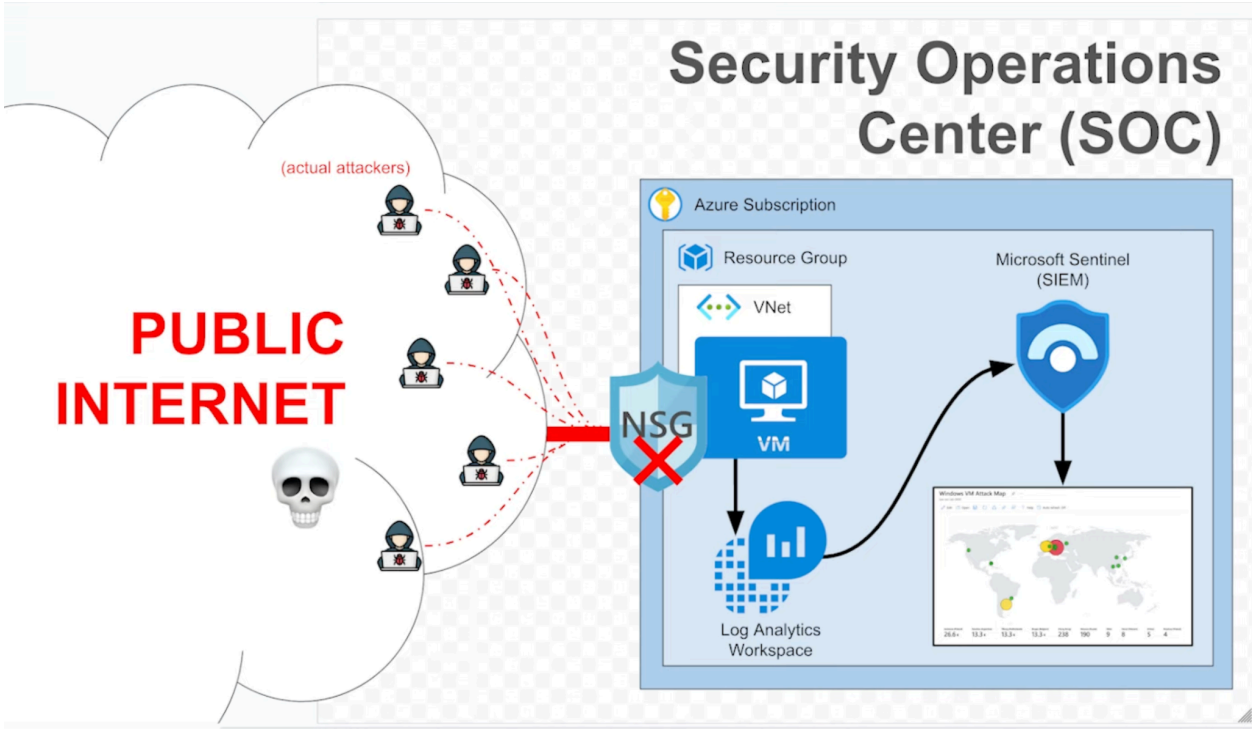
Azure - Live Threat Detection & Geo-Mapping SIEM Lab



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:

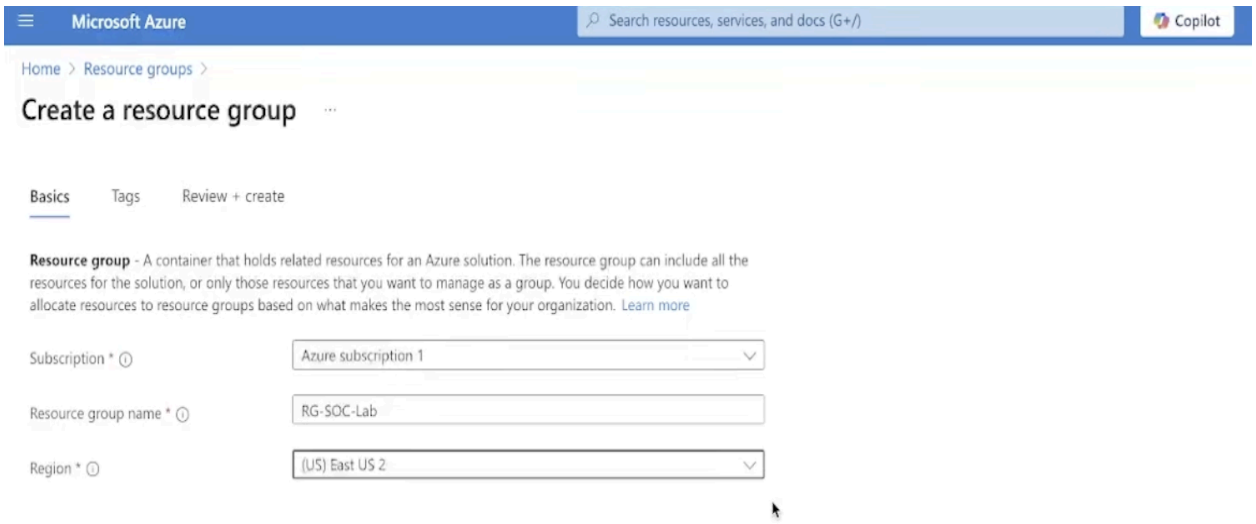
- **Target Asset:** Windows 10 Pro Virtual Machine.
- **Security Stack:** Microsoft Sentinel (SIEM) + Log Analytics Workspace (LAW).
- **Log Ingestion:** Azure Monitor Agent (AMA) via Data Collection Rules (DCR).
- **Intelligence:** Custom Geo-IP Watchlist for threat enrichment.

