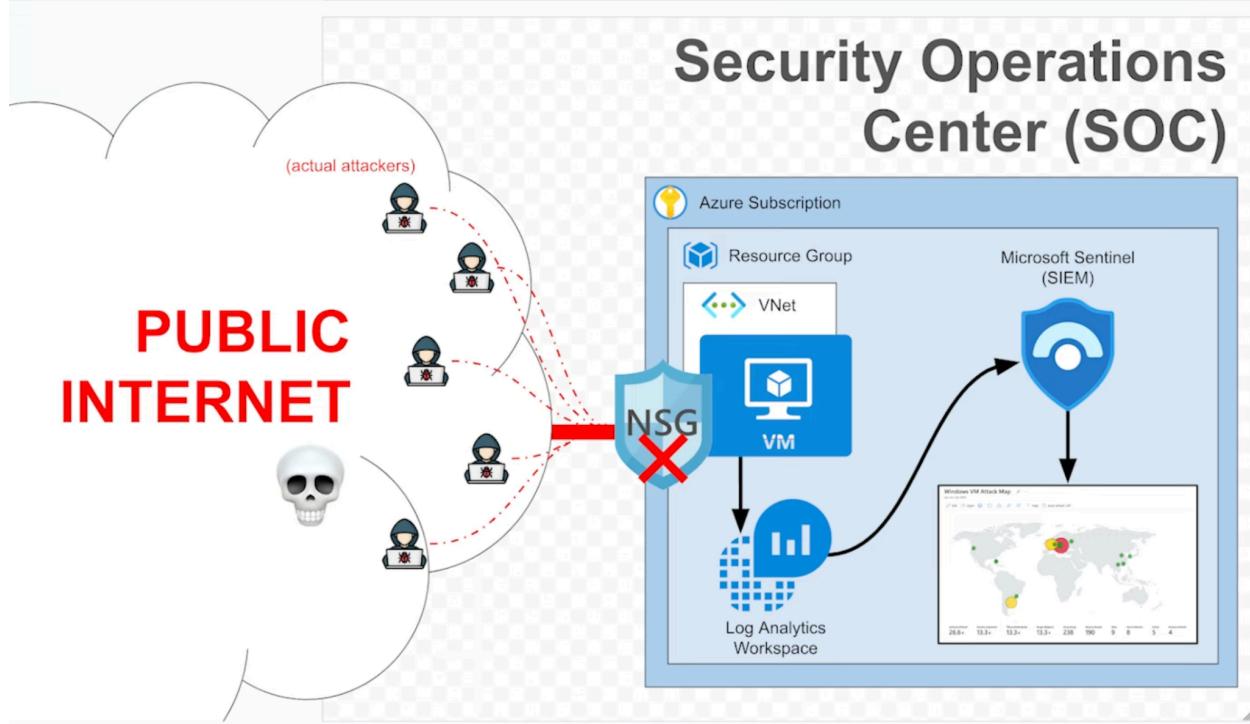


# Azure - Live Threat Detection & Geo-Mapping SIEM Lab



## 1. Executive Summary

The objective of this project was to design and deploy a live **Security Operations Center (SOC)** in a cloud environment using Microsoft Azure. By intentionally deploying a vulnerable Windows 10 Virtual Machine (Honeypot) to the public internet, I captured real-world cyber-attack data. This data was ingested into **Microsoft Sentinel (SIEM)**, analyzed using **Kusto Query Language (KQL)**, and visualized on a global geographic map to identify threat actor origins and attack patterns.

## 2. System Architecture

The lab environment was built entirely within the Azure cloud ecosystem to simulate a corporate security stack:

- **Target Asset:** Windows 10 Pro Virtual Machine.
- **Security Stack:** Microsoft Sentinel (SIEM) + Log Analytics Workspace (LAW).
- **Log Ingestion:** Azure Monitor Agent (AMA) via Data Collection Rules (DCR).
- **Intelligence:** Custom Geo-IP Watchlist for threat enrichment.

## 3. Implementation Phases

### Phase I: Cloud Environment Provisioning

The foundational infrastructure was established to ensure all assets were logically grouped and networked.

