Microsoft Sentinel – Windows Security Monitoring

## Objective

The objective of this project is to build a **cloud-native SOC monitoring environment** using **Microsoft Sentinel** to ingest, analyze, and investigate Windows security events.  
The lab simulates a **real enterprise SOC workflow**, focusing on log ingestion validation before detection and response.

**Architecture Flow:**

Windows 11 (Azure VM)

↓

Azure Monitor Agent (AMA)

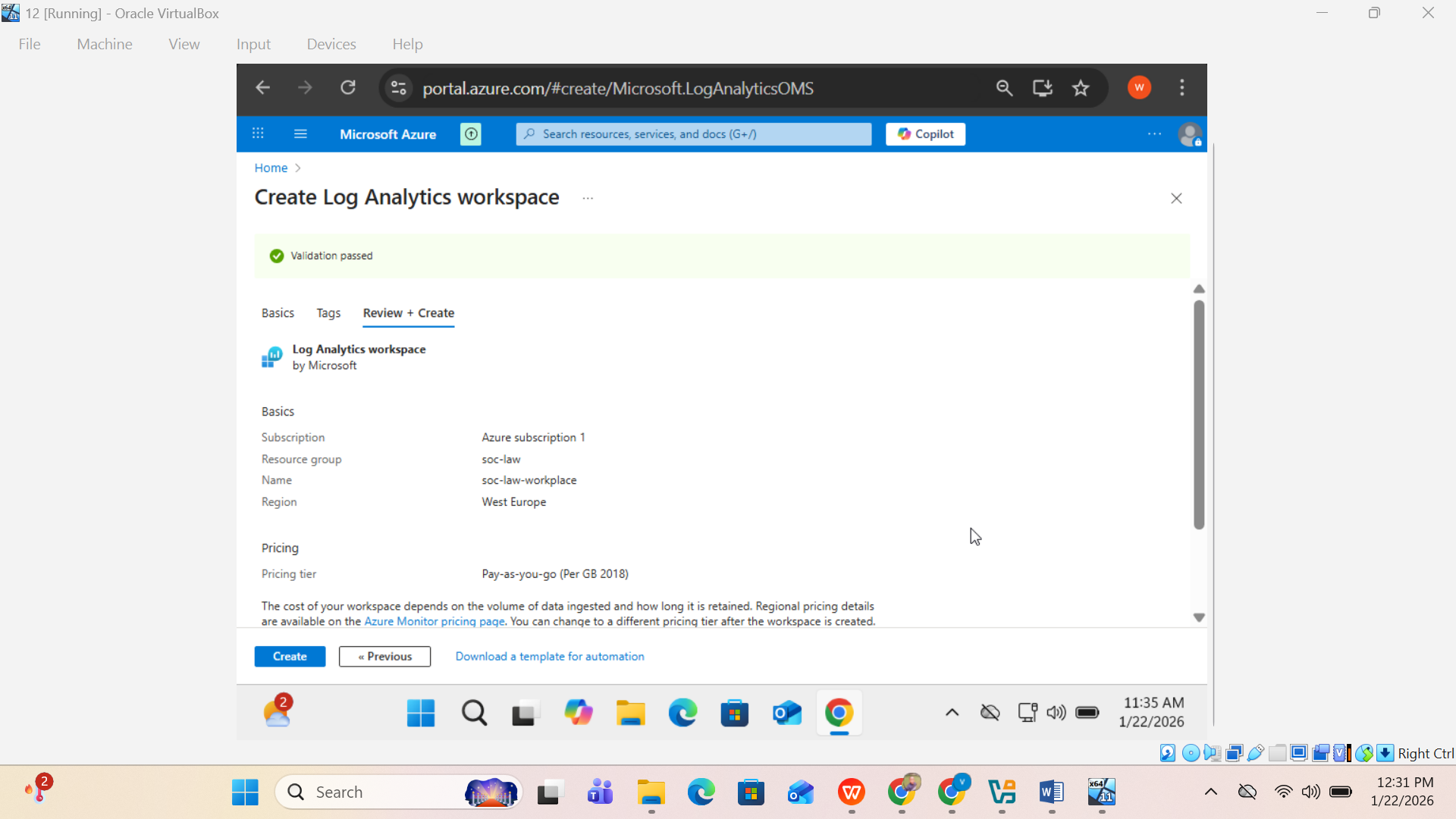