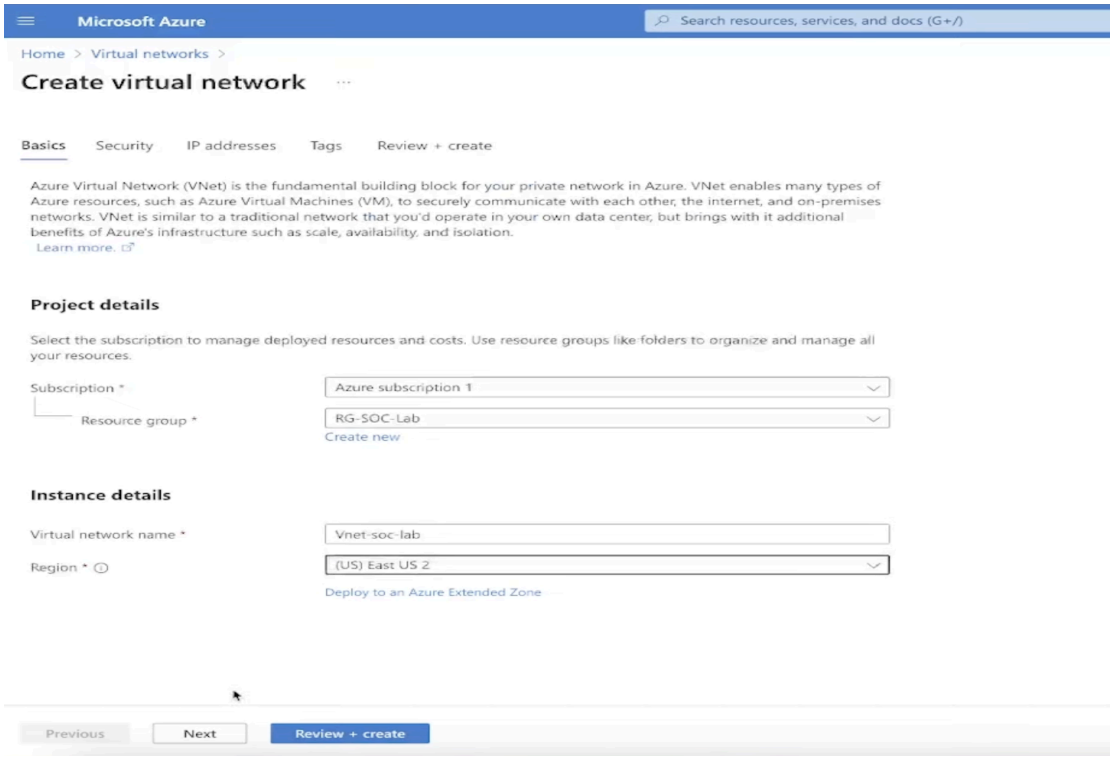
3. Implementation Phases

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.





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.