- **Resource Management:** Created a dedicated Azure Resource Group to contain all project assets, allowing for streamlined cost management and resource cleanup.
- **Network Topology:** Provisioned a Virtual Network (VNet) and Subnet to provide the networking layer for the Honeypot VM.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the 'Microsoft Azure' logo, a search bar containing 'Search resources, services, and docs (G+)', and a 'Copilot' button. Below the header, the URL 'Home > Resource groups >' is visible. The main content area has a title 'Create a resource group' with a three-dot ellipsis next to it. There are three tabs at the top of this section: 'Basics' (which is selected), 'Tags', and 'Review + create'. Under the 'Basics' tab, there's a descriptive text about what a resource group is, followed by three input fields: 'Subscription \*' (set to 'Azure subscription 1'), 'Resource group name \*' (set to 'RG-SOC-Lab'), and 'Region \*' (set to '(US) East US 2'). A small cursor icon is visible near the bottom right of the input fields.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', a search bar, and a breadcrumb trail: Home > Virtual networks > Create virtual network. Below the header, tabs for 'Basics', 'Security', 'IP addresses', 'Tags', and 'Review + create' are visible, with 'Basics' being the active tab.

**Project details**

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

Subscription \*: Azure subscription 1  
Resource group \*: RG-SOC-Lab  
Create new

**Instance details**

Virtual network name \*: Vnet-soc-lab  
Region \*: (US) East US 2  
Deploy to an Azure Extended Zone

At the bottom, there are 'Previous' and 'Next' buttons, and a prominent blue 'Review + create' button.

## Phase II: Honeypot Deployment & Security Modification

A Windows 10 VM was deployed with a specific configuration to attract and capture malicious traffic.

- **Intentional Vulnerability:** Modified the Network Security Group (NSG) to implement an "Any-to-Any" inbound rule, allowing traffic from all ports and protocols from the public internet.
- **Host-Level Exposure:** Logged into the VM via RDP and disabled the internal Windows Defender Firewall to ensure the machine was "pingable" and fully discoverable by external scanners.

