**Azure VM Honeypot Project**

This project demonstrates how to deploy a honeypot in Azure using a Windows 10 Virtual Machine (VM), configure log forwarding and enrichment, and visualise security threats using Microsoft Sentinel.

**Part 1: Creating the Honeypot (Azure Virtual Machine)**

**1. Access the Azure Portal**

* Go to [Azure Portal](https://portal.azure.com) and search for **Virtual Machines**.

**2. Create a Windows 10 Virtual Machine**

* Deploy a new **Windows 10 VM**.
* Select an **appropriate size** based on your requirements.
* Be mindful of **monthly costs** if the VM is left running.
  + **Recommendation:** Shut down the VM when not in use.
* **Important:** Save the **username and password** for future login.

**3. Configure Network Security Group (NSG)**

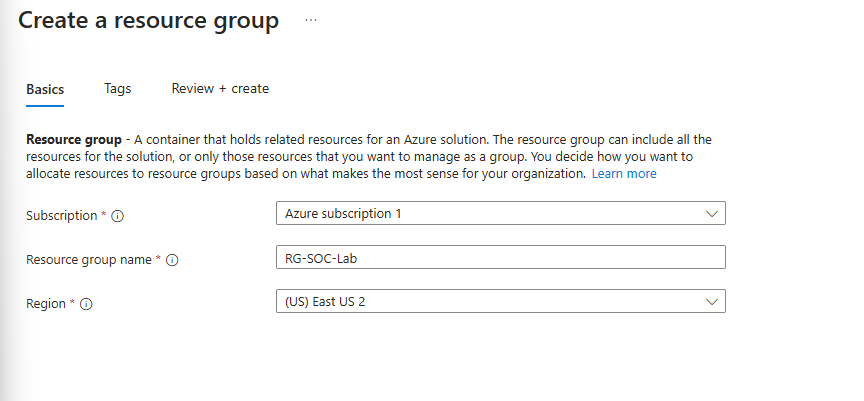
* Locate the **Network Security Group (NSG)** attached to your VM.
* Create an **inbound security rule**:
  + **Allow:** All inbound traffic
  + **Purpose:** Simulates a vulnerable system for honeypot analysis.

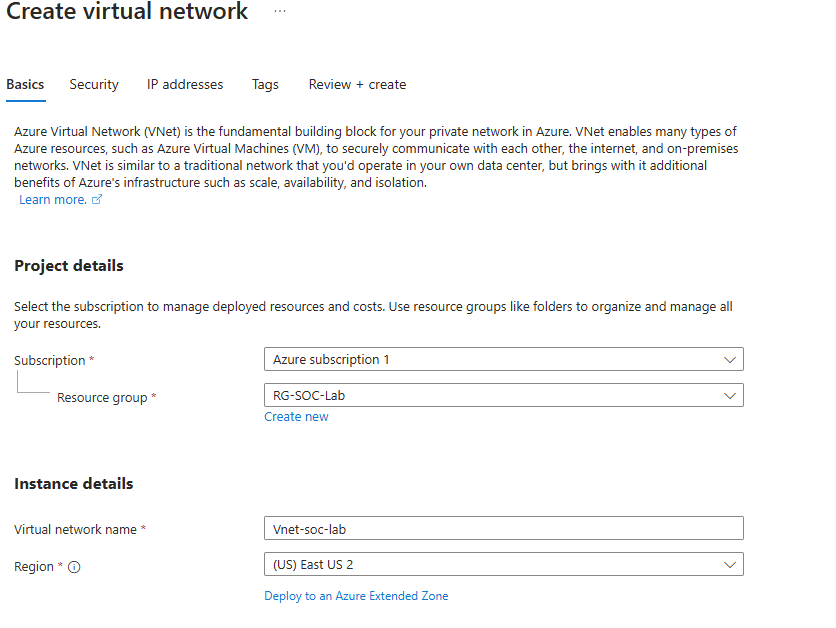
**4. Disable Windows Firewall**

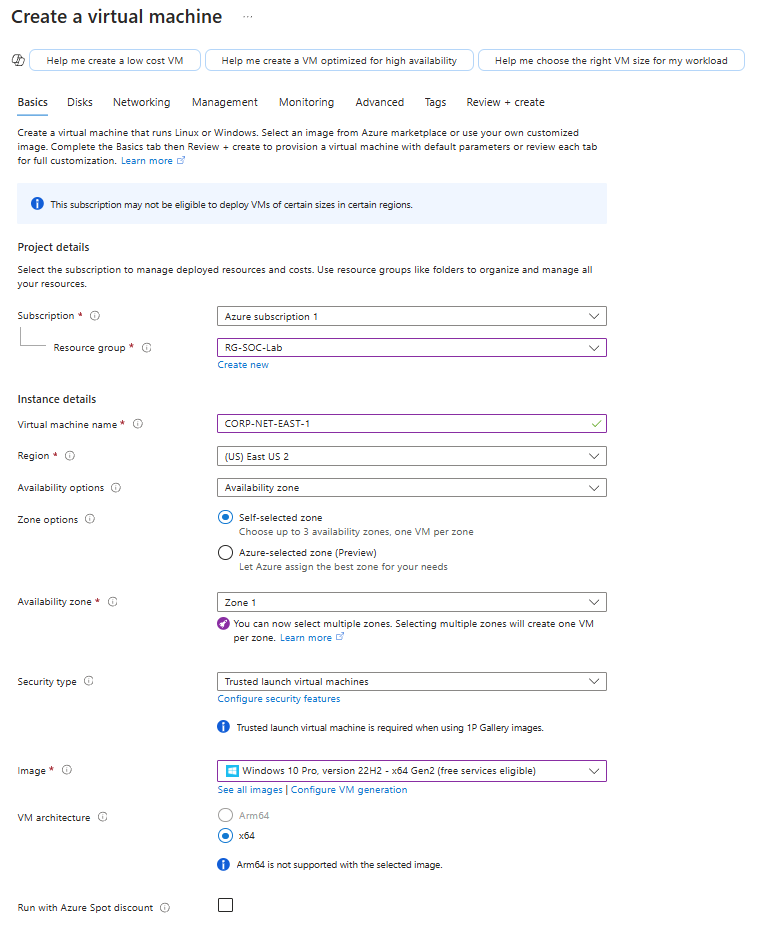
* Log into the **Windows 10 VM**.
* Open **Windows Firewall settings**:

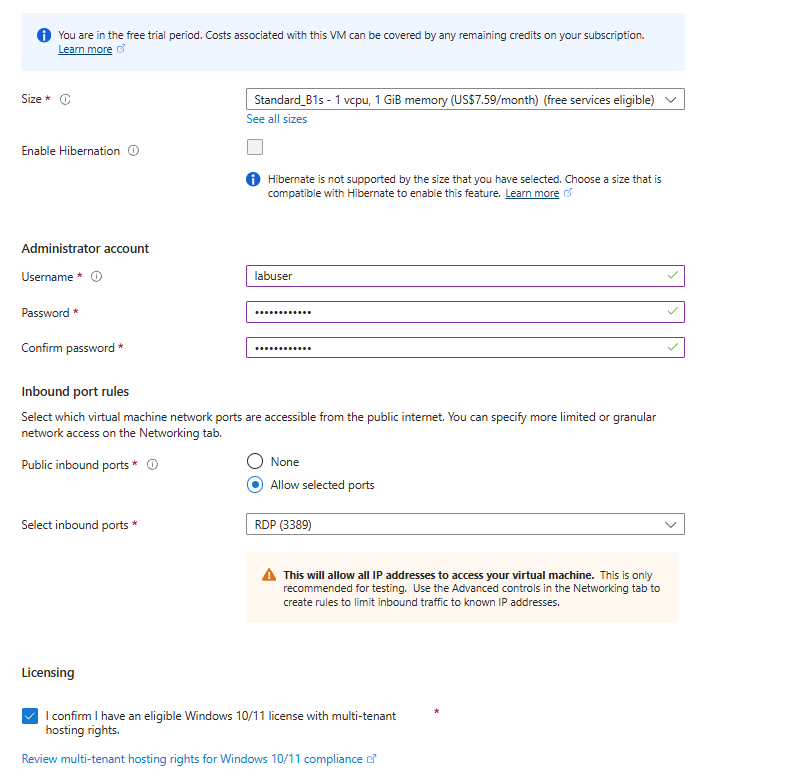
Win + R → Type `wf.msc` → Press Enter

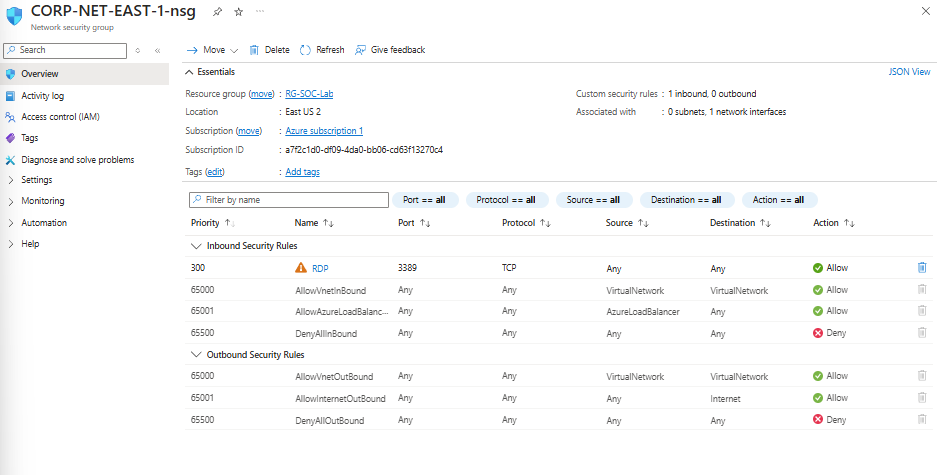
* Click **Properties** and set **Domain, Private, and Public** profiles to **Off**.