Home > Virtual machines >

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

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 *

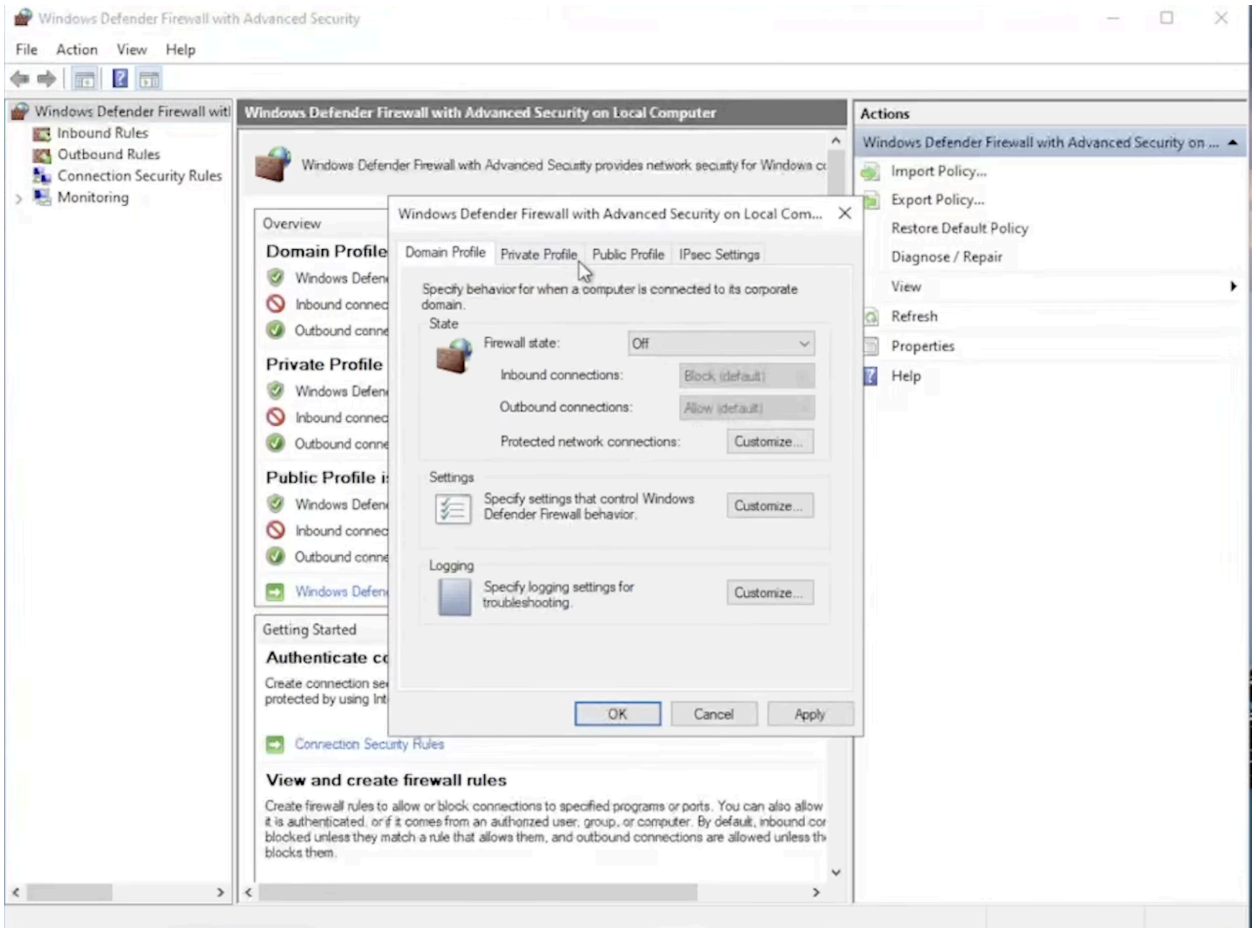
100

Name *

AllowAnyCustom8080Inbound