↓

Log Analytics Workspace

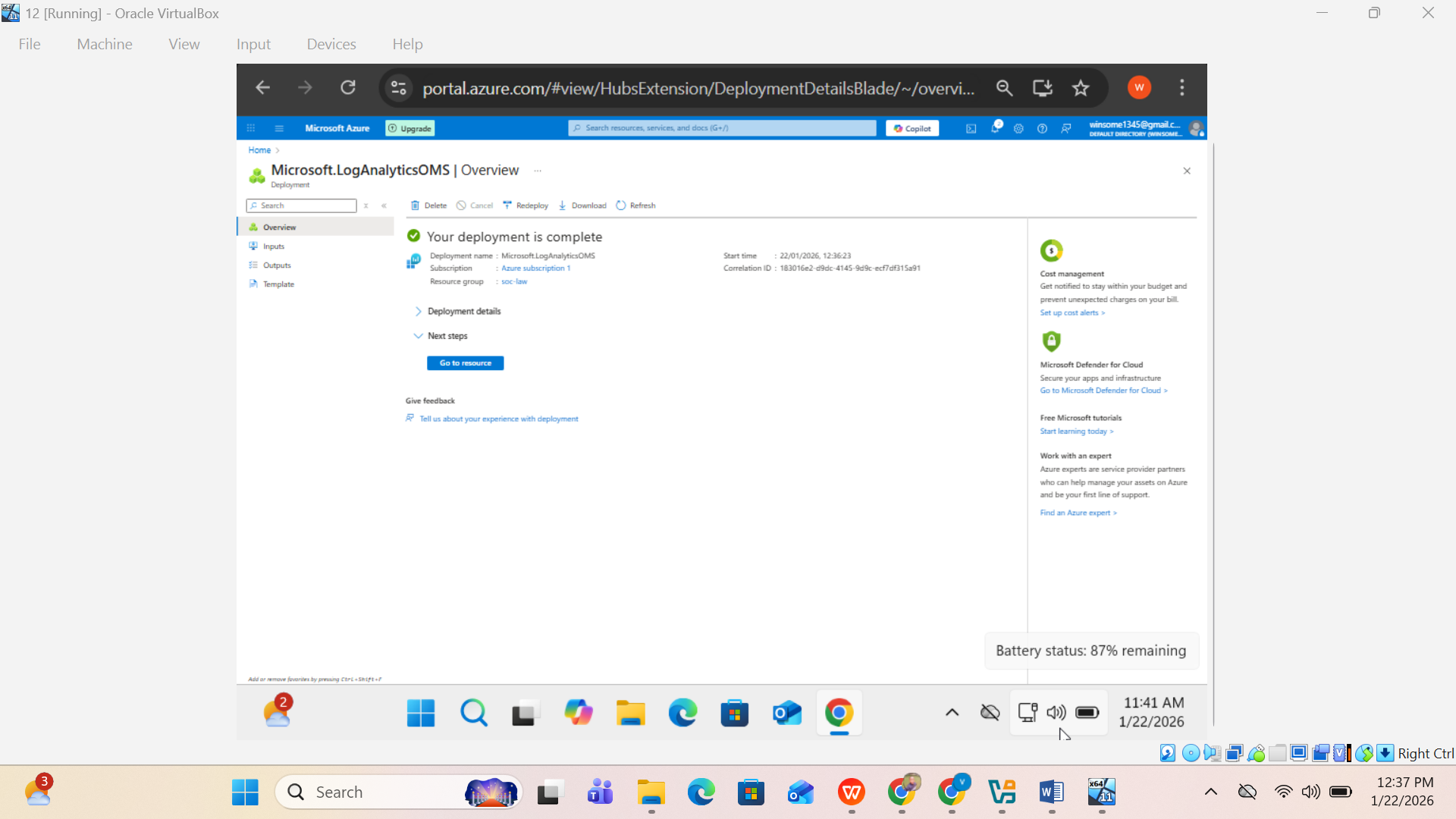
↓

Microsoft Sentinel

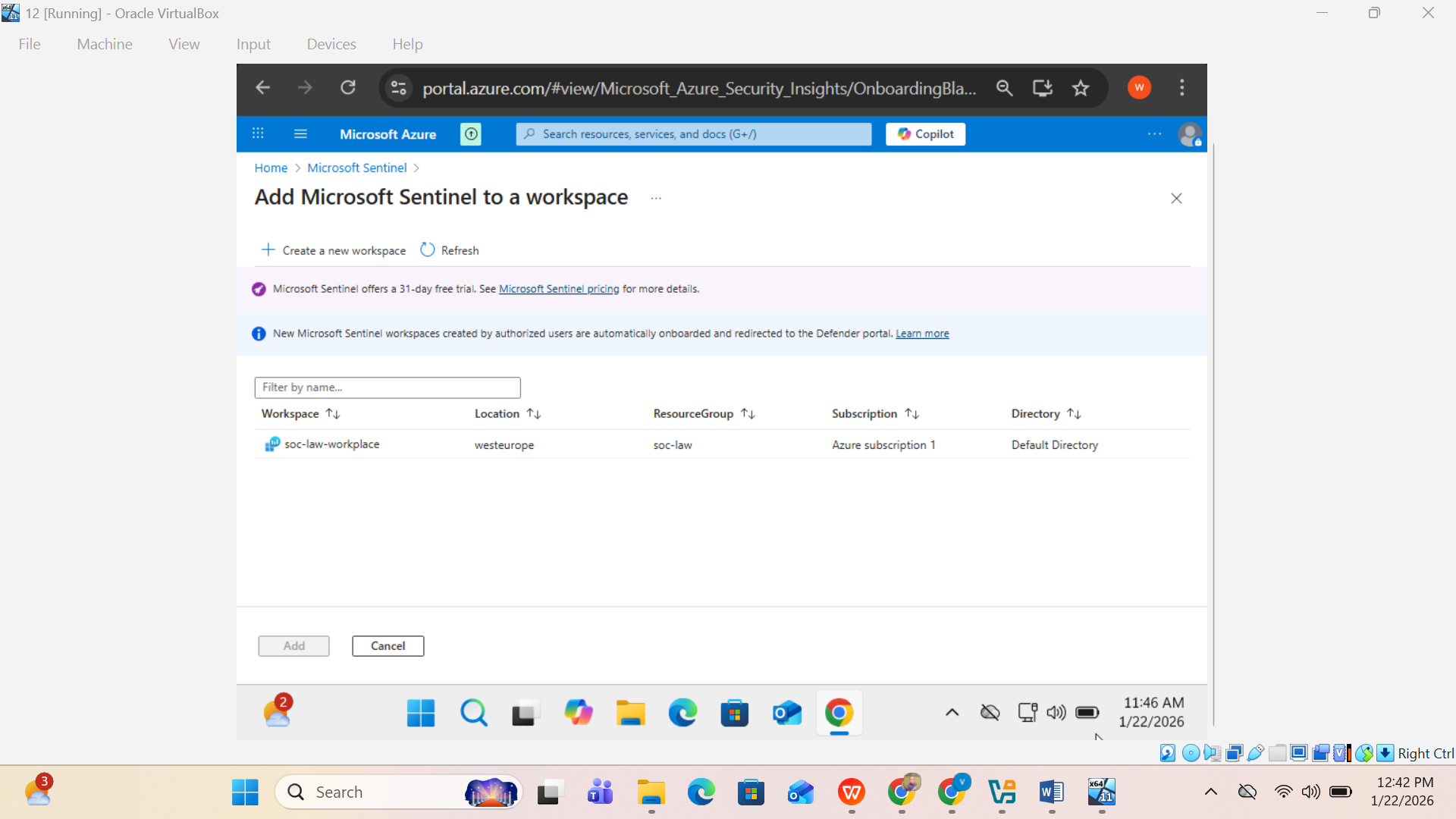
Step 1

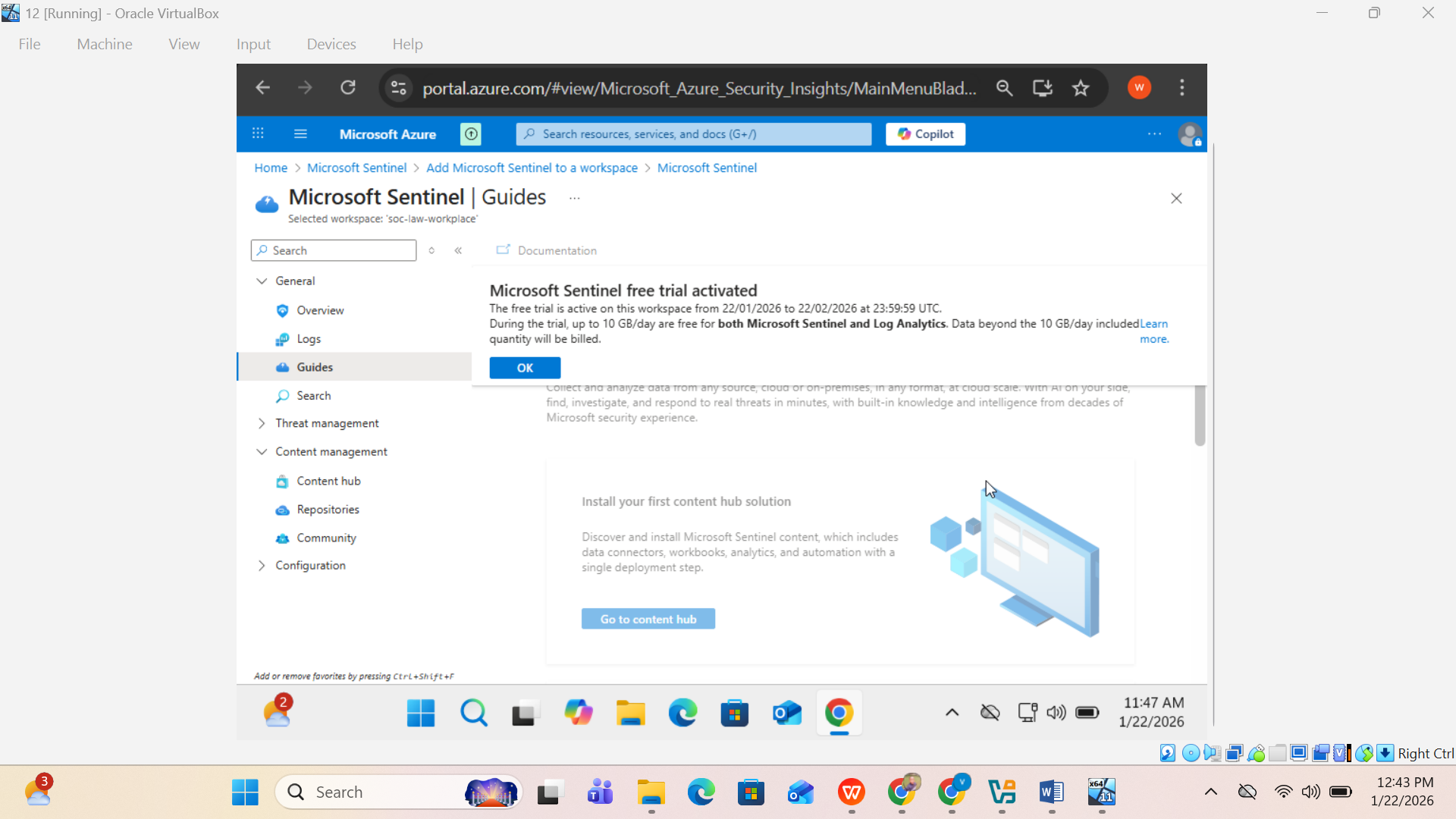


A Log Analytics Workspace named **soc-law-workplace** was created in the **West Europe** region to serve as the centralized log storage and analytics layer for the SOC lab. This workspace is used to collect, store, and query security telemetry from monitored endpoints and Azure services.