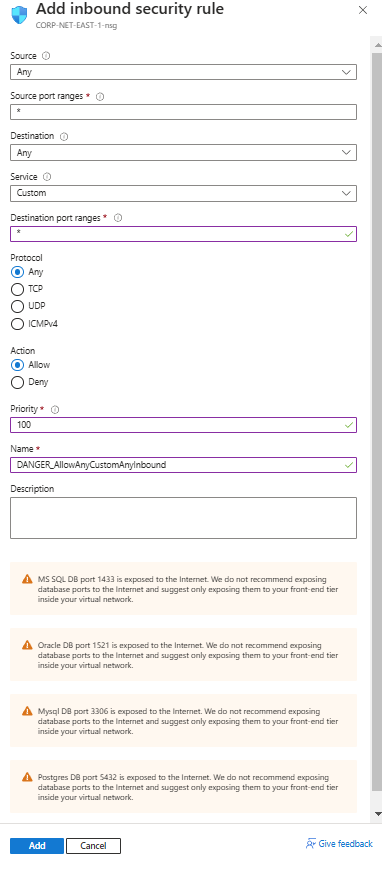


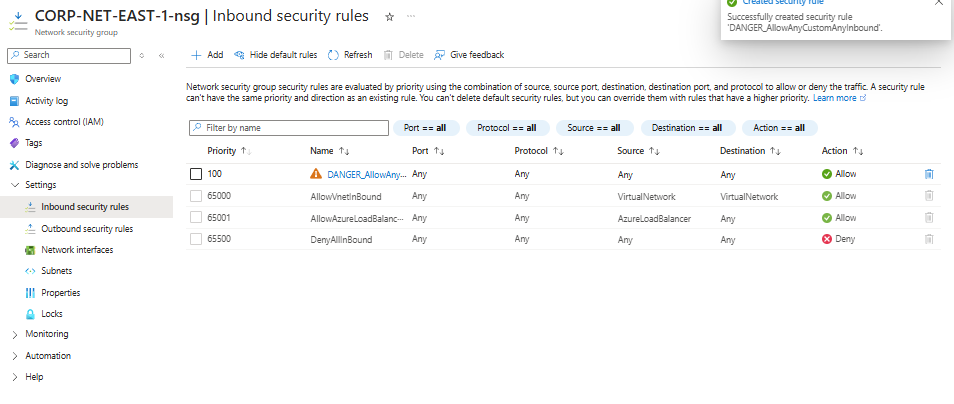


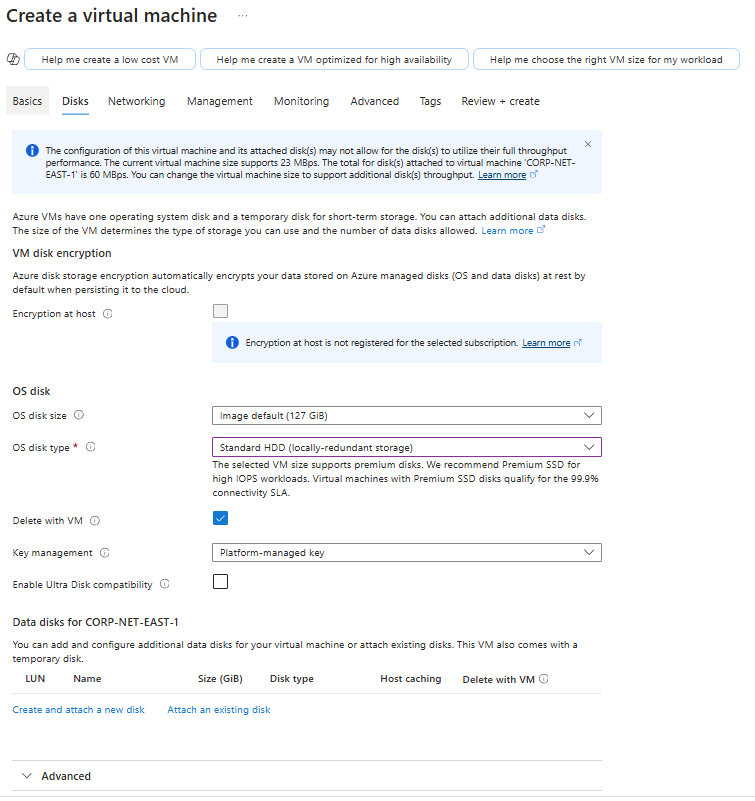


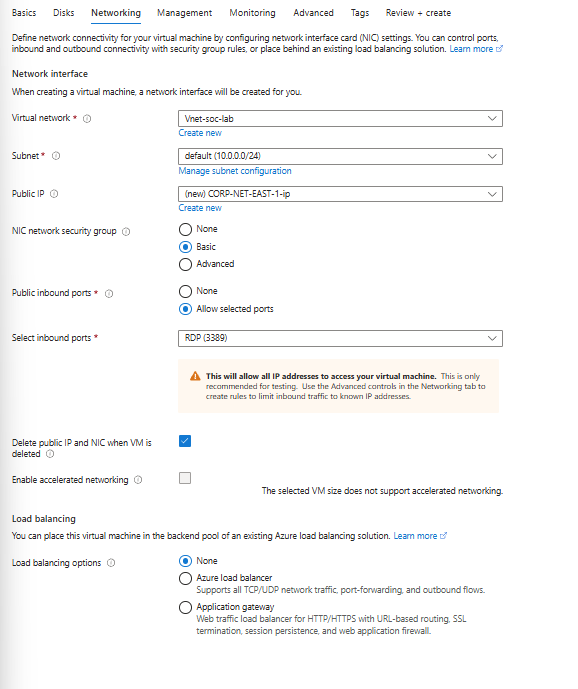


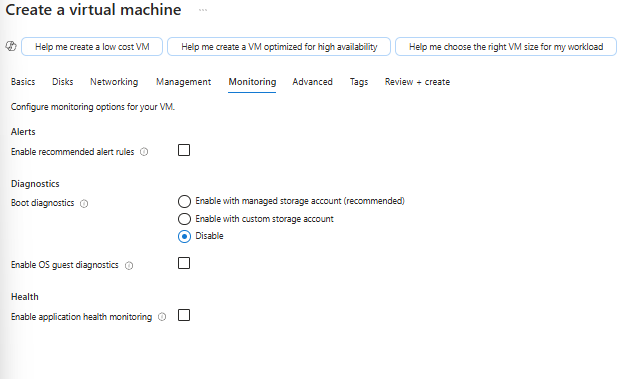


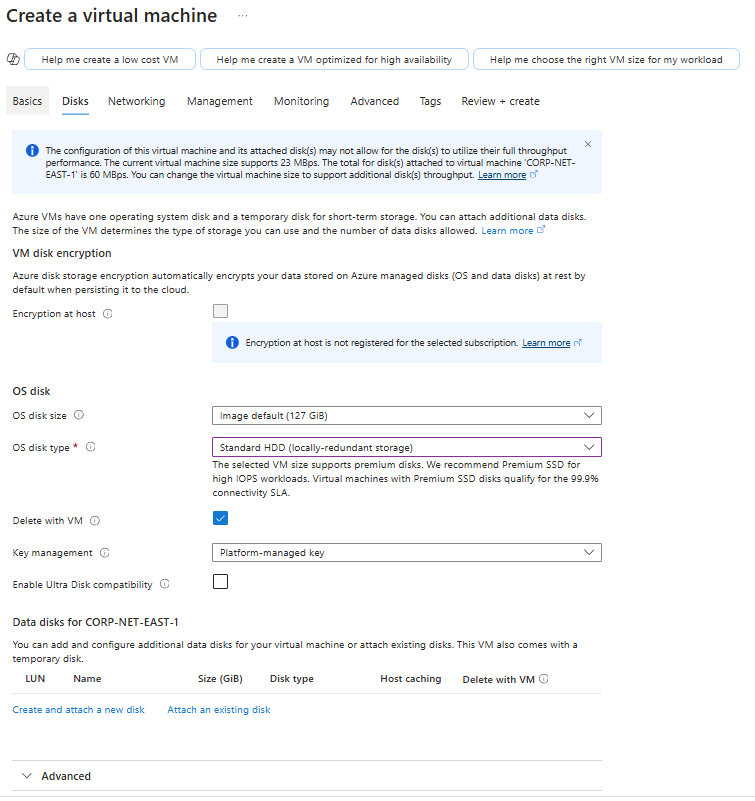


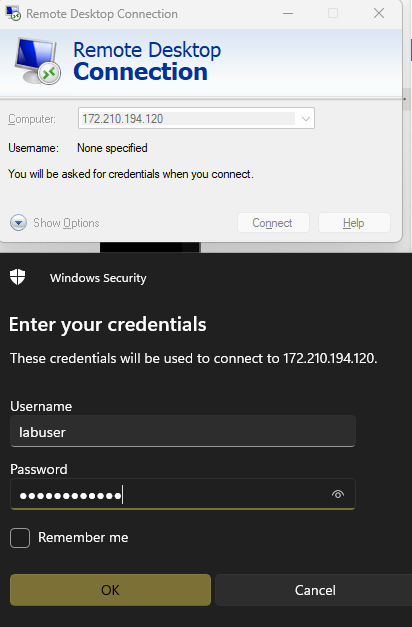


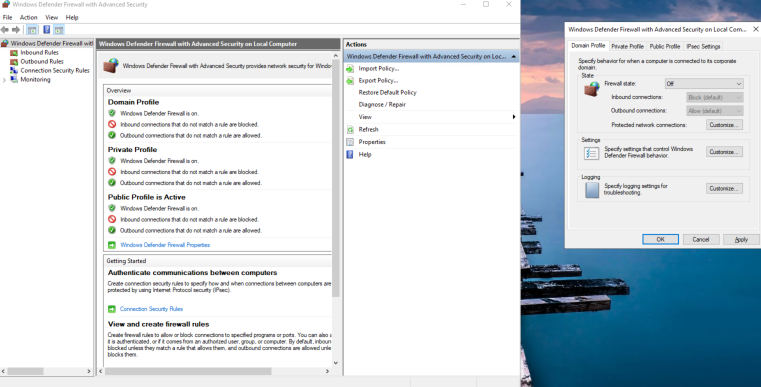


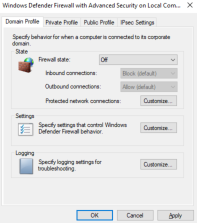


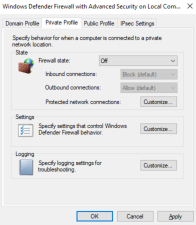


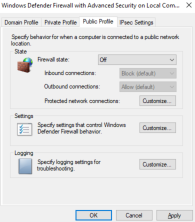


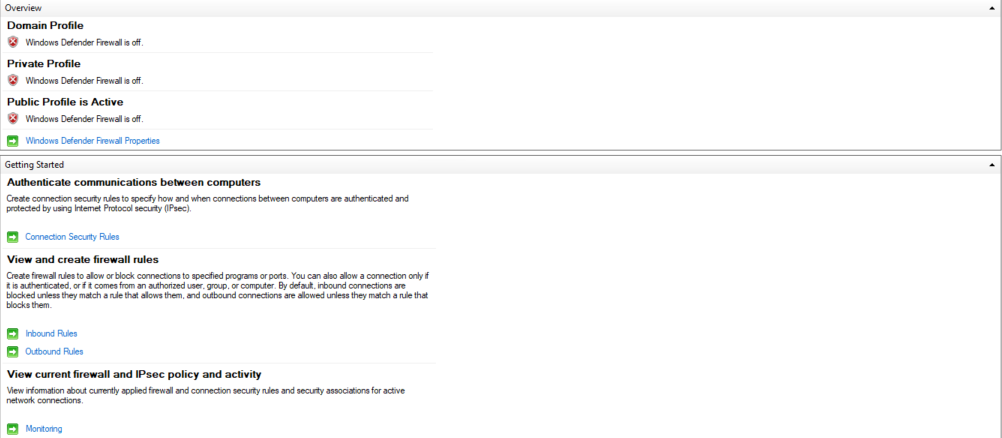


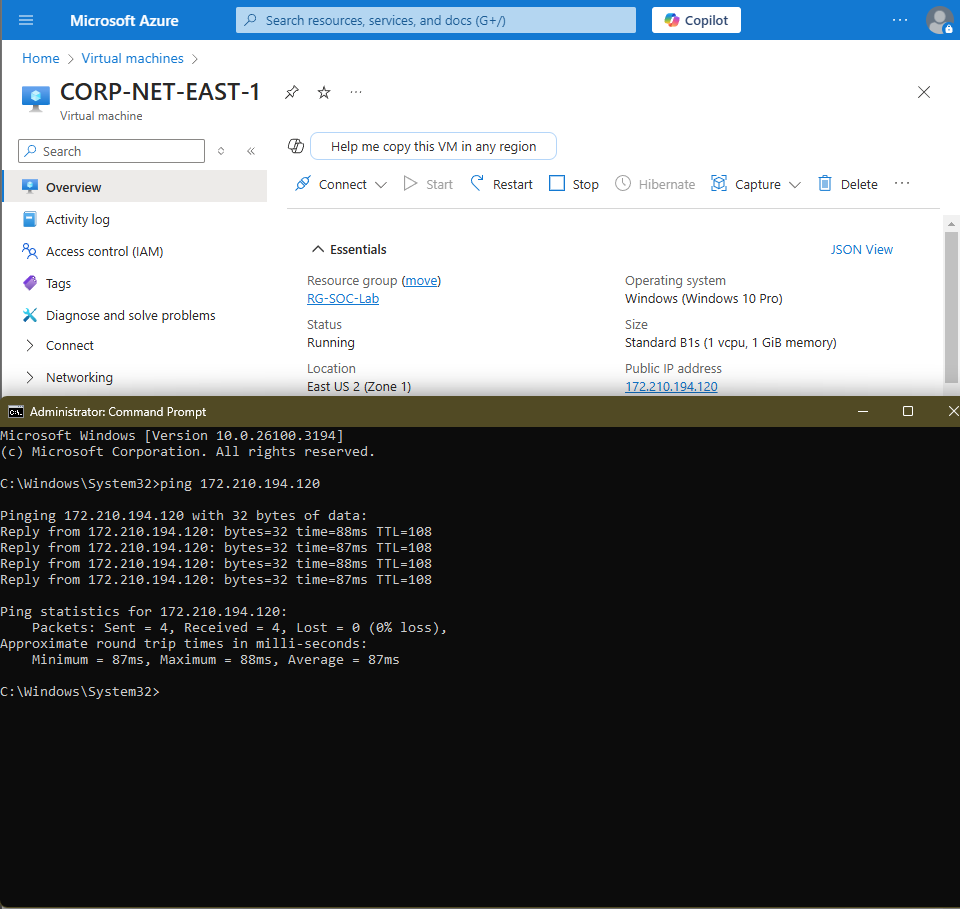












**Part 2: Logging into the VM and Inspecting Logs**

**1. Simulate Failed Logins**

* Attempt to **log in three times** with a non-existent username, e.g., **"employee"**.

**2. Access the Security Logs**

* Log into the **Windows 10 VM**.
* Open **Event Viewer**:

Win + R → Type `eventvwr.msc` → Press Enter

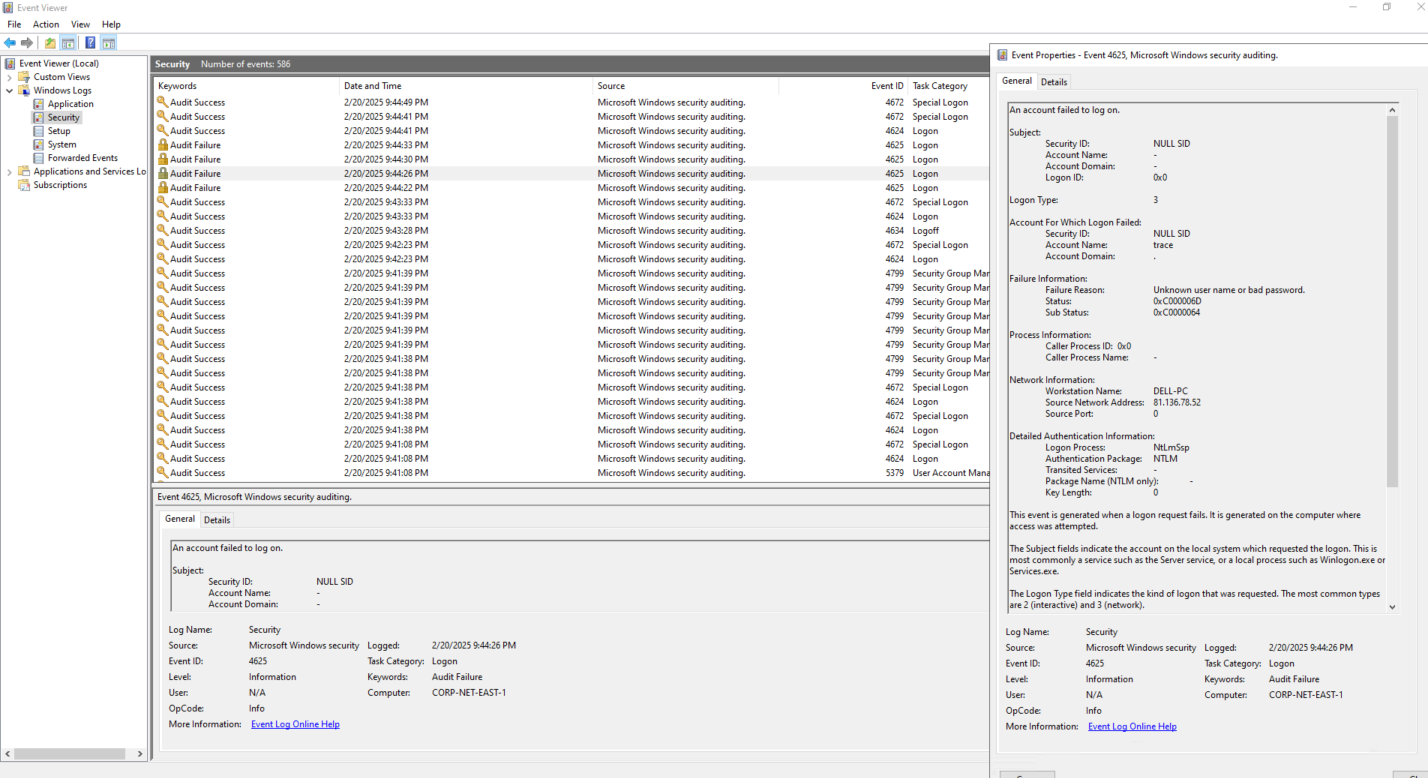
* Navigate to:

Windows Logs → Security