Description

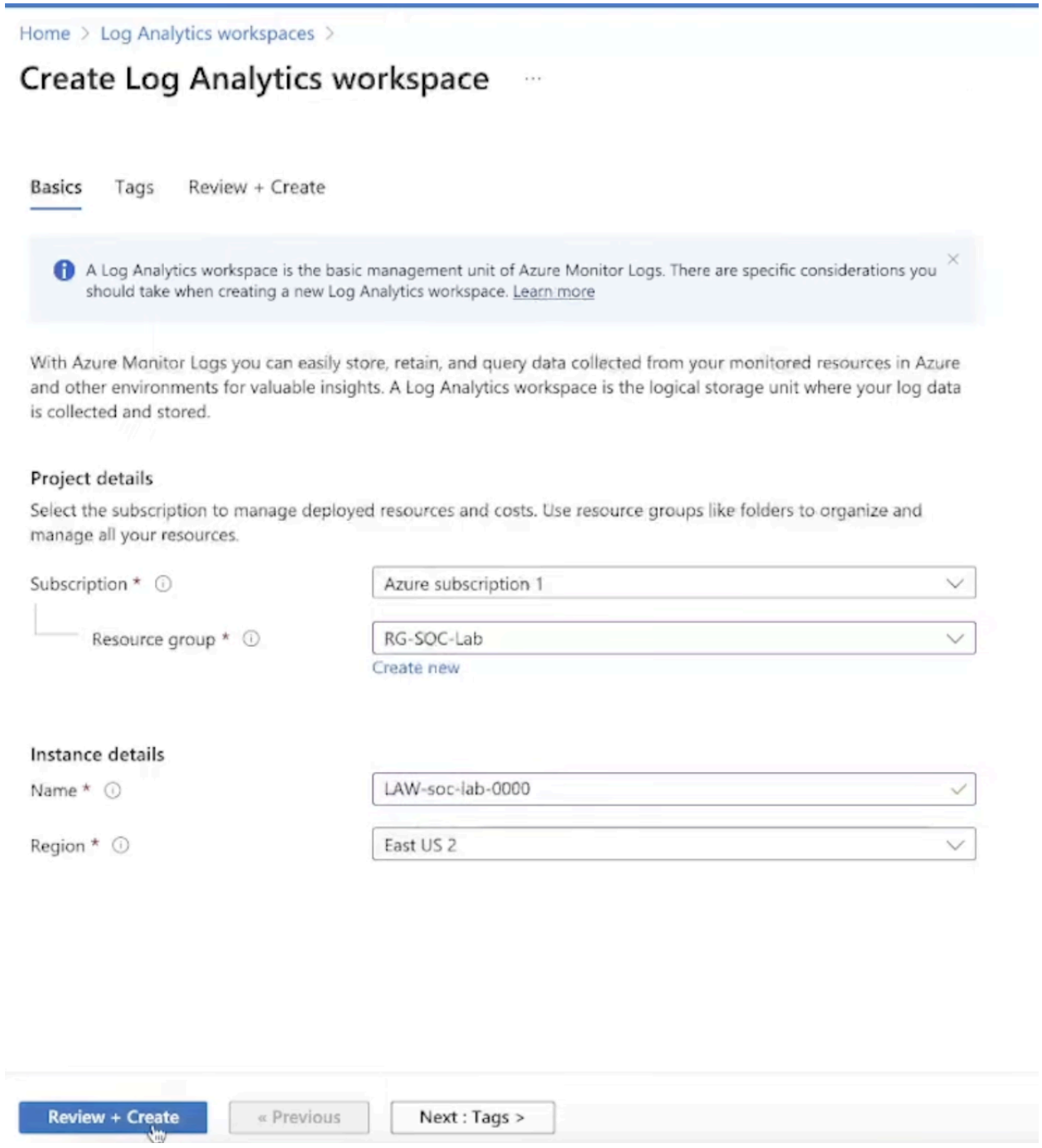
Add | Cancel | Give feedback

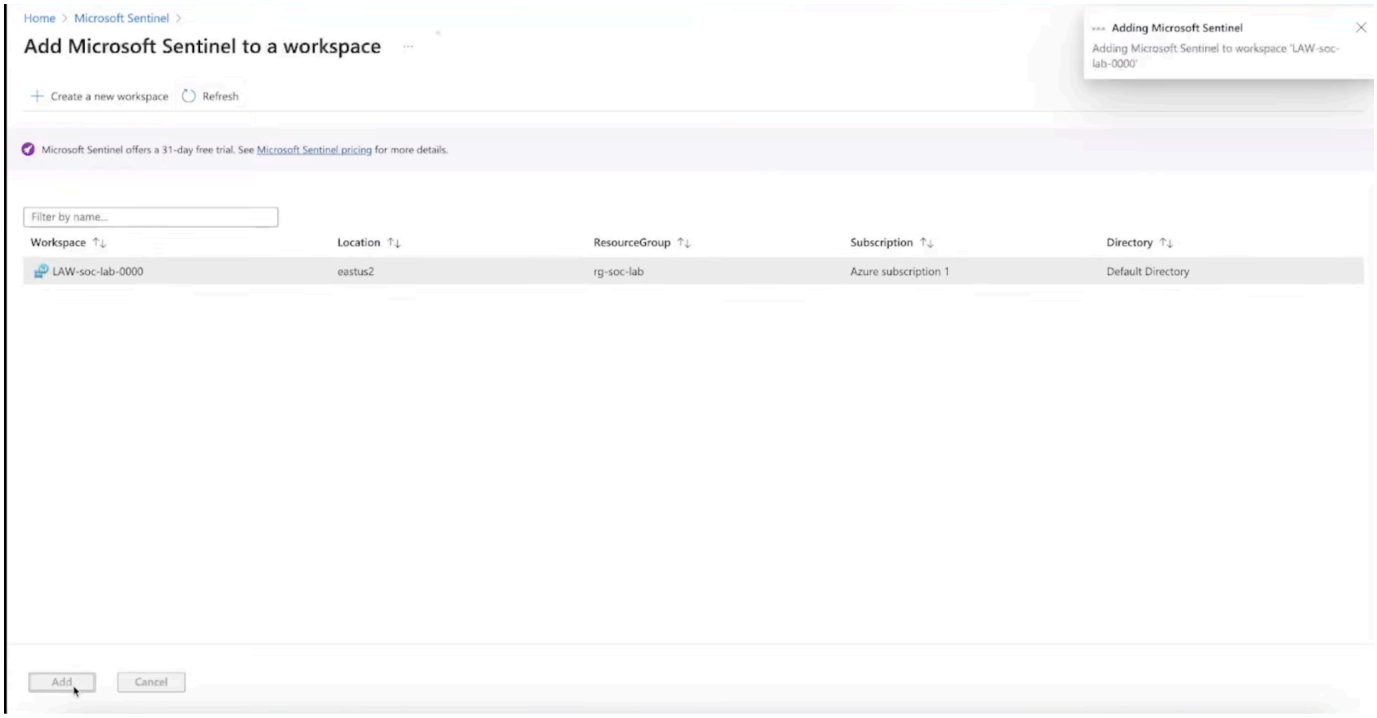


Phase III: SIEM & Log Analytics Configuration

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.