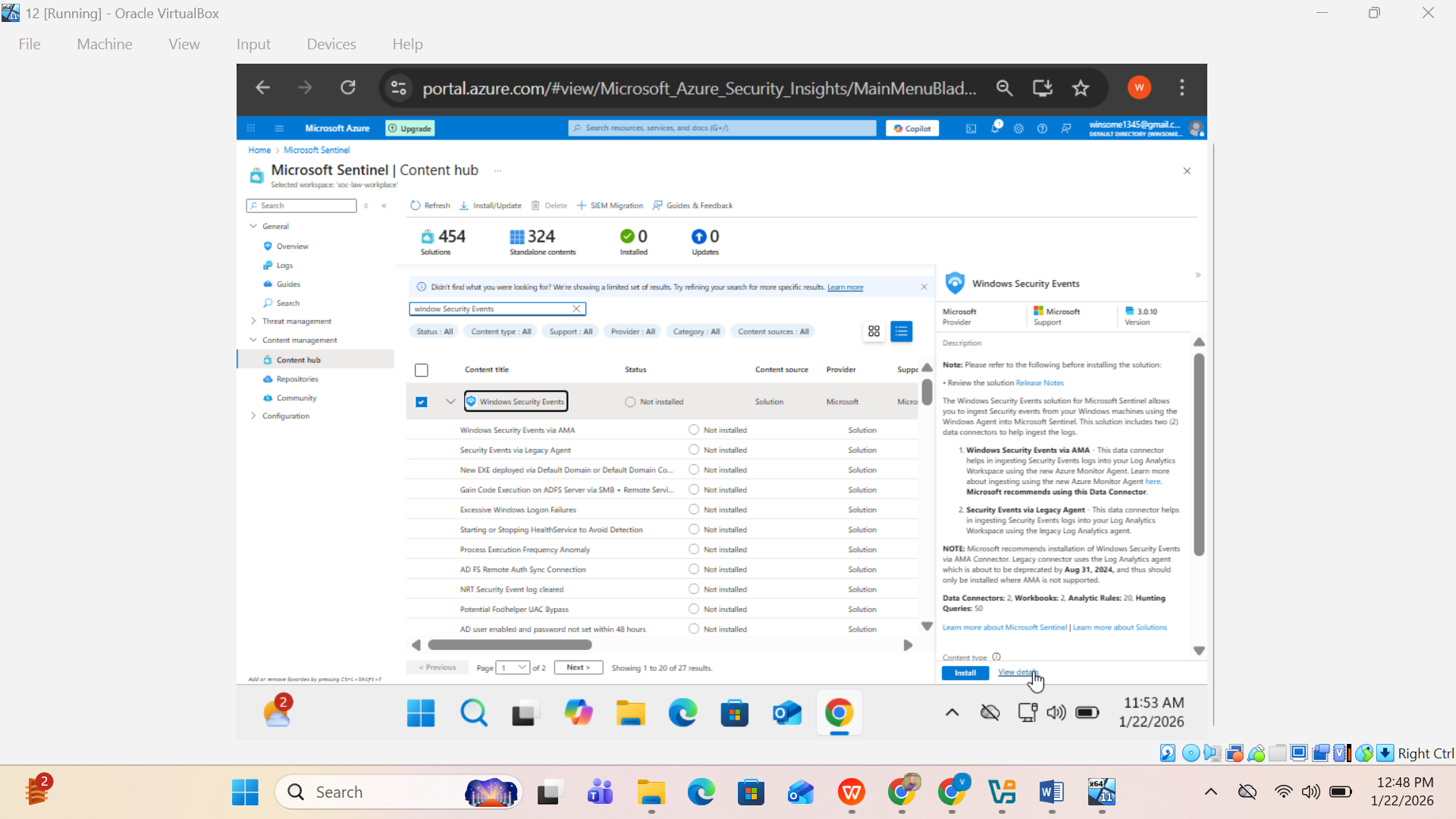
After deployment, the Log Analytics Workspace resource was opened to proceed with Microsoft Sentinel configuration.

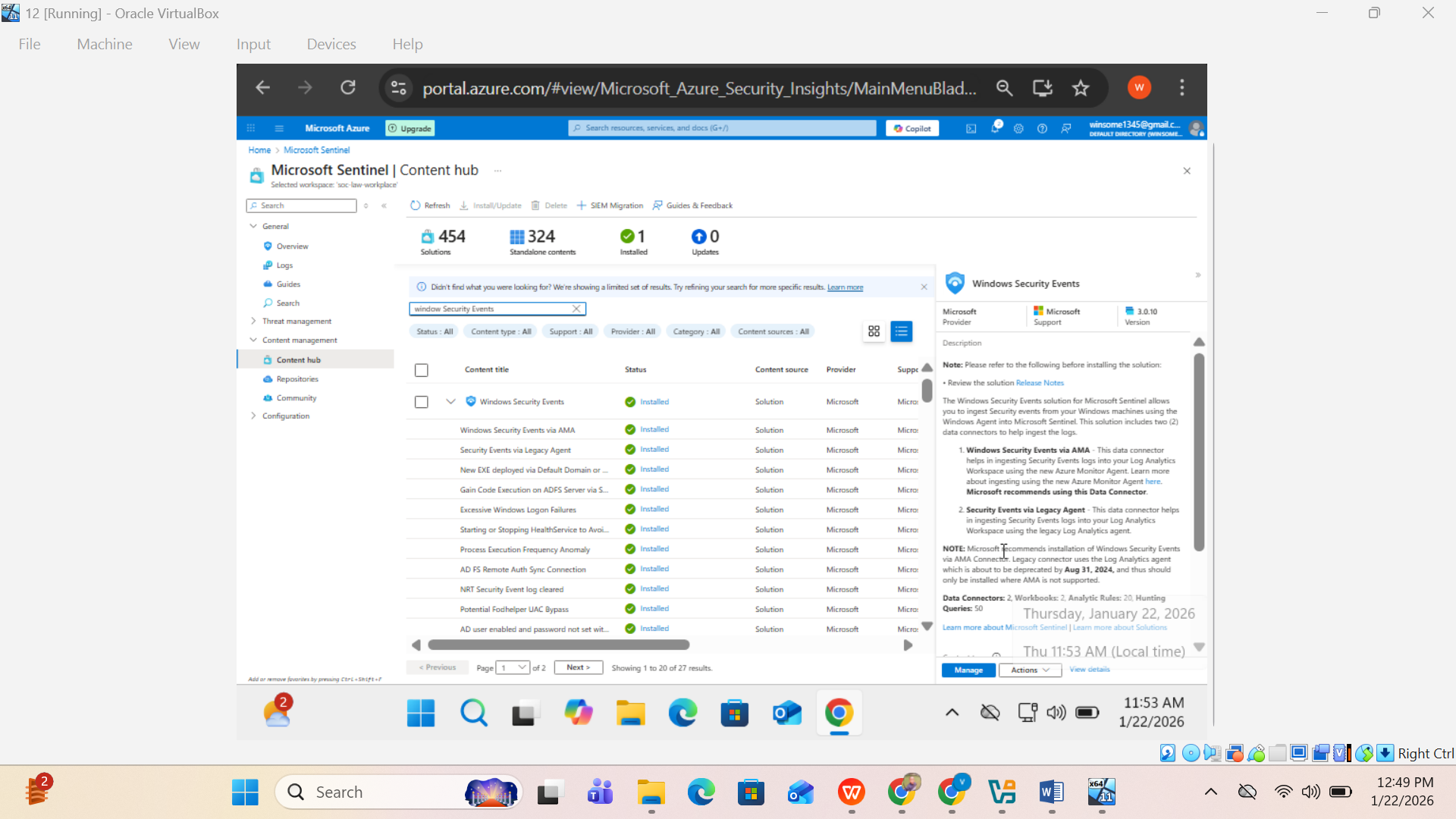




Microsoft Sentinel was successfully activated and the SIEM interface became available.