* Locate **three failed login attempts** recorded as **Event ID 4625**.

**3. Set Up Log Collection**

* Next, we will **centralise logs** using **Log Analytics Workspace (LAW)**.



**Part 3: Log Forwarding and KQL**

**1. Create a Log Analytics Workspace (LAW)**

* In **Azure Portal**, navigate to **Log Analytics Workspaces**.
* Create a new **Log Analytics instance**.

**2. Deploy Microsoft Sentinel**

* Set up a **Microsoft Sentinel** instance.
* Connect **Sentinel to your Log Analytics Workspace (LAW)**.
* Observe the **architecture** and data flow between Sentinel and LAW.

**3. Configure Security Event Forwarding**

* Enable the **Windows Security Events via AMA** connector.
* Create a **Data Collection Rule (DCR)** in Sentinel.
* Ensure successful **data extension creation**.

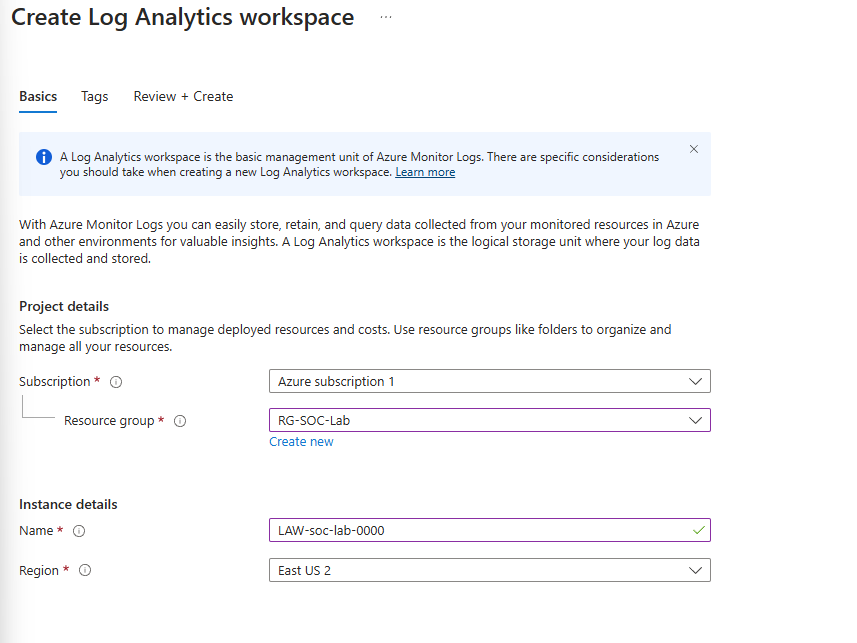
**4. Query Logs in Log Analytics Workspace (LAW)**

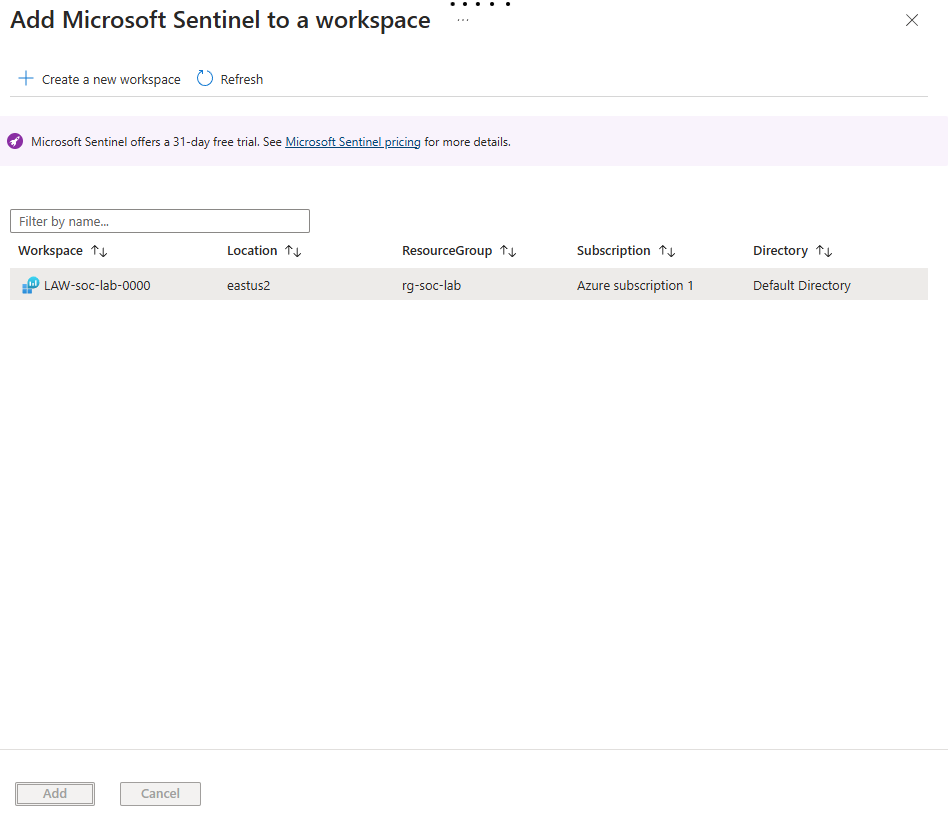
* Run the following **Kusto Query Language (KQL)** command:

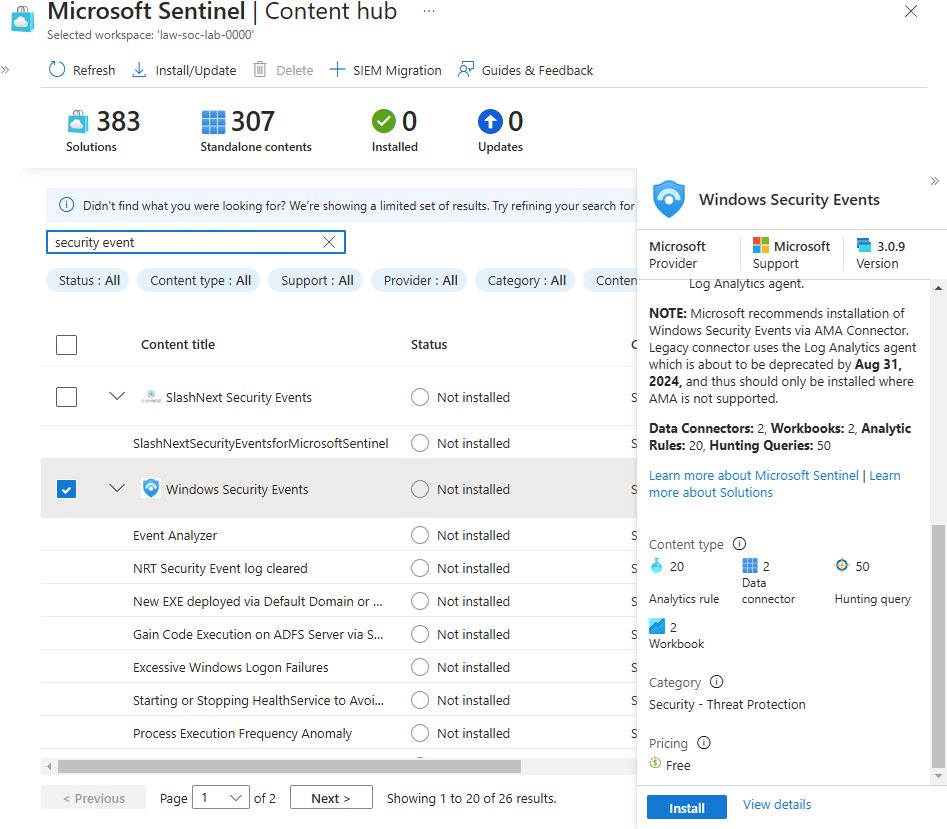
SecurityEvent

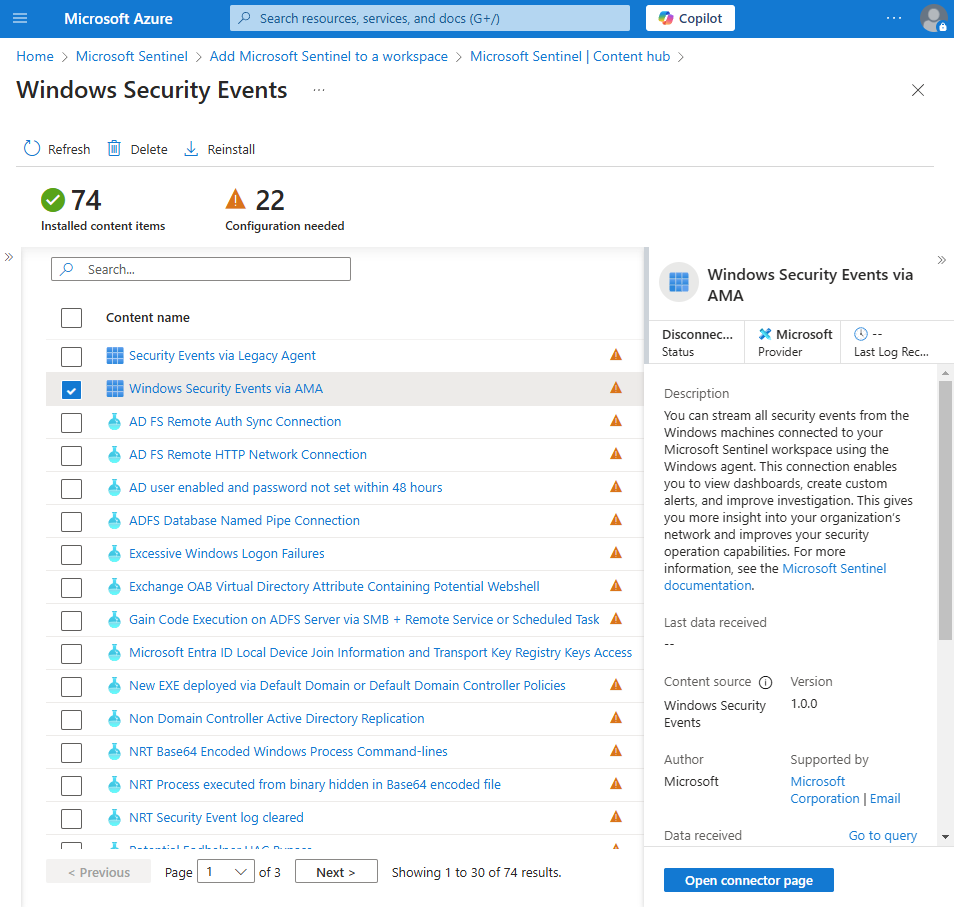
| where EventId == 4625

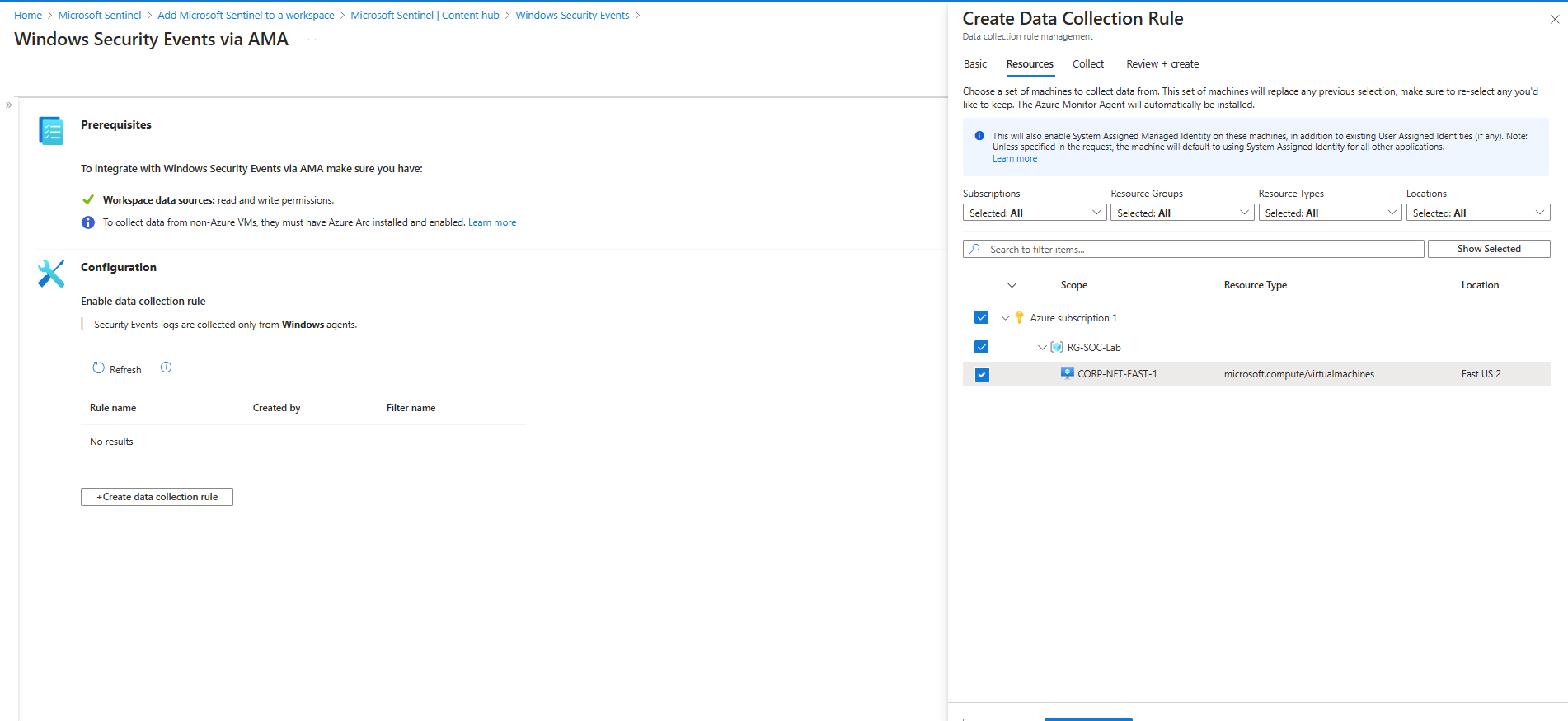
* **Observe:**
  + How logs flow into **Sentinel and LAW**.