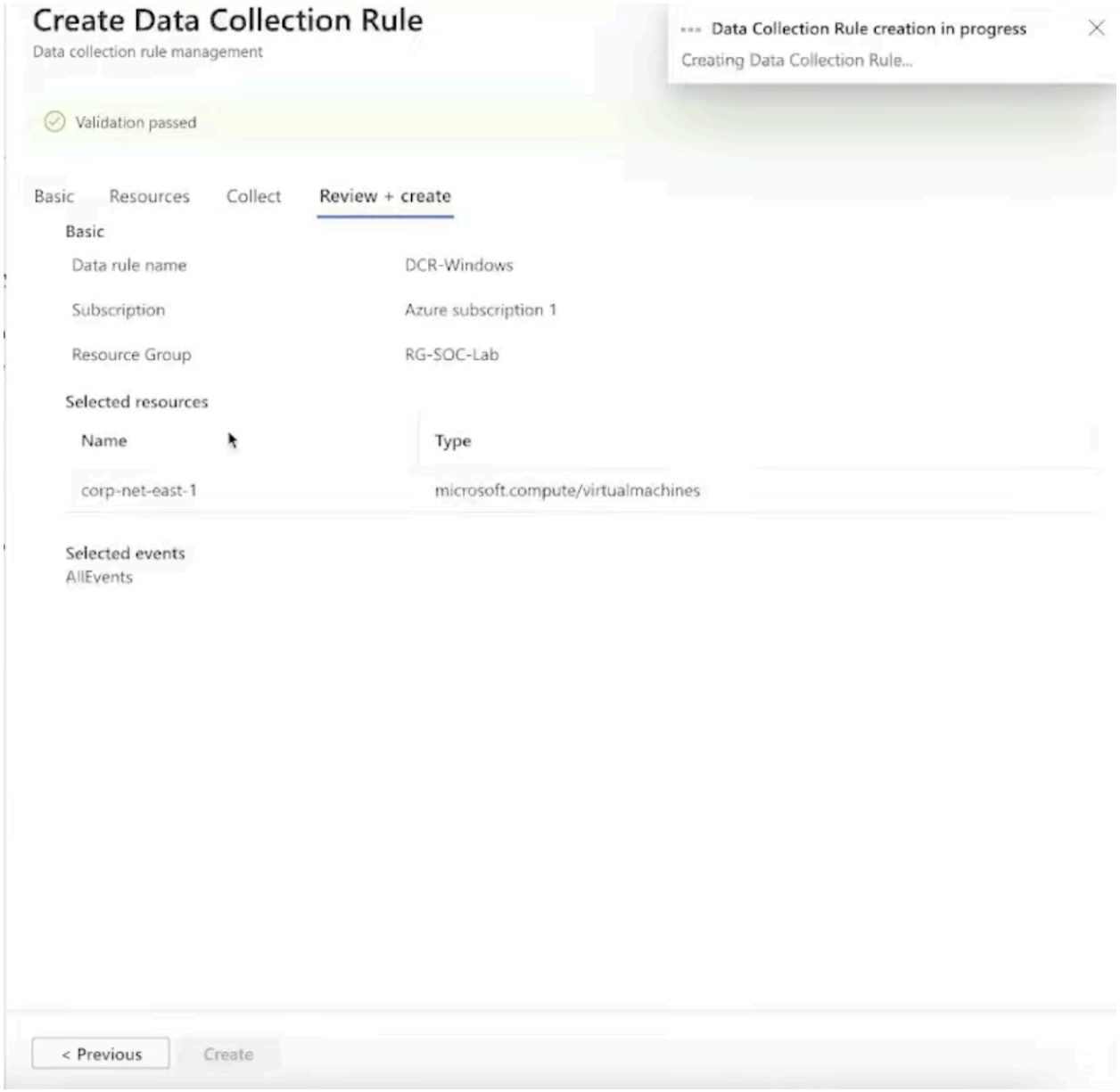

Home > Log Analytics workspaces >
Create Log Analytics workspace ...
Basics
Tags
Review + Create
A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more
With Azure Monitor Logs 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 >

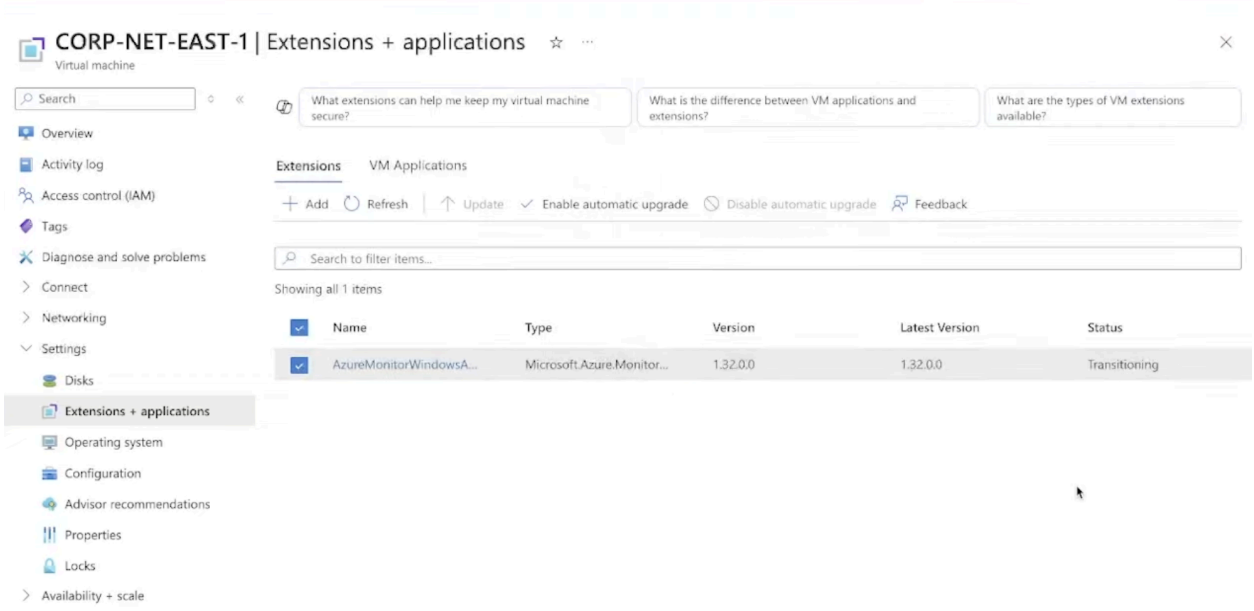


Phase IV: Data Ingestion & Agent Deployment

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.