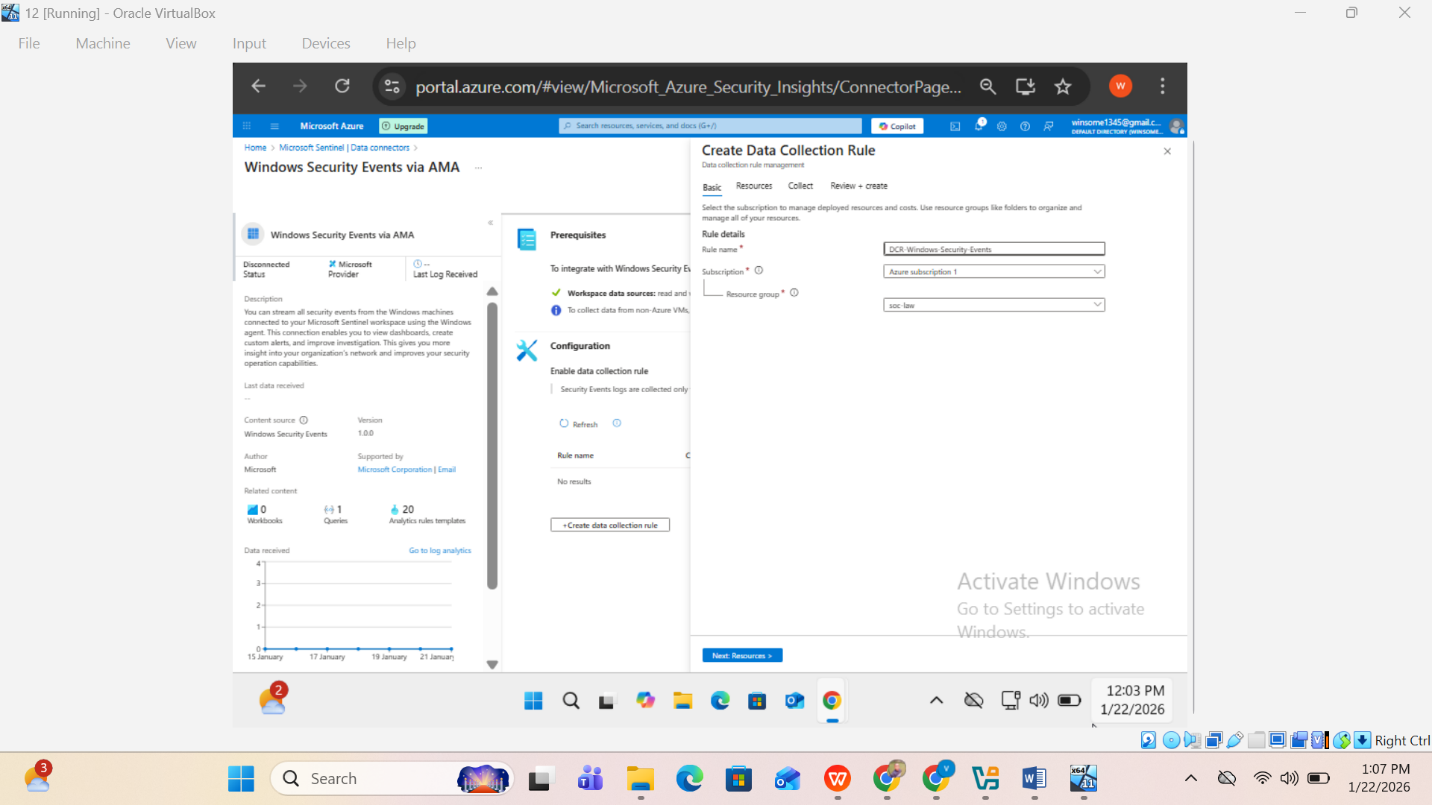
STEP 4️⃣ – Install Windows Security Events (AMA)





The Windows Security Events solution was installed via the Sentinel Content Hub using the Azure Monitor Agent.

STEP 5️⃣ – Create Data Collection Rule (DCR)