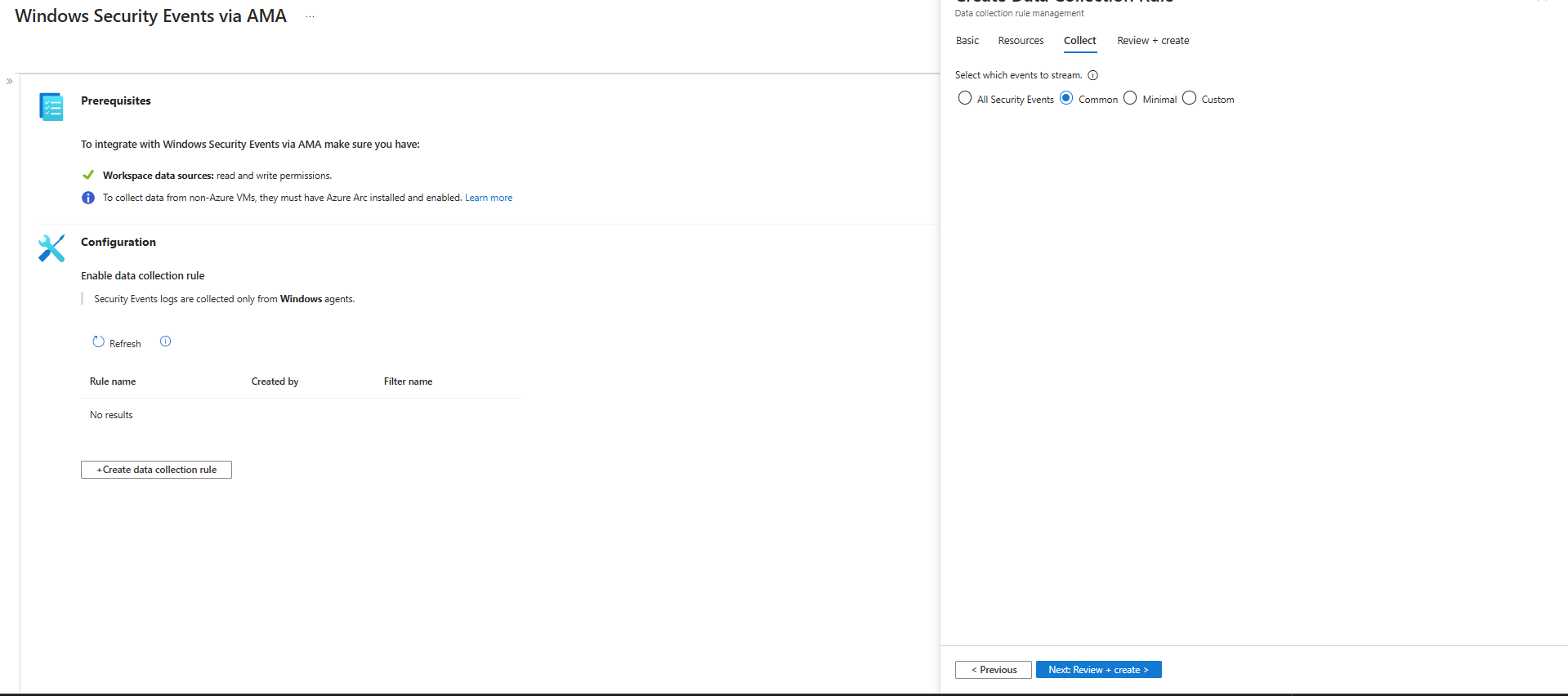


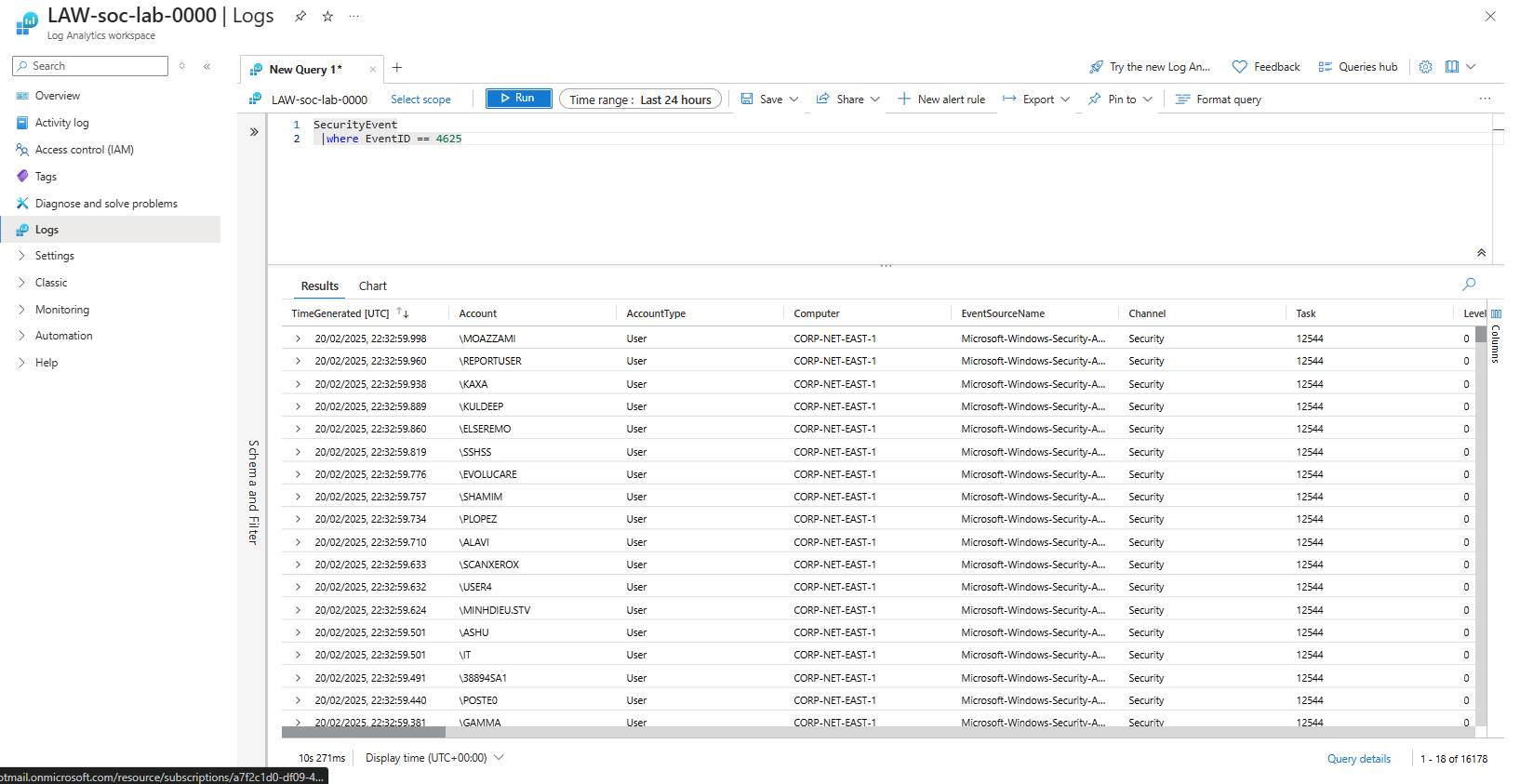


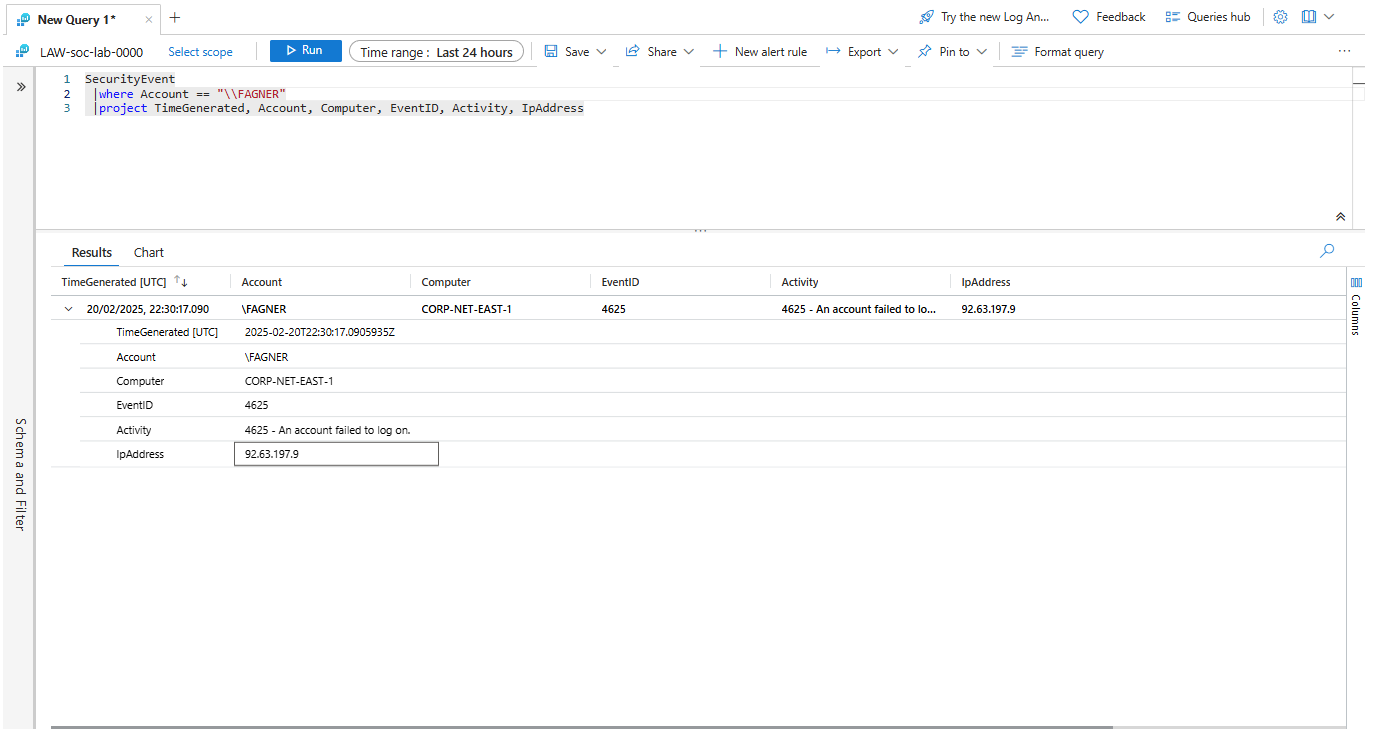


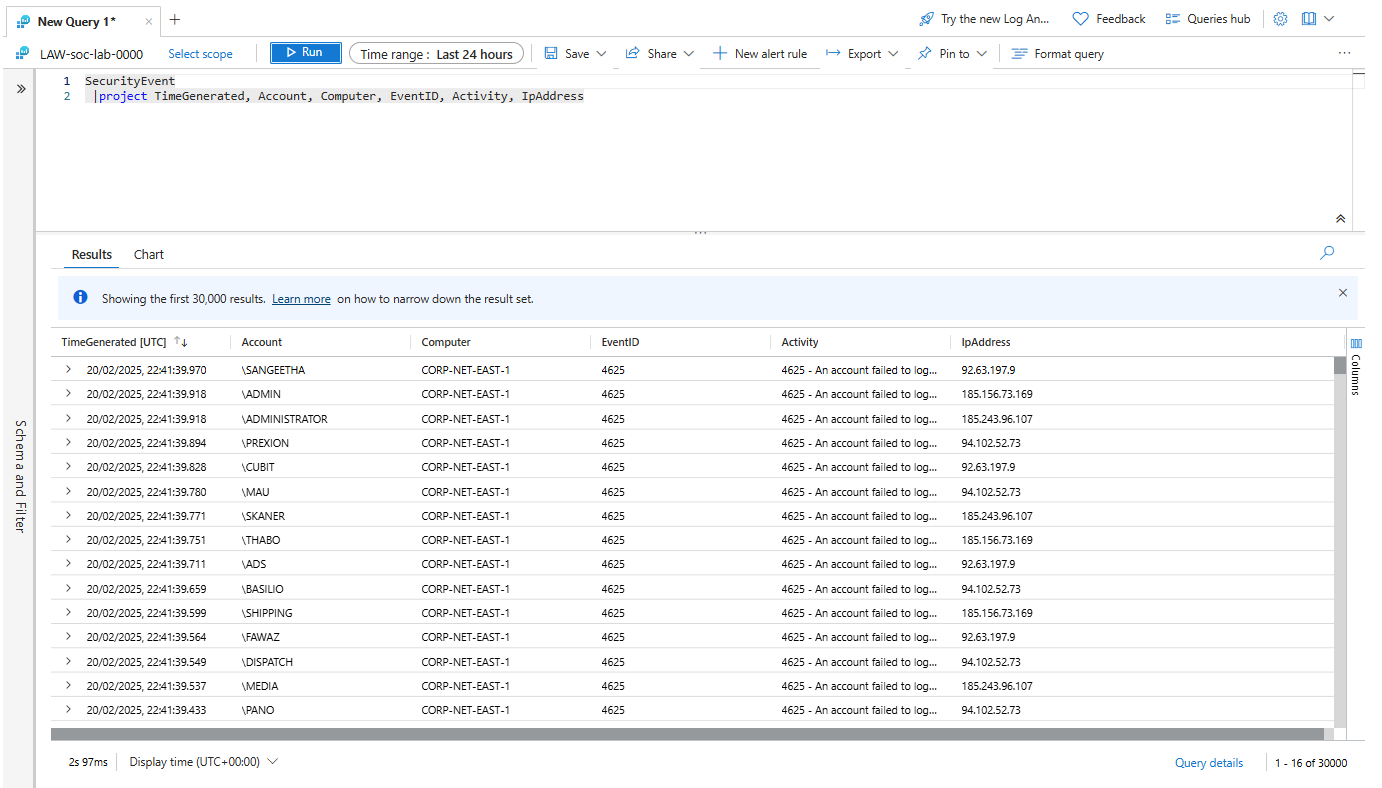


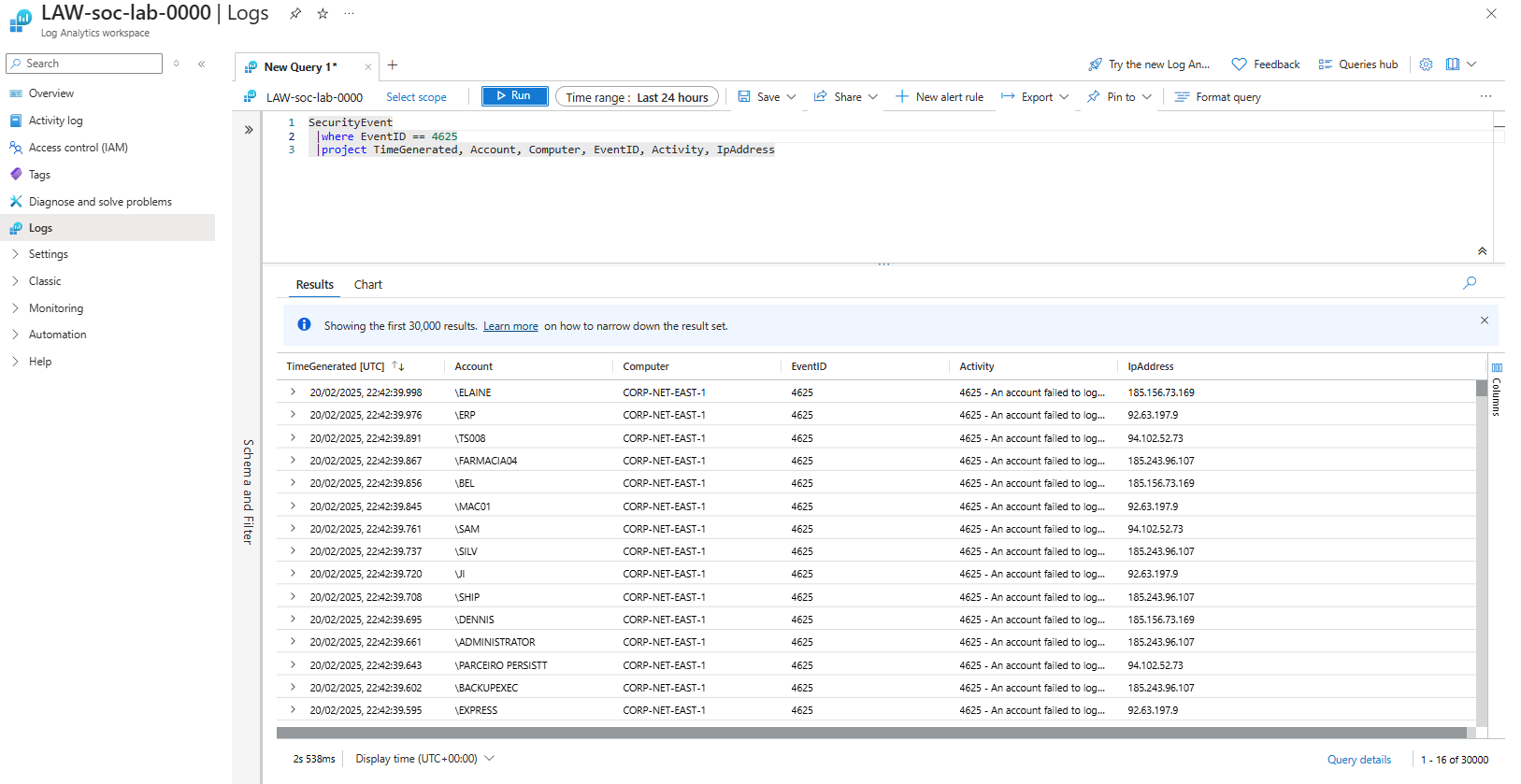












**Part 4: Log Enrichment and Finding Location Data**

**1. Analyse SecurityEvent Logs**

* Review logs in **Log Analytics Workspace (LAW)**.
* Notice that **no location data** is available—only IP addresses.

**2. Import a GeoIP Watchlist**

* **Download the GeoIP database file**:  
  [geoip-summarized.csv](https://drive.google.com/file/d/13EfjM_4BohrmaxqXZLB5VUBIz2sv9Siz/view)
* **Upload it as a Watchlist in Sentinel**:
  + **Name/Alias:** geoip
  + **Source Type:** Local File
  + **Number of Lines Before Row:** 0
  + **Search Key:** network
* **Import complete:** ~54,000 rows.

**3. Understand Real-World Data Sources**

* In real-world scenarios, **location data** comes from:
  + **Live data feeds**
  + **Security providers' backend systems**

**4. Run KQL Query to Identify Attackers' Locations**

kql

CopyEdit

let GeoIPDB\_FULL = \_GetWatchlist("geoip");

let WindowsEvents = SecurityEvent

| where IpAddress == "<attacker IP address>"

