded, which would indicate a compromised system.

The screenshot shows a Kusto Query Editor interface. At the top, there are buttons for 'Run' (highlighted in blue), 'Time range : Last 24 hours', 'Show : 1000 results', and a dropdown for 'KQL mode'. Below the query pane, the results are displayed in a table format. The table has four columns: 'TimeGenerated [UTC]', 'Account', 'IpAddress', and 'LogonType'. The data shows multiple entries for the account 'NT AUTHORITY\SYSTEM' at various times on 8/27/2025, all with LogonType 5 (Success). The bottom of the interface shows performance metrics ('0s 598ms'), a 'Display time (UTC+00:00)' dropdown, 'Query details', and '1 - 10 of 32' results.

TimeGenerated [UTC]	Account	IpAddress	LogonType
> 8/27/2025, 1:08:23.553 PM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 1:05:51.967 PM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 12:57:44.756 PM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 12:39:44.178 PM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 12:15:04.661 PM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 12:05:51.966 PM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 11:39:44.161 AM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 11:11:08.068 AM	NT AUTHORITY\SYSTEM	-	5
> 8/27/2025, 10:57:46.567 AM	NT AUTHORITY\SYSTEM	-	5

This query correlates attacker IP addresses from failed logon events with the custom watchlist containing geolocation data. This enrichment allows us to visualise where attacks are originating globally, providing greater situational awareness of threat patterns.



The screenshot shows the Kibana interface with a search bar set to "Time range : Last 24 hours" and "Show : 1000 results". The KQL mode dropdown is open. The query is:

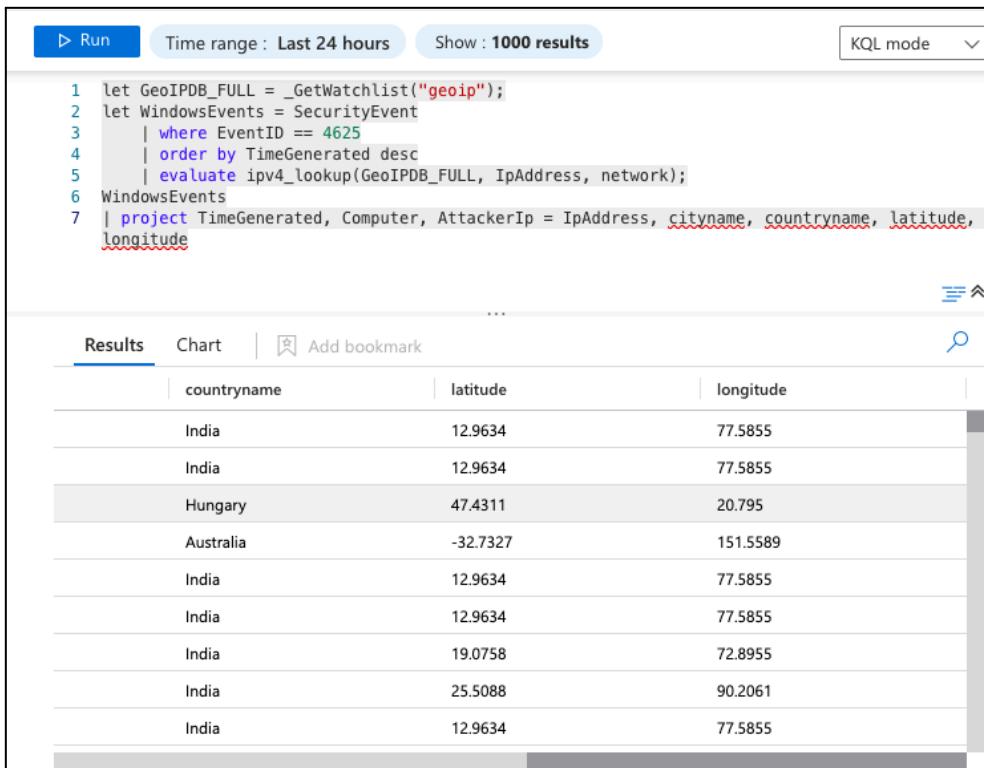
```

1 let GeoIPDB_FULL = _GetWatchlist("geoip");
2 let WindowsEvents = SecurityEvent
3 | where EventID == 4625
4 | order by TimeGenerated desc
5 | evaluate ipv4_lookup(GeoIPDB_FULL, IPAddress, network);
6 WindowsEvents
7 | project TimeGenerated, Computer, AttackerIp = IPAddress, cityname, countryname, latitude, longitude