## Create a virtual machine

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

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

**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.

### 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	1
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)

< Previous

Next >

**Create**



## Add inbound security rule

X

CORP-NET-EAST-1-nsg

Source ⓘ

Any



Source port ranges \* ⓘ

\*

Destination ⓘ

Any



Service ⓘ

Custom



Destination port ranges \* ⓘ

8080

Protocol

- Any
- TCP
- UDP
- ICMPv4

Action

- Allow
- Deny

Priority \*

100

Name \*

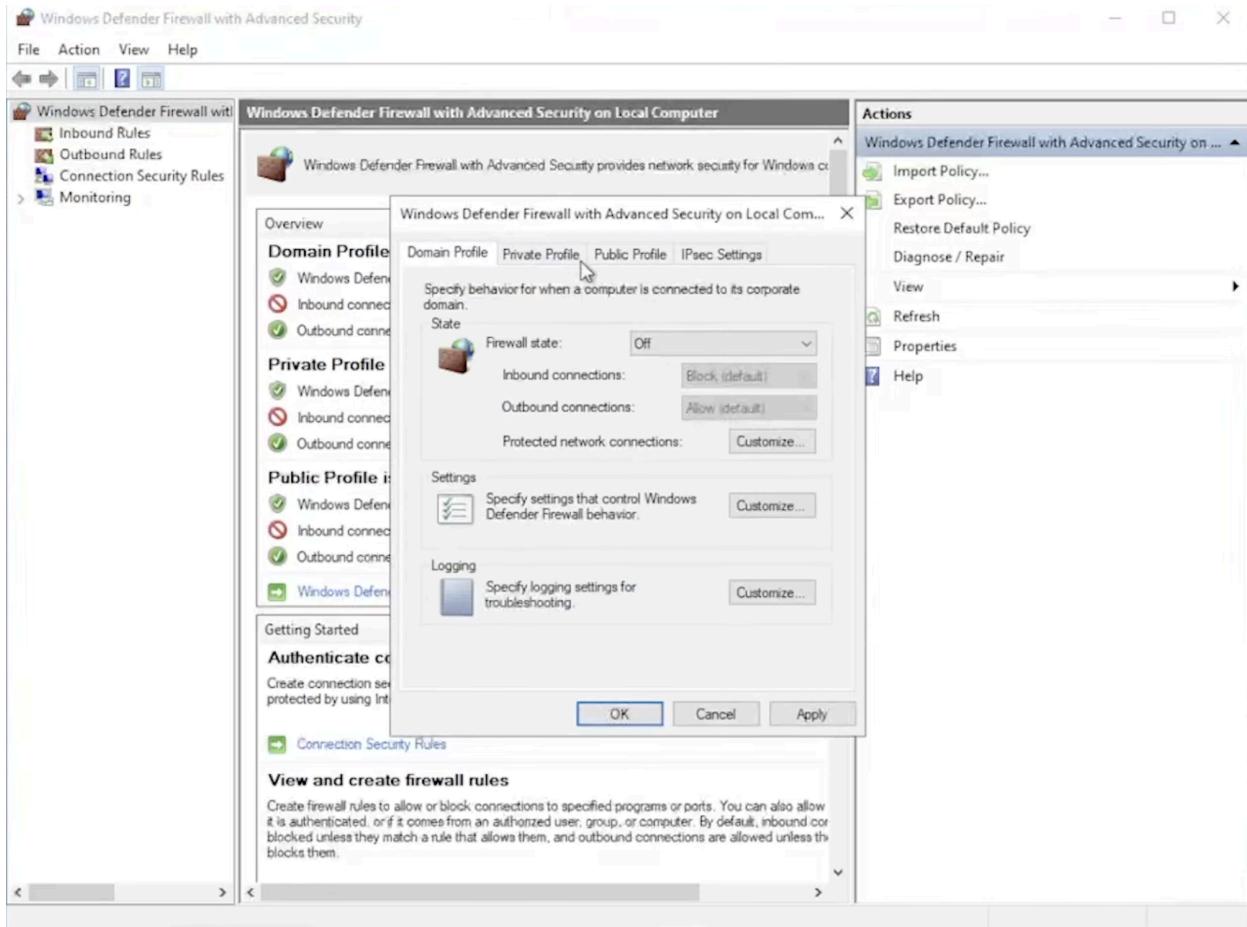
AllowAnyCustom8080Inbound

Description

Add

Cancel

Give feedback



## Phase III: SIEM & Log Analytics Configuration

To analyze the incoming attacks, a centralized logging and analysis hub was required.

- **Workspace Setup:** Deployed a **Log Analytics Workspace (LAW)** to act as the primary database for security events.
- **Sentinel Activation:** Provisioned **Microsoft Sentinel** on top of the LAW, enabling SIEM/SOAR capabilities, including incident management and advanced data visualization.

## Create Log Analytics workspace

...

Basics Tags Review + Create

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

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

### Project details

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

Subscription \* 

Azure subscription 1 

Resource group \* 

RG-SOC-Lab 

[Create new](#)

### Instance details

Name \* 

LAW-soc-lab-0000 

Region \* 

East US 2 

[Review + Create](#)

[« Previous](#)

[Next : Tags >](#)

The screenshot shows the Microsoft Sentinel 'Add Microsoft Sentinel to a workspace' interface. At the top, there's a navigation bar with 'Home > Microsoft Sentinel >' and a title 'Add Microsoft Sentinel to a workspace'. Below the title are buttons for 'Create a new workspace' and 'Refresh'. A message bar at the top states 'Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.' A search bar labeled 'Filter by name...' is present. The main area displays a table with columns: Workspace, Location, ResourceGroup, Subscription, and Directory. One row is visible, showing 'LAW-soc-lab-0000' in the Workspace column, 'eastus2' in Location, 'rg-soc-lab' in ResourceGroup, 'Azure subscription 1' in Subscription, and 'Default Directory' in Directory. A progress bar at the bottom right indicates 'Adding Microsoft Sentinel' and 'Adding Microsoft Sentinel to workspace 'LAW-soc-lab-0000''. At the bottom left are 'Add' and 'Cancel' buttons.

## Phase IV: Data Ingestion & Agent Deployment

Bridging the gap between the target VM and the SIEM was critical for real-time monitoring.