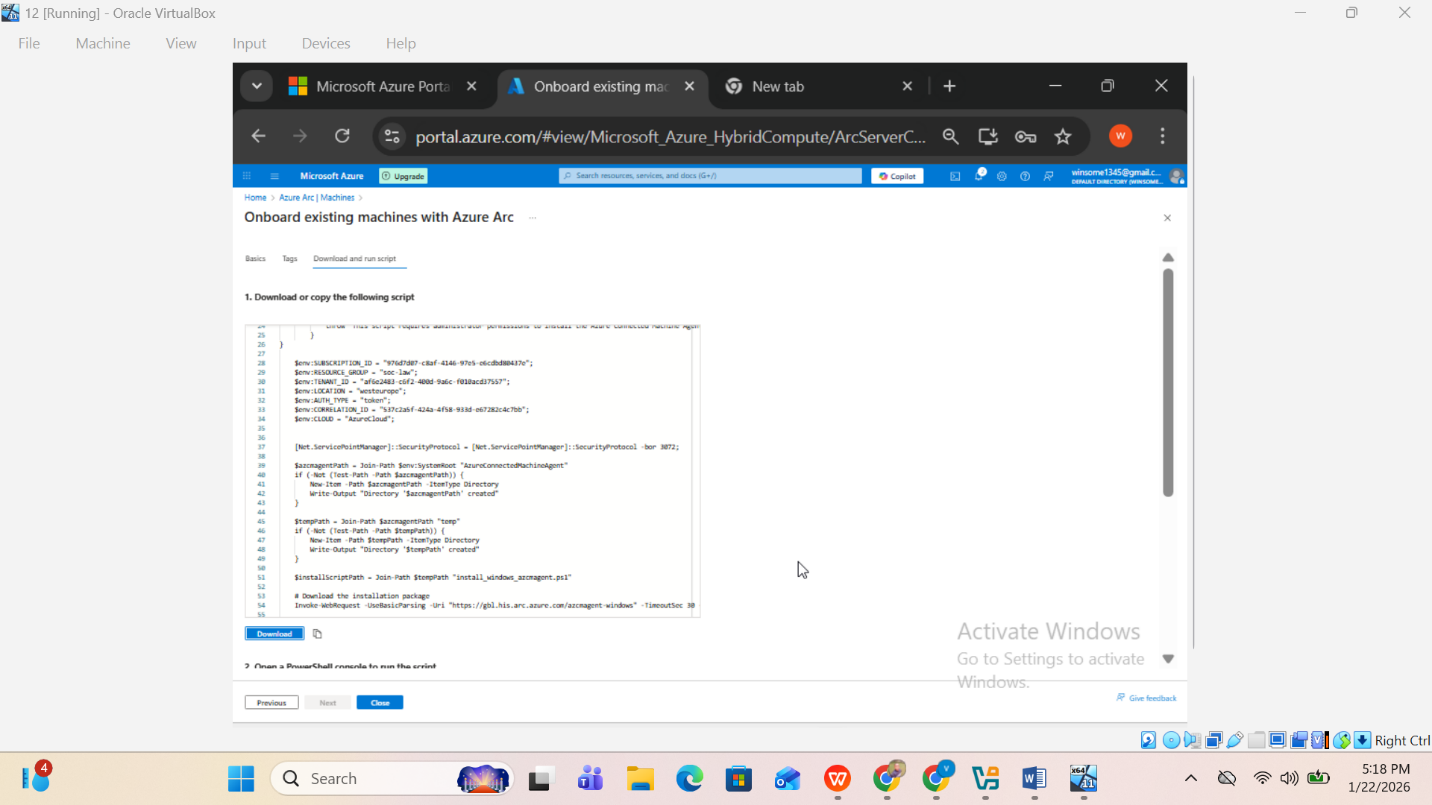


## Azure Arc Onboarding

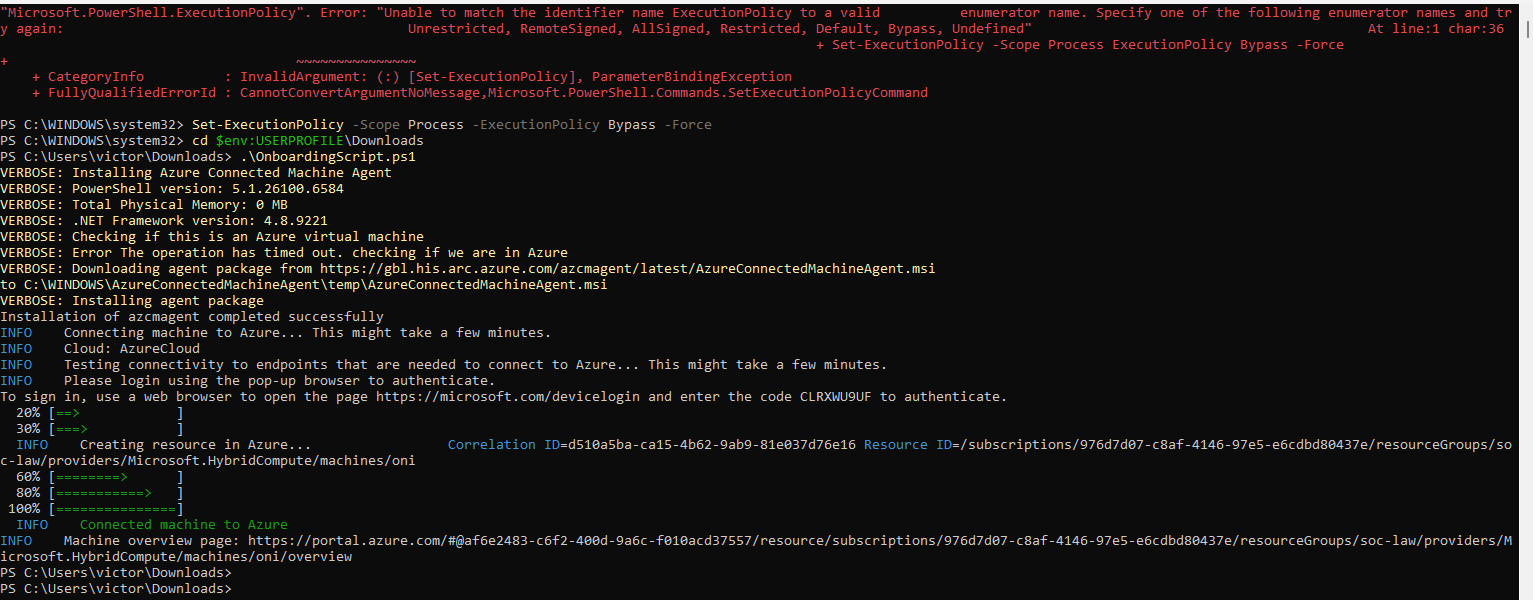
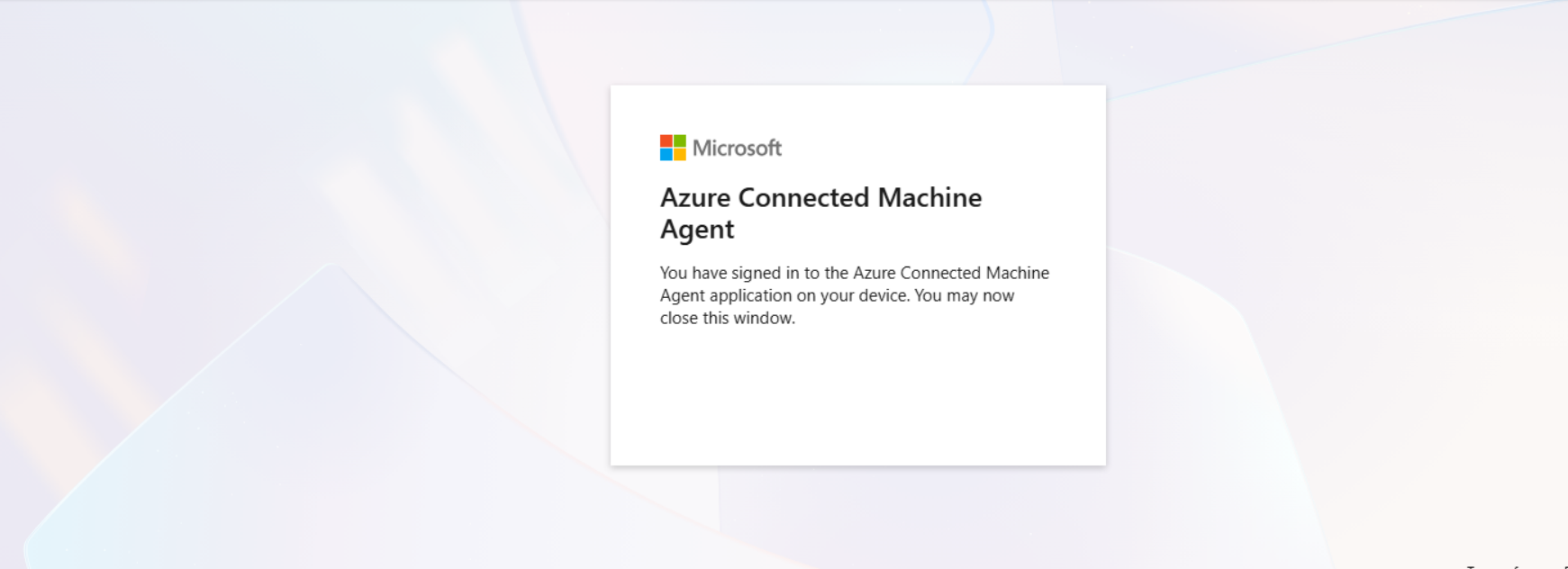
### 5.1 Generate Onboarding Script

Azure Portal → Azure Arc → Machines → **Add / Onboard**

* Select subscription
* Select resource group
* Copy or download the PowerShell onboarding script



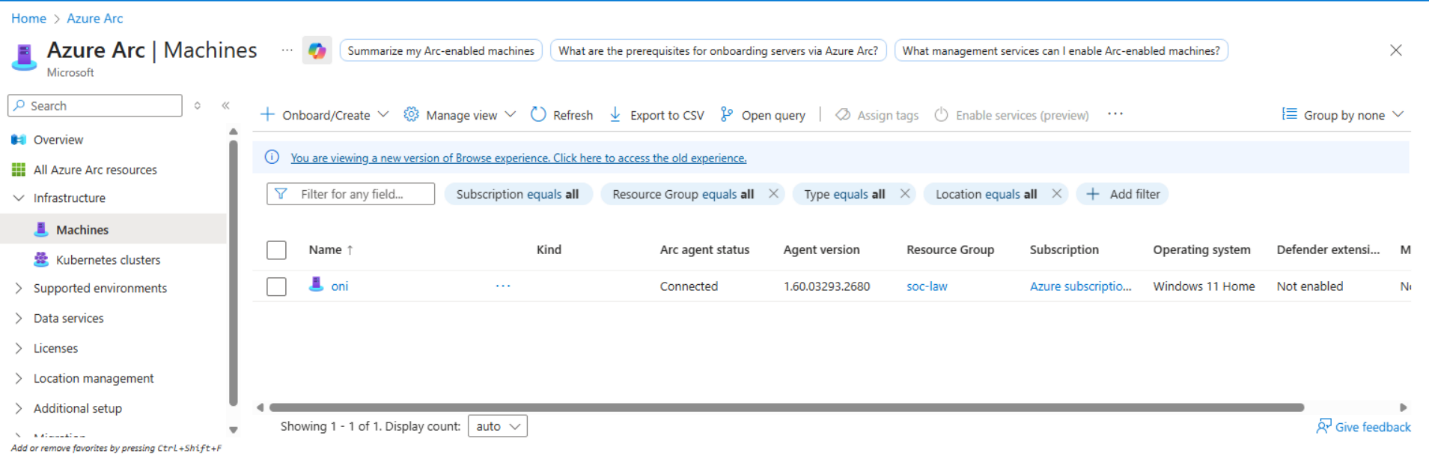
### Run Script on Windows VM

Run **PowerShell as Administrator**:  
  