```

The results table has columns: d [UTC] (sorted), Computer, AttackerIp, ..., cityname. The data includes:

d [UTC]	Computer	AttackerIp	cityname
5, 1:26:32.452 PM	MAIN-VM-1	115.88.154.252	Bengaluru
5, 1:26:26.230 PM	MAIN-VM-1	115.88.154.252	Bengaluru
5, 1:26:23.501 PM	MAIN-VM-1	79.112.47.154	Kunmadaras
5, 1:26:21.240 PM	MAIN-VM-1	125.142.157.171	Maitland
5, 1:26:20.812 PM	MAIN-VM-1	115.88.154.252	Bengaluru
5, 1:26:15.025 PM	MAIN-VM-1	115.88.154.252	Bengaluru
5, 1:26:09.200 PM	MAIN-VM-1	223.83.34.8	Mumbai
5, 1:26:09.200 PM	MAIN-VM-1	223.83.34.8	Tura
5, 1:26:06.781 PM	MAIN-VM-1	115.88.154.252	Bengaluru



The screenshot shows the Kibana interface with the same search parameters and KQL mode. The query is identical to the one above.

The results table has columns: countryname, latitude, longitude. The data includes:

countryname	latitude	longitude
India	12.9634	77.5855
India	12.9634	77.5855
Hungary	47.4311	20.795
Australia	-32.7327	151.5589
India	12.9634	77.5855
India	12.9634	77.5855
India	19.0758	72.8955
India	25.5088	90.2061
India	12.9634	77.5855

5.2 Attack Mapping

- Created a geographical visualisation within Sentinel showing attacker origins.
- This provided clear insight into global attack distribution.

Screenshot Example:

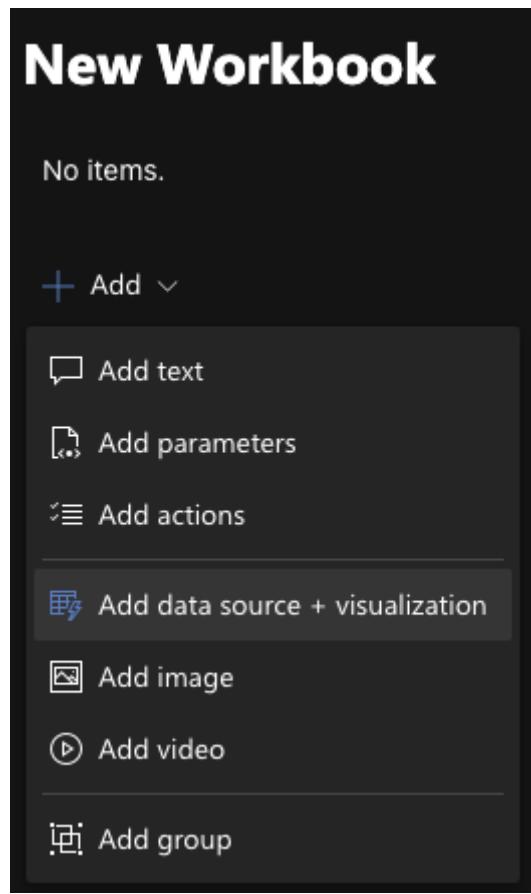
Create a sentinel workbook.

The screenshot shows the Microsoft Defender interface with a dark theme. On the left, there's a navigation sidebar with categories like Exposure management, Investigation & response, Threat intelligence, Microsoft Sentinel (which is selected), Email & collaboration, Cases, SOC optimization, Reports, Learning hub, Trials, More resources, and System. At the top center, it says "Microsoft Defender | Default Directory" with a search bar and various icons. In the center, under "My workbooks", there are sections for "My workbooks" (0), "Templates" (2), and "Updates" (0). A "Content hub" link is also present. Below this, there's a "Microsoft Sentinel Workbooks" section with a "What is it?" description, a "Getting started" button, and a "Featured workbooks" section. A large "New Workbook" button is located at the bottom right of this central area.

Clear pre-existing rules.

The screenshot shows the "New Workbook" editor. At the top, it says "New Workbook". Below that, there's a message "No items." and a "Add" button. At the top right, there are several status indicators: "Done Editing", "Advanced editor", "Refresh", and "Auto refresh: Off". The main area is completely blank, indicating no existing items in the workbook.

Create a new “Add data source + visualization” workbook.