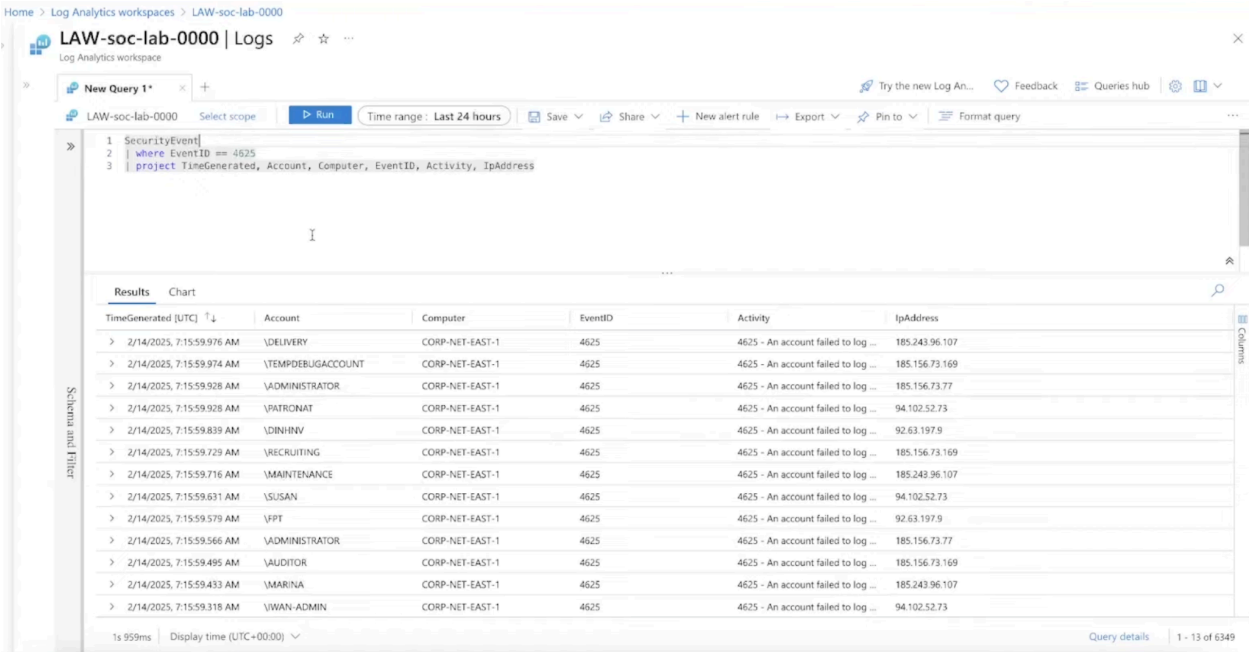

Create Data Collection Rule
Data collection rule management
Data Collection Rule creation in progress
Creating Data Collection Rule...
Validation passed
Basic
Resources
Collect
Review + create
Basic
Data rule name
DCR-Windows
Subscription
Azure subscription 1
Resource Group
RG-SOC-Lab
Selected resources
Name
Type
corp-net-east-1
microsoft.compute/virtualmachines
Selected events
AllEvents
< Previous
Create

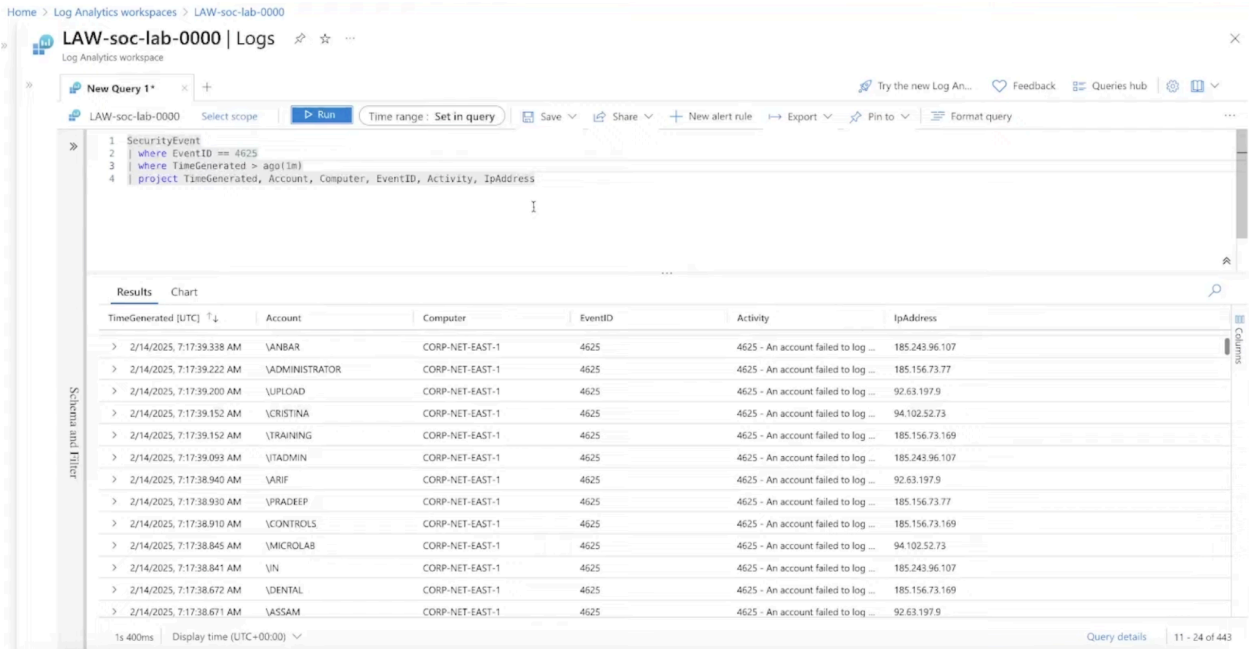


Phase V: Threat Detection & Analysis (KQL)

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.