### Validation

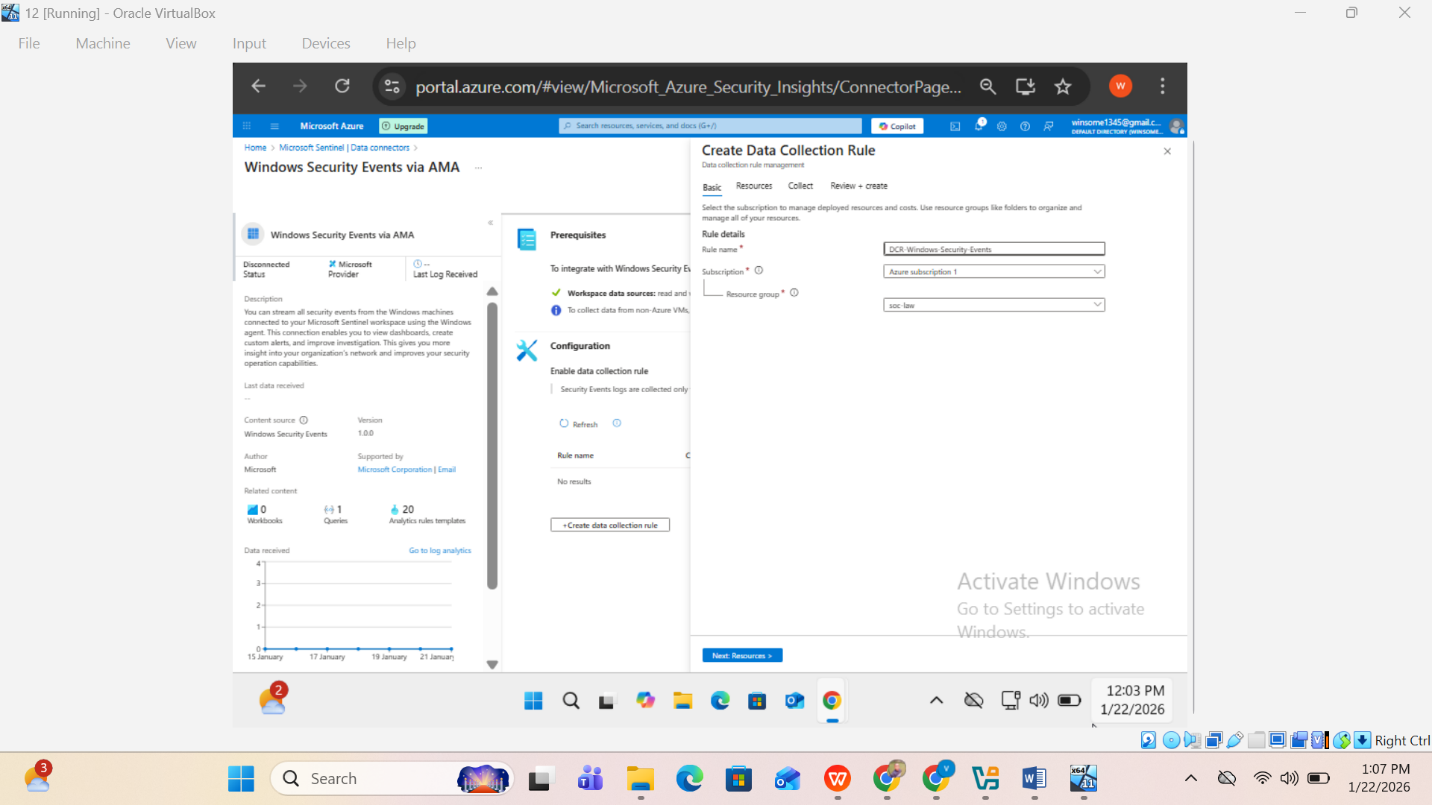
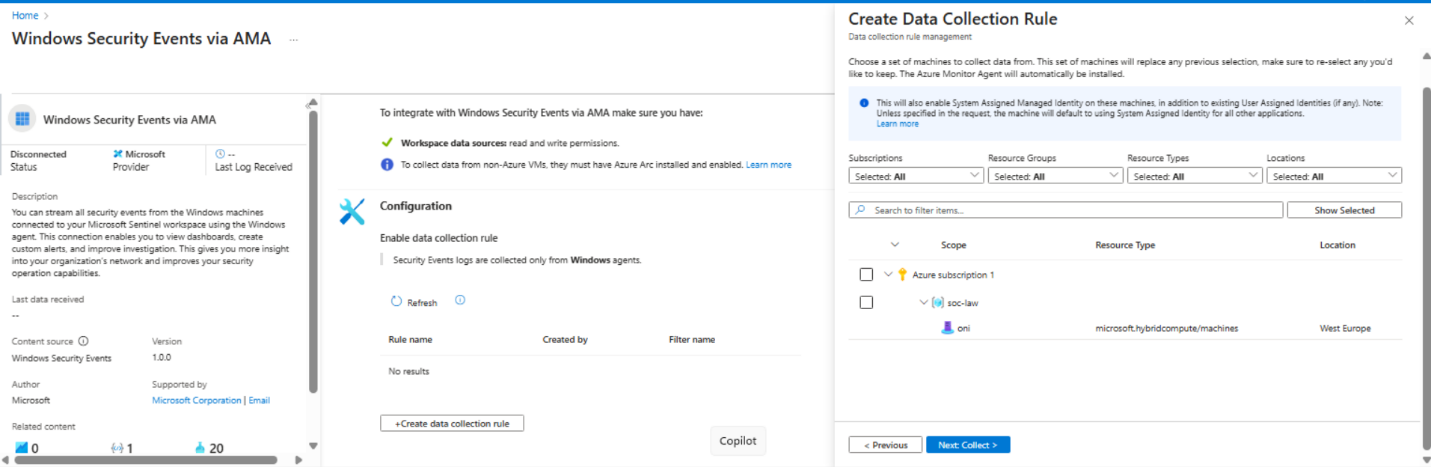
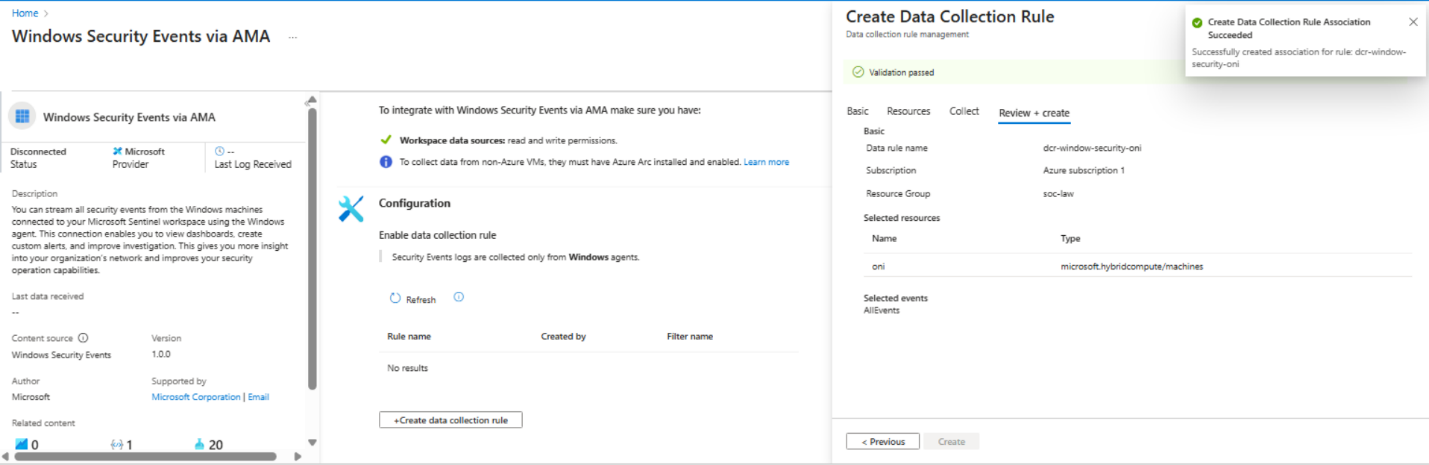
Azure Portal → Azure Arc → Machines