JSON code for the attack map, sourced from Josh Madakor, used to visualise attacker locations.

```
{
    "type": 3,
    "content": {
        "version": "KqlItem/1.0",
        "query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n| order by TimeGenerated desc\n| evaluate ipv4 lookup(GeoIPDB_FULL,IpAddress, network)\n| summarize FailureCount = count() byIpAddress, latitude, longitude, cityname, countryname\n| project FailureCount, AttackerIp = IpAddress, latitude, longitude, city = cityname, country = countryname,\nfriendly_location = strcat(cityname, \" (\", countryname, \")\")",
        "size": 3,
        "timeContext": {
            "durationMs": 2592000000
        },
        "queryType": 0,
        "resourceType": "microsoft.operationalinsights/workspaces",
        "visualization": "map",
        "mapSettings": {
            "locInfo": "LatLong",
            "locInfoColumn": "countryname",
            "latitude": "latitude",
            "longitude": "longitude",
            "sizeSettings": "FailureCount",
            "sizeAggregation": "Sum",
            "opacity": 0.8,
            "labelSettings": "friendly_location",
            "legendMetric": "FailureCount",
            "legendAggregation": "Sum",
            "itemColorSettings": {
                "nodeColorField": "FailureCount",
                "colorAggregation": "Sum",
                "type": "heatmap",
                "heatmapPalette": "greenRed"
            }
        }
    },
    "name": "query - 0"
}
```

Navigate to Advanced Editor, clear pre-existing code and insert the map code.

New Workbook

1 Editing: text - 0

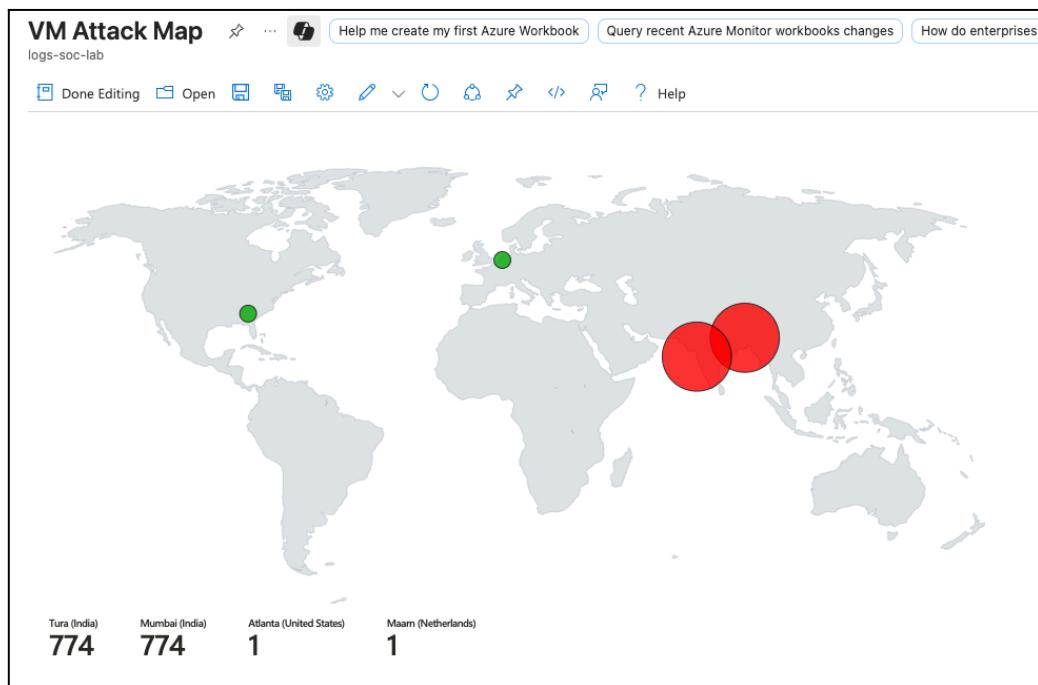
Text Settings Visual Formatting Step Settings Advanced Editor

① Shown below is a JSON representation of the current item. Any changes you make here will be reflected when you press 'Apply'.