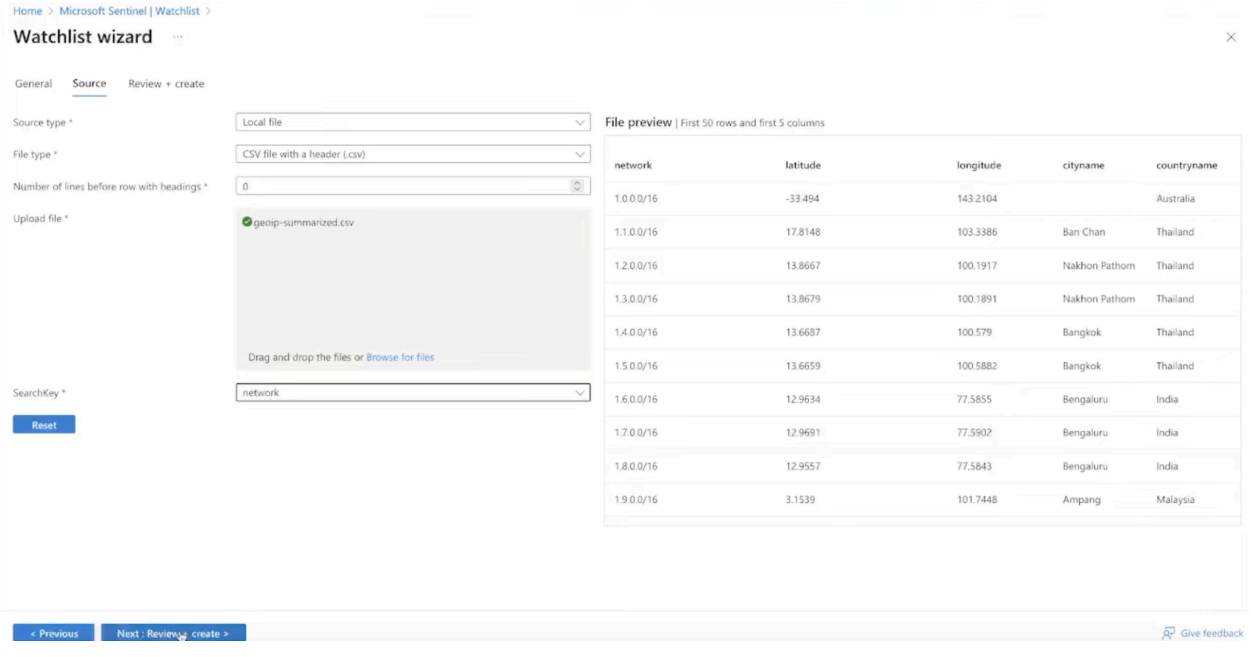


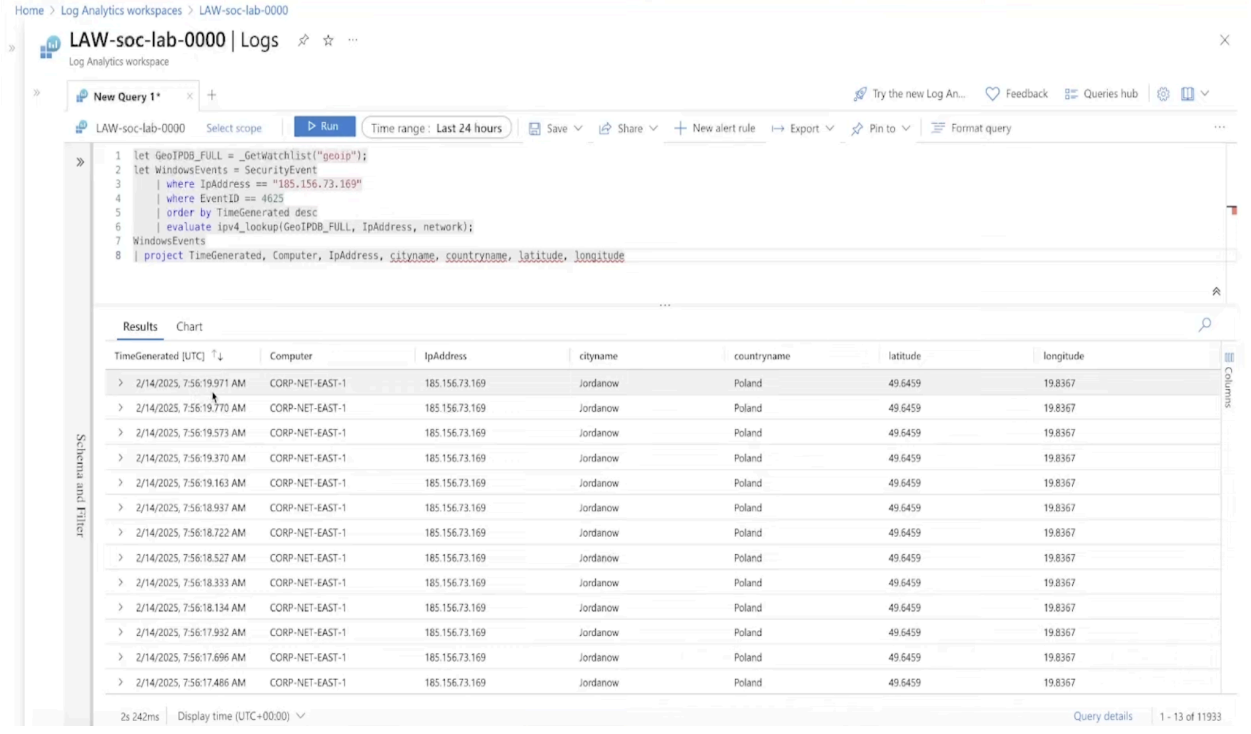


Phase VI: Threat Intelligence Enrichment & Visualization

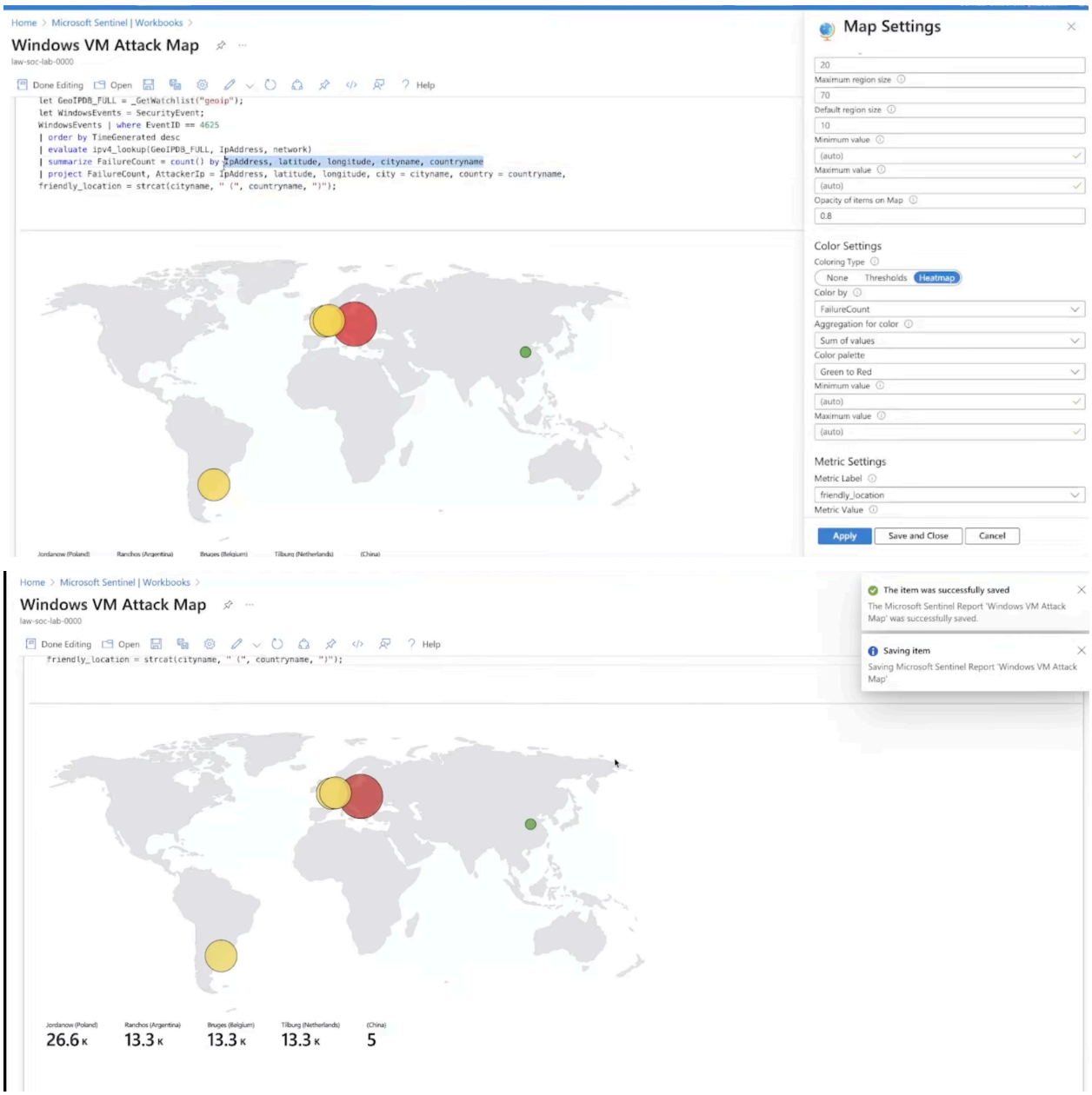
The final phase involved adding context to the data to understand the "Who" and "Where" of the attacks.

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





- **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.