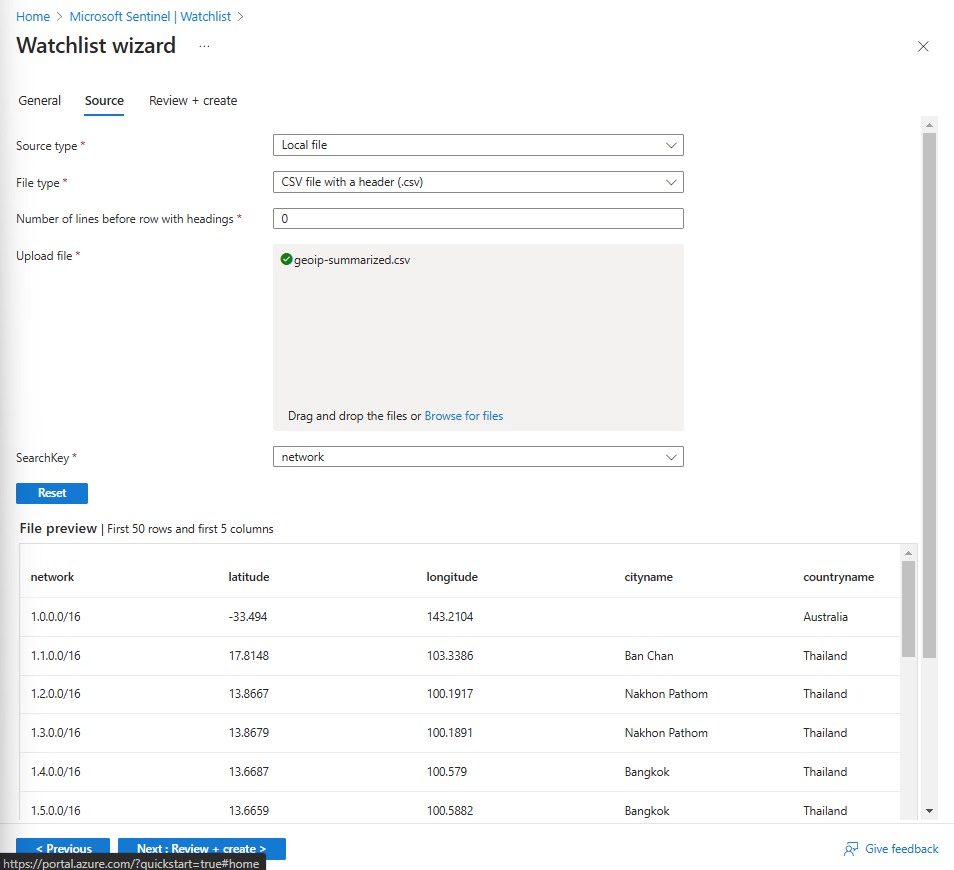
| where EventID == 4625

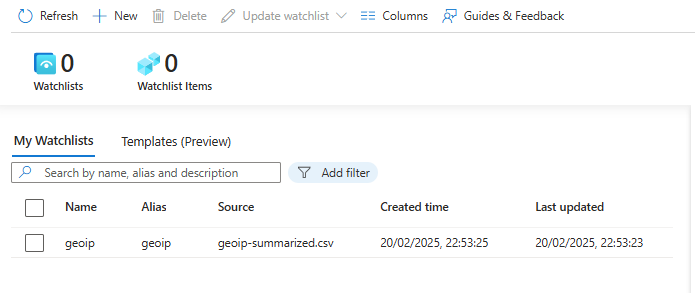
| order by TimeGenerated desc

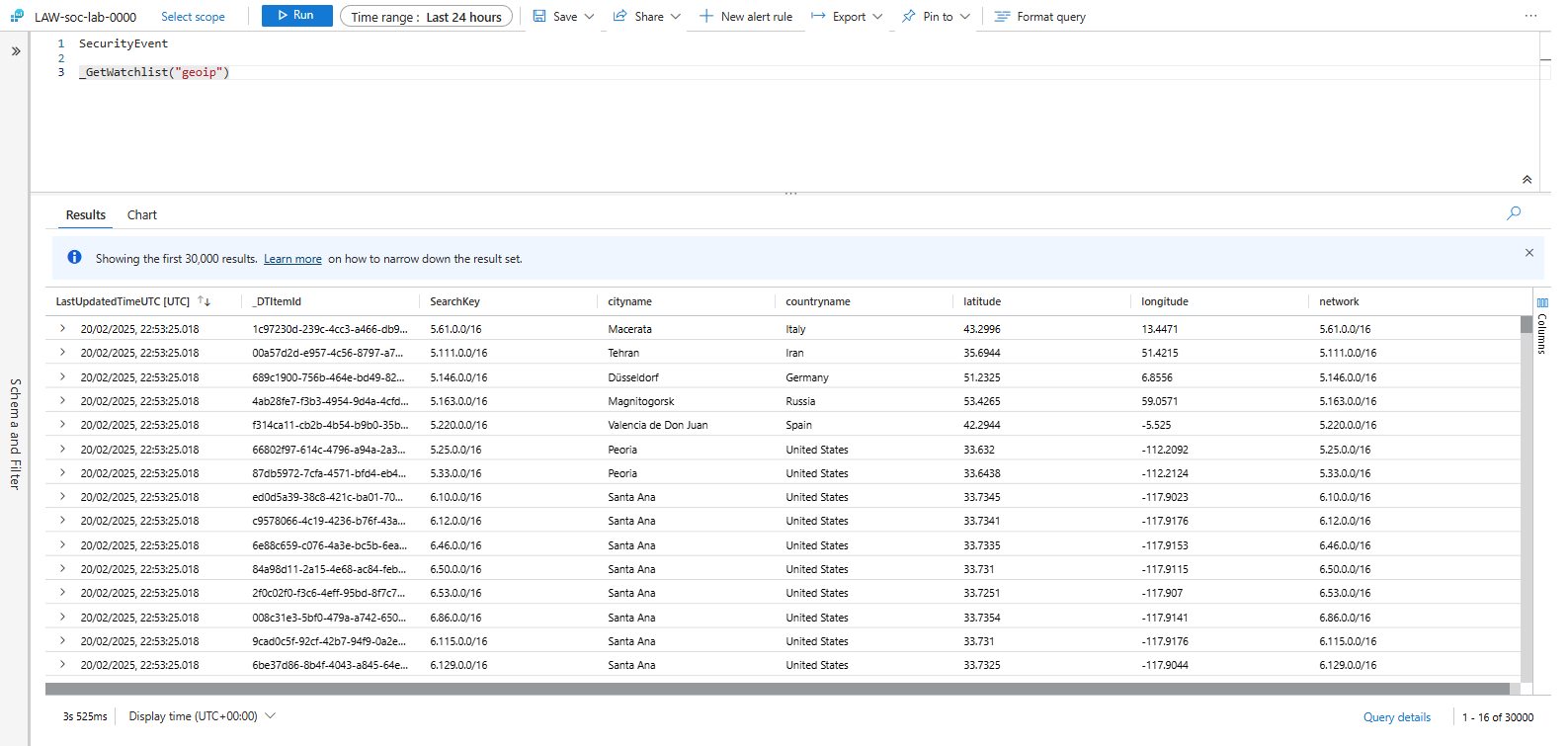
| evaluate ipv4\_lookup(GeoIPDB\_FULL, IpAddress, network);

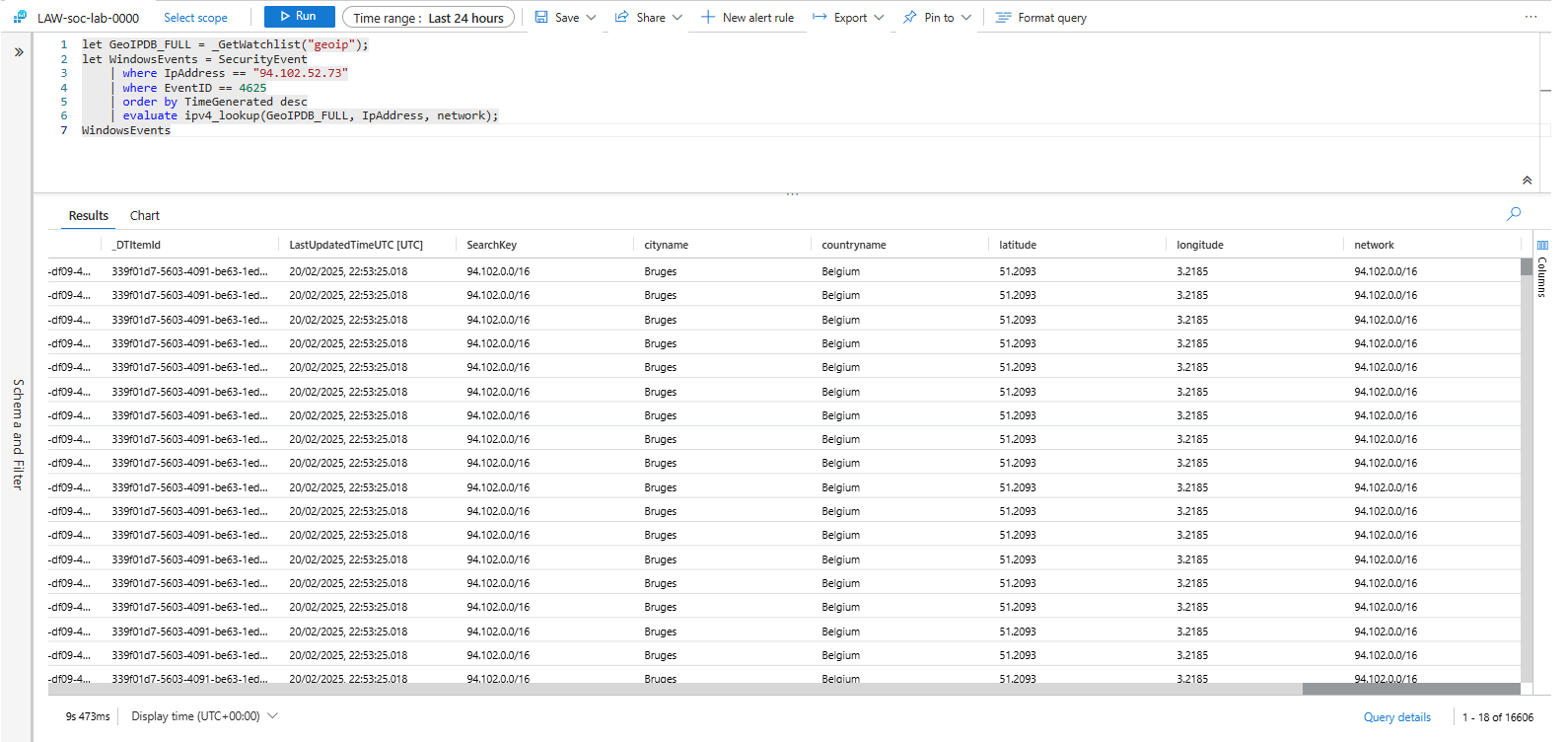
WindowsEvents

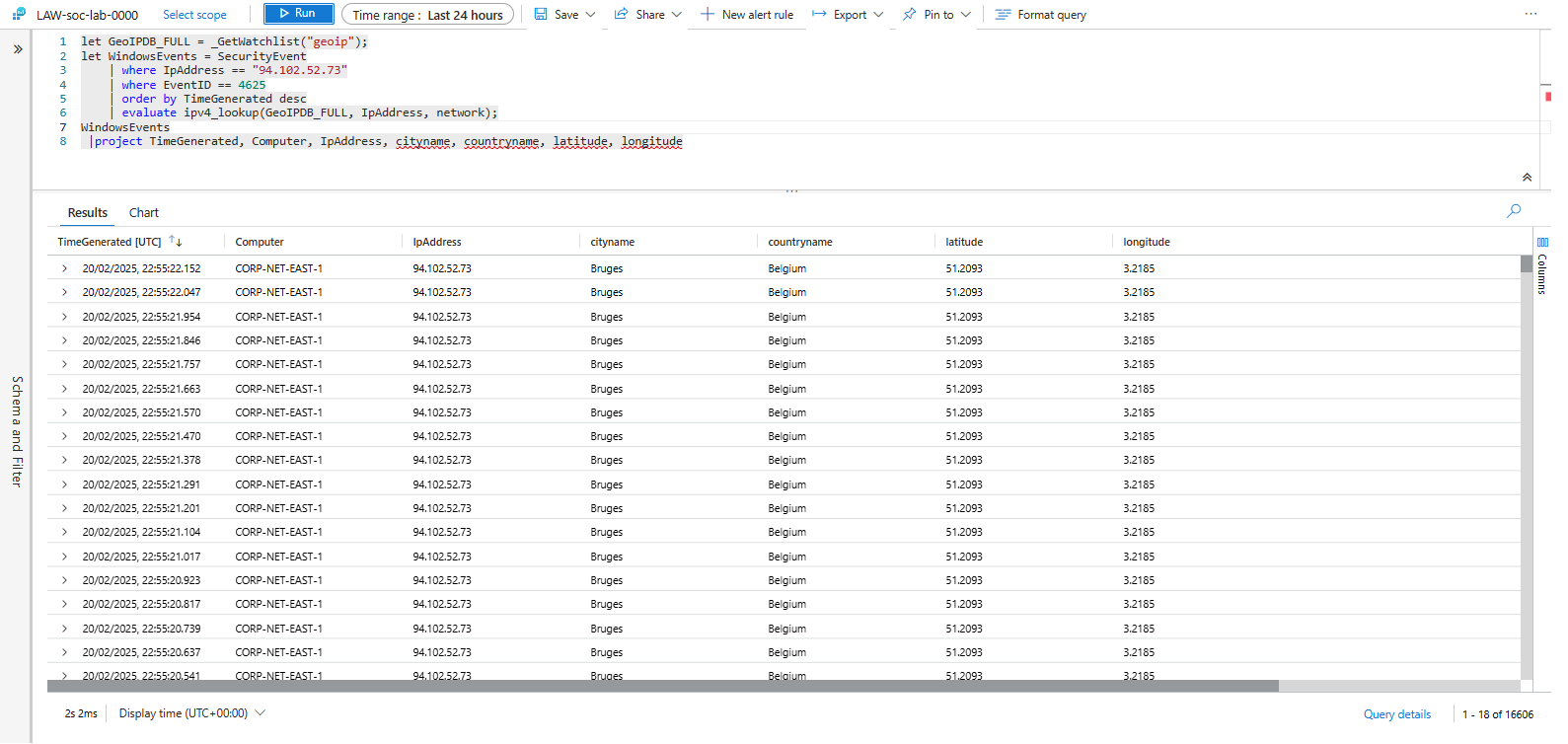
* Replace <attacker IP address> with an **actual IP** from your logs.
* **Observe:** Logs are now enriched with **geolocation data**.