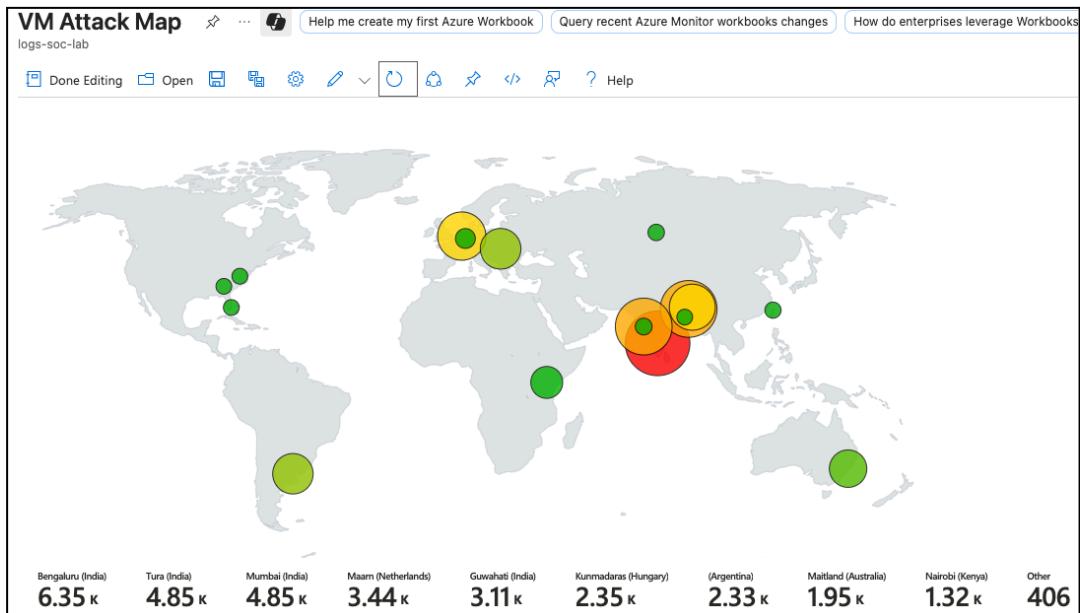
```
1 {  
2   "type": 3,  
3   "content": {  
4     "version": "KqlItem/1.0",  
5     "query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n",  
6     "size": 3,  
7     "timeContext": {  
8       "durationMs": 2592000000  
9     },  
10    "queryType": 0,  
11    "resourceType": "microsoft.operationalinsights/workspaces",  
12    "visualization": "map",  
13    "mapSettings": {  
14      "locInfo": "LatLong",  
15      "locInfoColumn": "countryname",  
16    }  
17  }  
18}  
19
```

Apply

3 hours of attack data.



12 hours of attack data.



Section Takeaway

Through KQL queries and geographic mapping, raw attack logs were enriched with context, making patterns of malicious activity clear and actionable.

Cleanup and Teardown

Once the lab is complete, it is best practice to remove all deployed resources to reduce unnecessary costs and eliminate exposure of public-facing services. In Azure, this process is straightforward:

- **Delete the Virtual Machine (VM):** Remove the VM and any associated disks.
- **Remove the Network Security Group (NSG):** Delete custom inbound rules to prevent open attack surfaces.
- **Delete the Log Analytics Workspace:** If no longer needed, removing the workspace ensures logs and data ingestion stop, preventing additional charges.
- **Delete the Microsoft Sentinel Instance:** If it was only used for this lab, removing the instance avoids ongoing costs.
- **Clean Up Resource Groups:** Deleting the entire resource group will automatically remove all associated resources in one step.

Delete a resource group

LR-SOC-Lab 

Dependent resources to be deleted (12)
All dependent resources, including hidden types, are shown

Name	Resource type
 4739a7b6-f0bc-480b-a66b-a29ea537d014 (VM At)	Azure Workbook
 4f2bd3e1-f43d-4397-a880-d5ba00da689d (VM At)	Azure Workbook
 AzureMonitorWindowsAgent (main-vm-1/AzureM	microsoft.compute/virtualMachines/exten...
 Data-Windows	Data collection rule
 Logs-SOC-Lab	Log Analytics workspace
 MAIN-VM-1	Virtual machine
 MAIN-VM-1-ip	Public IP address
 MAIN-VM-1-nsg	Network security group
 main-vm-1959_z1	Network interface
 MAIN-VM-1_OsDisk_1_c5f2ab9721384dd3bfff400C	Disk
 SecurityInsights(logs-soc-lab)	Solution
 Vnet-SOC-Lab	Virtual network

Apply force delete for selected Virtual machines and Virtual machine scale sets 

Enter resource group name to confirm deletion *

Delete **Cancel**

Final Things Learned

Completing this project reinforced my understanding of cloud-based security monitoring and SIEM operations. I gained practical insights into:

- Building and securing Azure environments while deliberately exposing a honeypot for research.
- Using Sentinel and KQL to detect, enrich, and visualise attack data.
- How real-world brute-force and probing activity appears in logs.
- The importance of contextual enrichment (watchlists, geolocation) for actionable threat analysis.
- The end-to-end process of turning raw logs into meaningful security intelligence.

This project not only strengthened my Azure and Sentinel skills but also mirrored workflows commonly used in professional security operations, providing a strong foundation for practical threat hunting and incident response.