Status should show:

* **Connected**
* Agent installed  
  

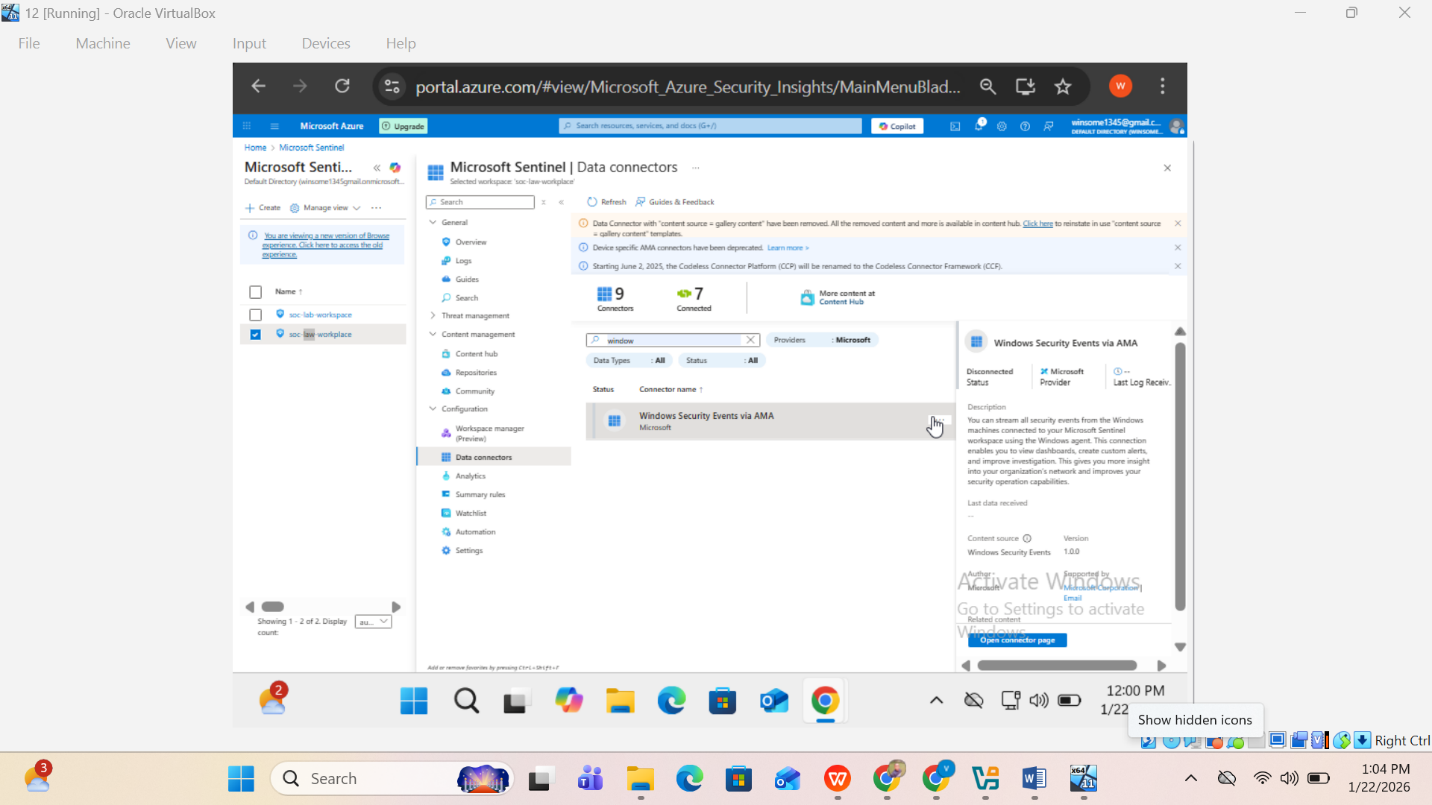
## Azure Monitor Agent (AMA)

AMA is automatically installed when:

* A Data Collection Rule is associated
* Azure Arc machine is selected  
    
    
    
  

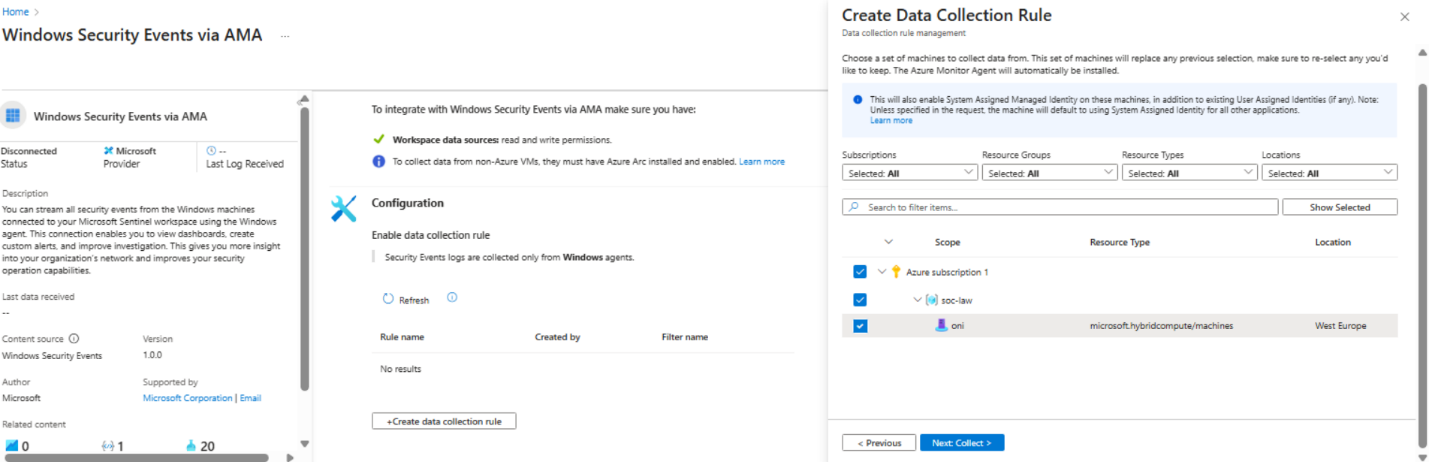
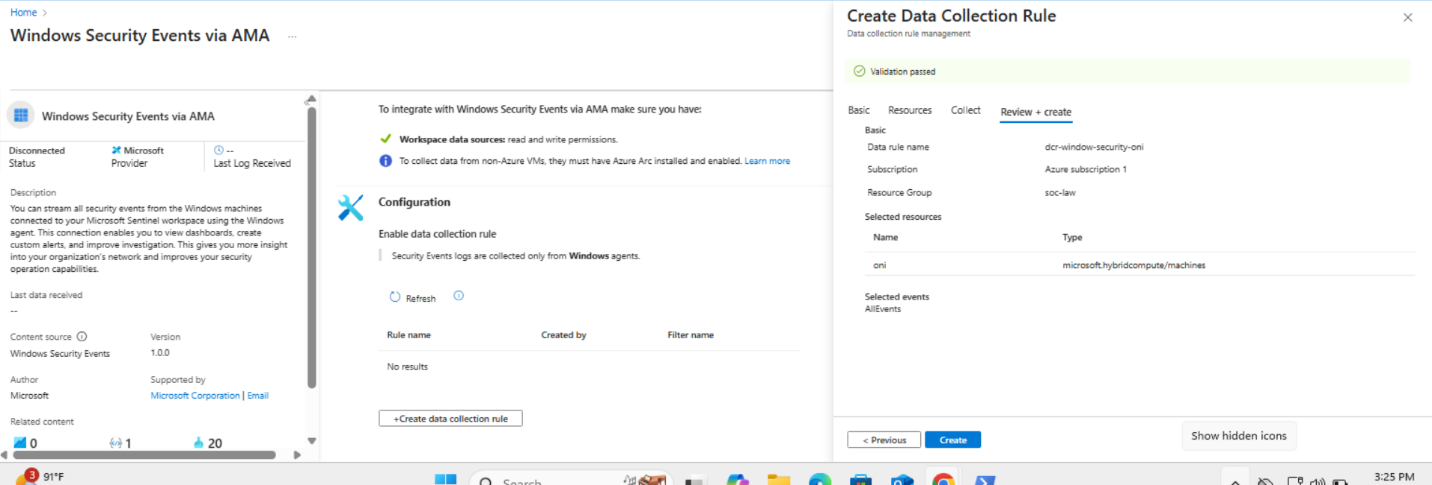
## Configure Windows Security Events via AMA