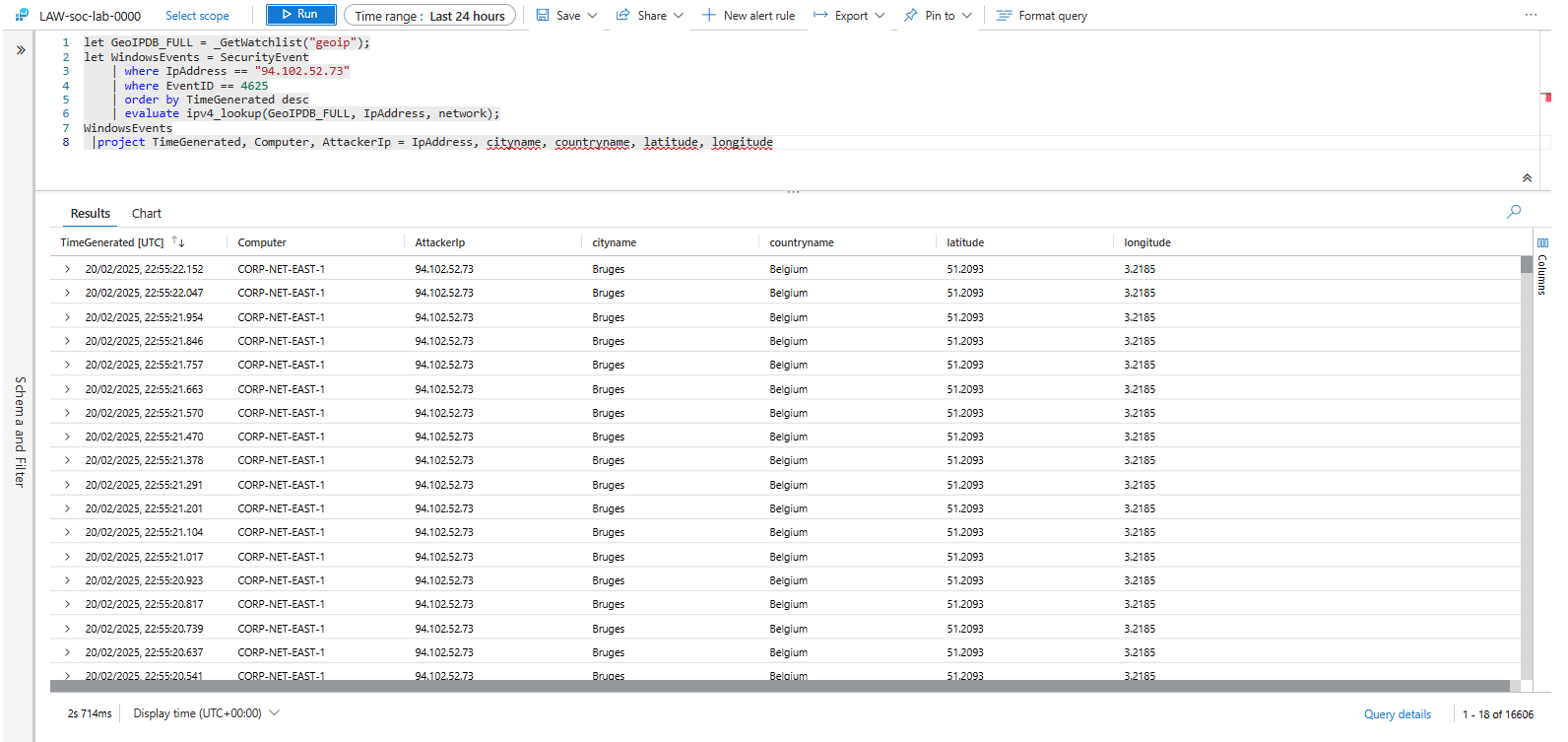












**Part 5: Creating an Attack Map**

**1. Create a New Workbook in Sentinel**

* Navigate to **Microsoft Sentinel → Workbooks**.
* Click **+ New Workbook**.

**2. Remove Default Elements**

* Delete any **prepopulated** workbook elements.

**3. Add a Query Element**

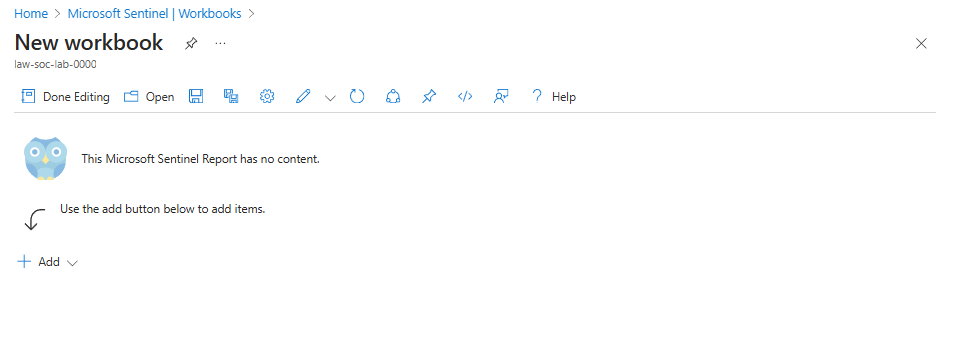
* Click **+ Add**, then select **Query**.

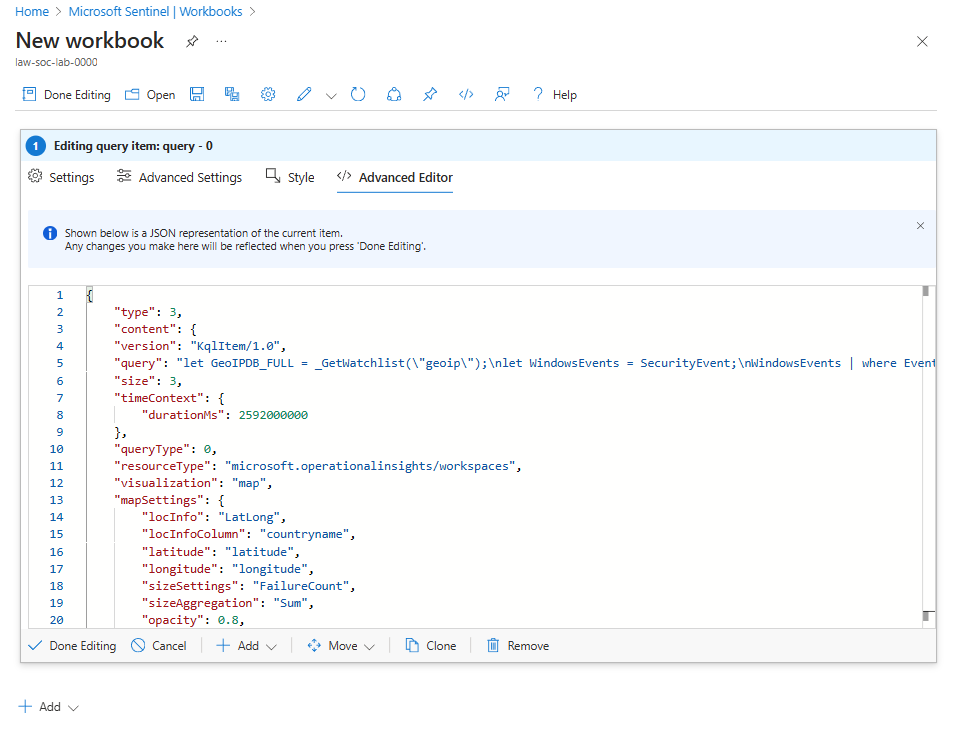
**4. Import Attack Map Configuration**

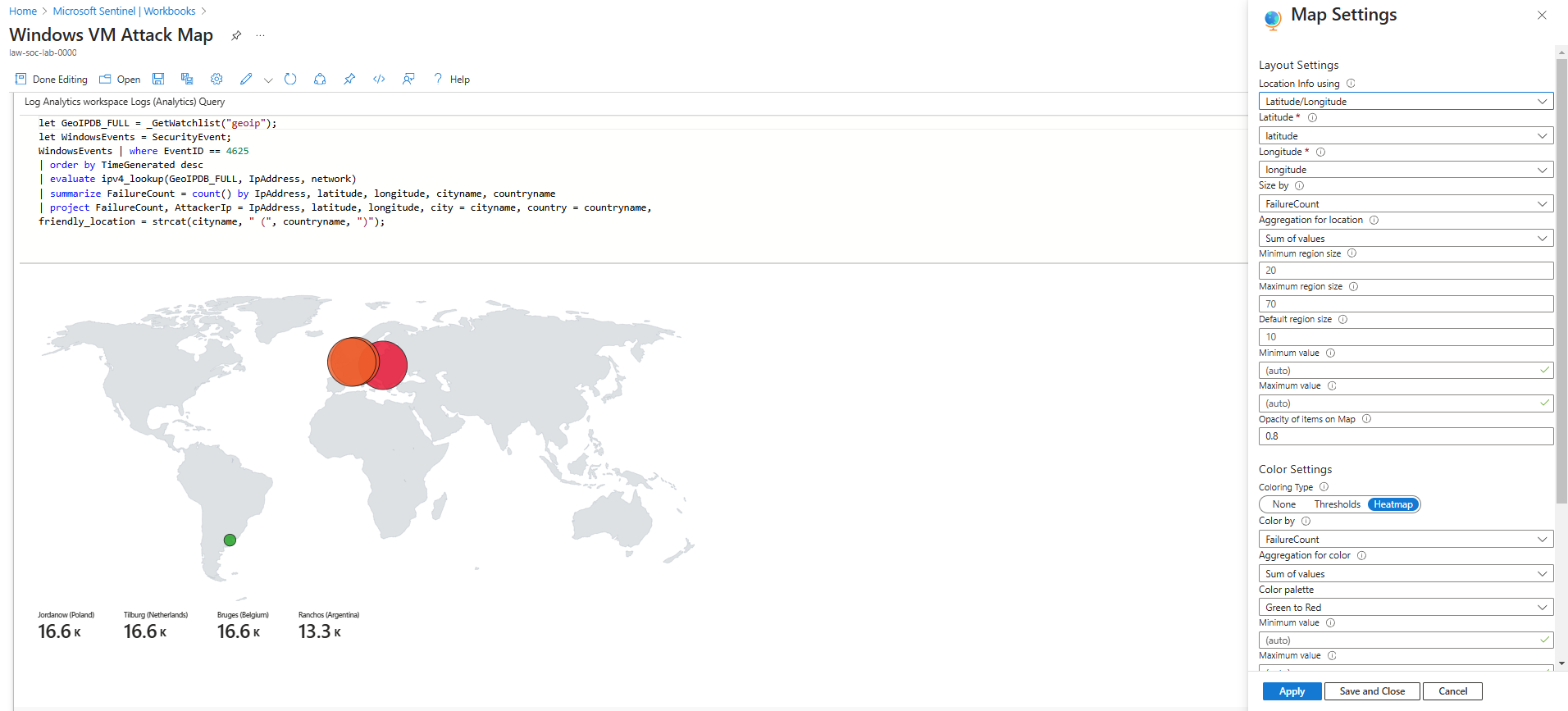
* **Download the JSON file**:  
  [map.json](https://drive.google.com/file/d/1ErlVEK5cQjpGyOcu4T02xYy7F31dWuir/view)
* Open the **Advanced Editor** tab.
* Copy and paste the JSON configuration.

**5. Observe the Attack Map**

* **Review the Query:** See how data is retrieved and visualised.
* **Check the Map Settings:** Ensure correct attack source display.
* **View the Map:** Visualise failed login attempts **by geographic origin**.







**Final Observations and Key Takeaways**

**By completing this project, you will have learned:**  
**How to set up a honeypot** using Azure Virtual Machines.  
**How to collect and query logs** using Log Analytics and Sentinel.  
**How to enrich security logs** with geolocation data.  
**How to create an attack map** to visualise security threats.

**Why This Matters for Security Operations (SecOps)**

* Querying logs is **an essential skill** for Security Analysts.
* Depending on your organisation, you might use:
  + **SQL (Structured Query Language)**
  + **KQL (Kusto Query Language - used in Azure Sentinel)**
  + **SPL (Search Processing Language - used in Splunk)**
* **If you understand one of these languages, you can learn the others easily.**