- **Data Collection Rules (DCR):** Configured a DCR to specifically target Windows Security Events.
- **Agent Installation:** Deployed the **Azure Monitor Agent (AMA)** to the Honeypot. This facilitated the streaming of Event ID 4625 (Failed Logon attempts) from the VM's local event viewer directly to the cloud workspace.

## Create Data Collection Rule

Data collection rule management

... Data Collection Rule creation in progress



Creating Data Collection Rule...

Validation passed

Basic Resources Collect Review + create

Basic

Data rule name DCR-Windows

Subscription Azure subscription 1

Resource Group RG-SOC-Lab

Selected resources

Name	Type
corp-net-east-1	microsoft.compute/virtualmachines

Selected events

AllEvents

< Previous

Create

The screenshot shows the Azure portal interface for a virtual machine named "CORP-NET-EAST-1". The main title bar says "CORP-NET-EAST-1 | Extensions + applications". On the left, there's a navigation sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Settings, Disks, and Extensions + applications (which is currently selected). The main content area is titled "Extensions" and "VM Applications". It includes buttons for Add, Refresh, Update, Enable automatic upgrade, Disable automatic upgrade, and Feedback. A search bar at the top right says "Search to filter items...". Below it, a table lists one item: "AzureMonitorWindowsA..." with Type "Microsoft.Azure.Monitor...", Version "1.32.0.0", Latest Version "1.32.0.0", and Status "Transitioning".

## Phase V: Threat Detection & Analysis (KQL)

With data flowing, I utilized **Kusto Query Language (KQL)** to transform raw logs into actionable intelligence.

- **Log Querying:** Authored queries to parse the **SecurityEvent** table, filtering for authentication failures.
- **Field Extraction:** Extracted critical metadata including Source IP, Account Username attempted, and Timestamp to build a profile of the ongoing brute-force attacks.

Home > Log Analytics workspaces > LAW-soc-lab-0000

LAW-soc-lab-0000 | Logs Log Analytics workspace

New Query 1 + Try the new Log An... Feedback Queries hub ...

LAW-soc-lab-0000 Select scope Run Time range: Last 24 hours Save Share New alert rule Export Pin to Format query ...

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

Results Chart

TimeGenerated [UTC] ↑	Account	Computer	EventID	Activity	IpAddress
> 2/14/2025, 7:15:59.976 AM	\DELIVERY	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107
> 2/14/2025, 7:15:59.974 AM	\TEMPDEBUGACCOUNT	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.169
> 2/14/2025, 7:15:59.928 AM	\ADMINISTRATOR	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.77
> 2/14/2025, 7:15:59.928 AM	\PATRONAT	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	94.102.52.73
> 2/14/2025, 7:15:59.839 AM	\DINHNV	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	92.63.197.9
> 2/14/2025, 7:15:59.729 AM	\RECRUITING	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.169
> 2/14/2025, 7:15:59.716 AM	\MAINTENANCE	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107
> 2/14/2025, 7:15:59.631 AM	\JSUSAN	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	94.102.52.73
> 2/14/2025, 7:15:59.579 AM	\PFT	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	92.63.197.9
> 2/14/2025, 7:15:59.566 AM	\ADMINISTRATOR	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.77
> 2/14/2025, 7:15:59.495 AM	\AUDITOR	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.169
> 2/14/2025, 7:15:59.433 AM	\MARINA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107
> 2/14/2025, 7:15:59.318 AM	\WAN-ADMIN	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	94.102.52.73

1s 959ms Display time (UTC+00:00) ▾

Query details | 1 - 13 of 6349

Home > Log Analytics workspaces > LAW-soc-lab-0000

LAW-soc-lab-0000 | Logs Log Analytics workspace

New Query 1 + Try the new Log An... Feedback Queries hub ...

LAW-soc-lab-0000 Select scope Run Time range: Set in query Save Share New alert rule Export Pin to Format query ...

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

Results Chart

TimeGenerated [UTC] ↑	Account	Computer	EventID	Activity	IpAddress
> 2/14/2025, 7:17:39.338 AM	\NABAR	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107
> 2/14/2025, 7:17:39.222 AM	\ADMINISTRATOR	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.77
> 2/14/2025, 7:17:39.200 AM	\UPLOAD	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	92.63.197.9
> 2/14/2025, 7:17:39.152 AM	\CRISTINA	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	94.102.52.73
> 2/14/2025, 7:17:39.152 AM	\TRAINING	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.169
> 2/14/2025, 7:17:39.093 AM	\TADMIN	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107
> 2/14/2025, 7:17:38.940 AM	\RIF	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	92.63.197.9
> 2/14/2025, 7:17:38.930 AM	\PRADEEP	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.77
> 2/14/2025, 7:17:38.910 AM	\CONTROLS	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.169
> 2/14/2025, 7:17:38.845 AM	\MICROLAB	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	94.102.52.73
> 2/14/2025, 7:17:38.841 AM	\VN	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.243.96.107
> 2/14/2025, 7:17:38.672 AM	\DENTAL	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	185.156.73.169
> 2/14/2025, 7:17:38.671 AM	\VASSAM	CORP-NET-EAST-1	4625	4625 - An account failed to log ...	92.63.197.9

1s 400ms Display time (UTC+00:00) ▾

Query details | 11 - 24 of 443

## Phase VI: Threat Intelligence Enrichment & Visualization

The final phase involved adding context to the data to understand the "Who" and "Where" of the attacks.

- **Geo-IP Mapping:** Integrated a custom Watchlist into Sentinel containing global IP-to-location mappings.

Home > Microsoft Sentinel | Watchlist >

**Watchlist wizard** ... X

General    **Source**    Review + create

Source type \* Local file

File type \* CSV file with a header (.csv)

Number of lines before row with headings \* 0

Upload file \* geoip-summarized.csv

SearchKey \* network

Reset

**File preview** | First 50 rows and first 5 columns

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

< Previous    Next : Review + create > Give feedback

Home > Log Analytics workspaces > LAW-soc-lab-0000

**LAW-soc-lab-0000 | Logs** X

Log Analytics workspace

New Query 1\* + Run Try the new Log An... Feedback Queries hub Format query

Law-soc-lab-0000 Select scope Time range: Last 24 hours Save Share New alert rule Export Pin to Format query

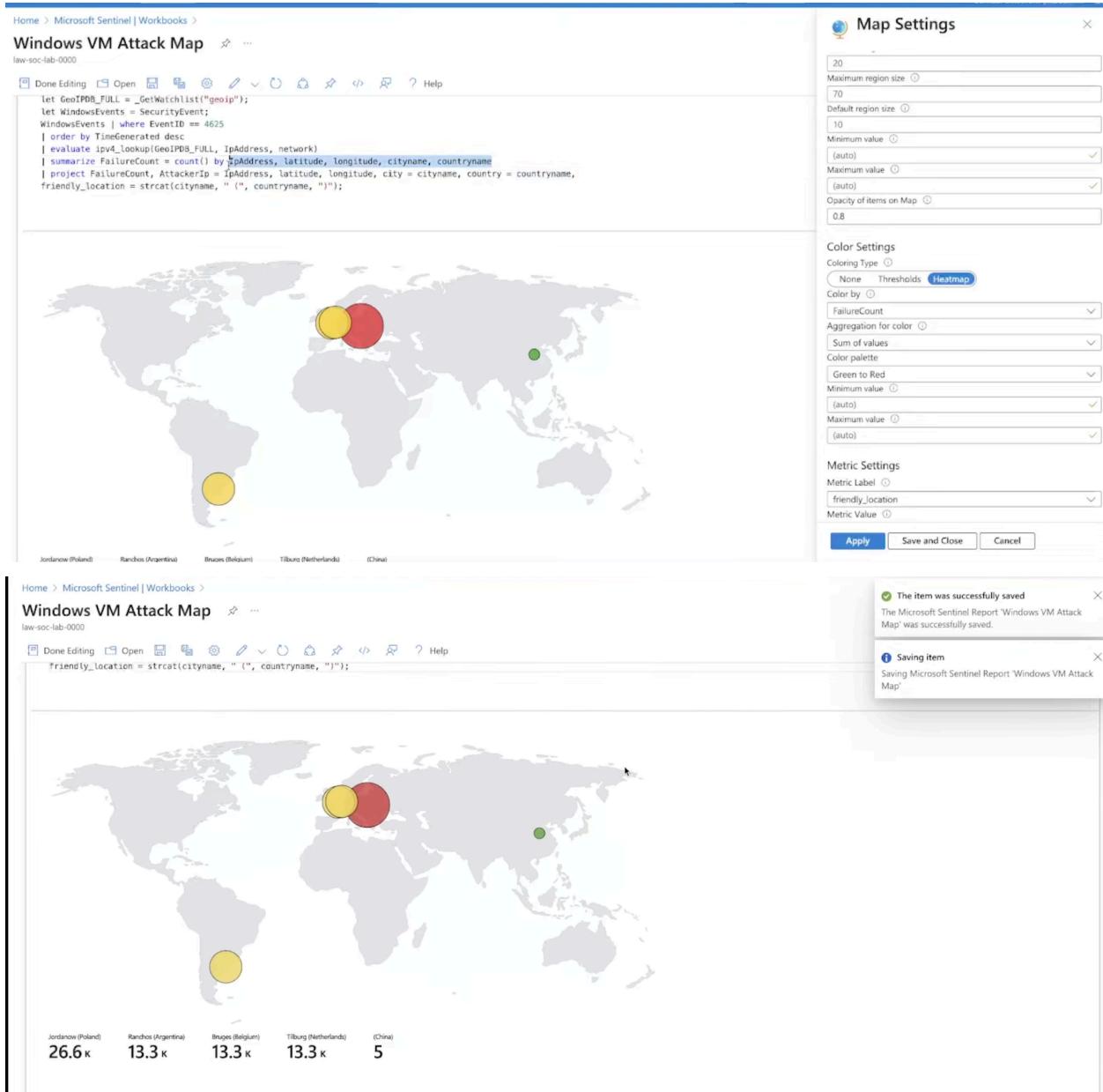
```
1 let GeoIPDB_FULL = _GetWatchlist("geoip");
2 let WindowsEvents = SecurityEvent
3 | where ipAddress == "185.156.73.169"
4 | where EventID == 4625
5 | order by TimeGenerated desc
6 | evaluate ipv4_lookup(GeoIPDB_FULL, IPAddress, network);
7 WindowsEvents
8 | project TimeGenerated, Computer, IPAddress, cityname, countryname, latitude, longitude
```

Results Chart

TimeGenerated [UTC] ↑	Computer	IPAddress	cityname	countryname	latitude	longitude
2/14/2025, 7:56:19.971 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:19.770 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:19.573 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:19.370 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:19.163 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:18.937 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:18.722 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:18.527 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:18.333 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:18.134 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:17.932 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:17.696 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367
2/14/2025, 7:56:17.486 AM	CORP-NET-EAST-1	185.156.73.169	Jordanow	Poland	49.6459	19.8367

2s 242ms | Display time (UTC+00:00) Query details | 1 - 13 of 11933

- **Dashboard Development:** Created a custom Microsoft Sentinel Workbook. I used KQL to join live logs with the Watchlist data, generating a dynamic **Global Heat Map** that visualized attack origins by latitude and longitude.



## 4. Key Results & Findings

- **Real-world Exposure:** Within minutes of disabling the firewall, the honeypot began receiving hundreds of brute-force RDP attempts from various international IP addresses.
  - **Data Insights:** Identified top-targeted usernames (e.g., "Administrator", "User") and identified high-frequency attack origins (e.g., specific regions in Russia, China, and Brazil).
  - **SIEM Proficiency:** Successfully demonstrated the ability to manage the full data lifecycle: Collection → Processing → Analysis → Visualization.
- 

## 5. Technical Skills Demonstrated

- **Cloud Platforms:** Microsoft Azure (VNets, NSGs, Resource Groups, VMs).
- **SIEM/Log Management:** Microsoft Sentinel, Log Analytics Workspaces.
- **Languages:** Kusto Query Language (KQL).
- **Security Concepts:** Honeypot Architecture, Log Analysis (Event ID 4625), Threat Intelligence, Geo-location Mapping.