### 7.1 Navigate to Connector

Microsoft Sentinel → Data connectors → **Windows Security Events via AMA  
**

### Create Data Collection Rule (DCR)

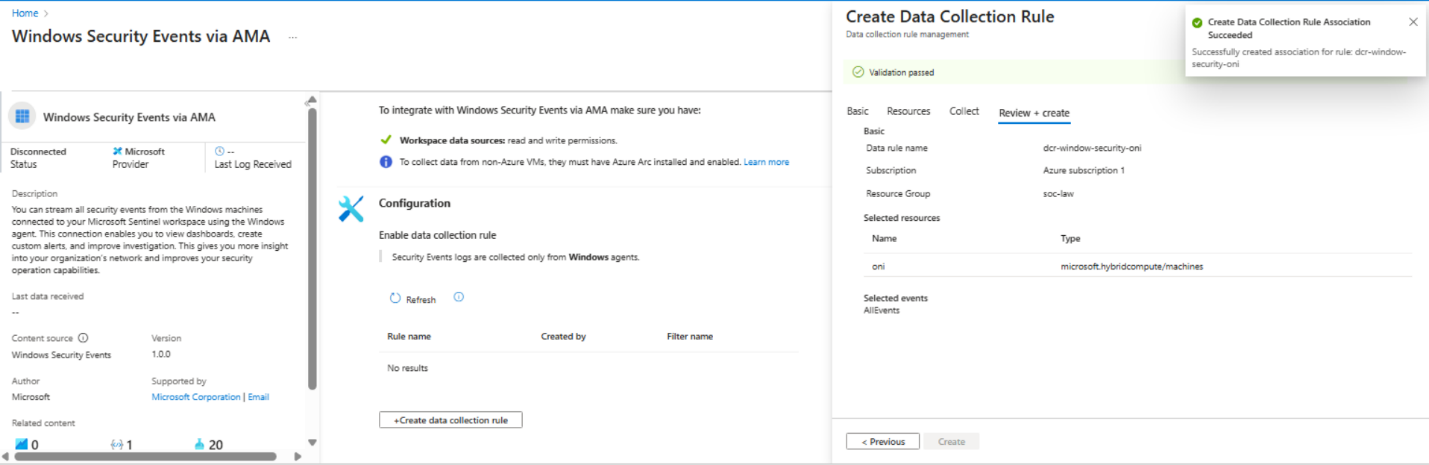
* Rule name: dcr-windows-security-oni
* Target: Azure Arc machine
* Events collected: **AllEvents**

**  
**

### 7.3 Associate DCR

* Select Arc-enabled machine
* Validate and create

**Status:** DCR Association Succeeded

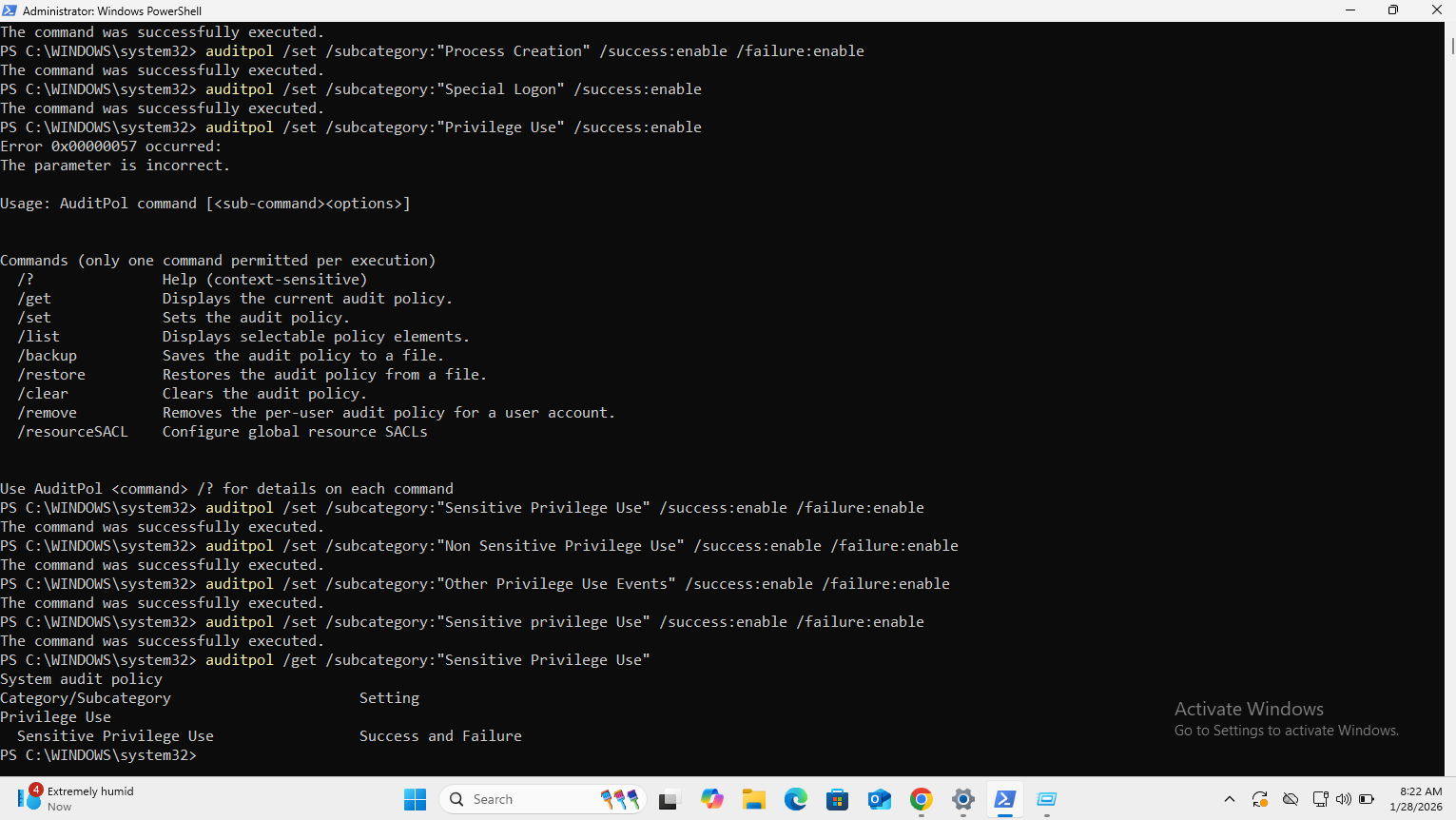


## Enable Windows Audit Policies

### Advanced auditing is required for security events. Verification

auditpol /get /subcategory:"Sensitive Privilege Use"

Expected output:

* **Success and Failure**  
  

## Log Validation in Microsoft Sentinel

### 9.1 SecurityEvent Table

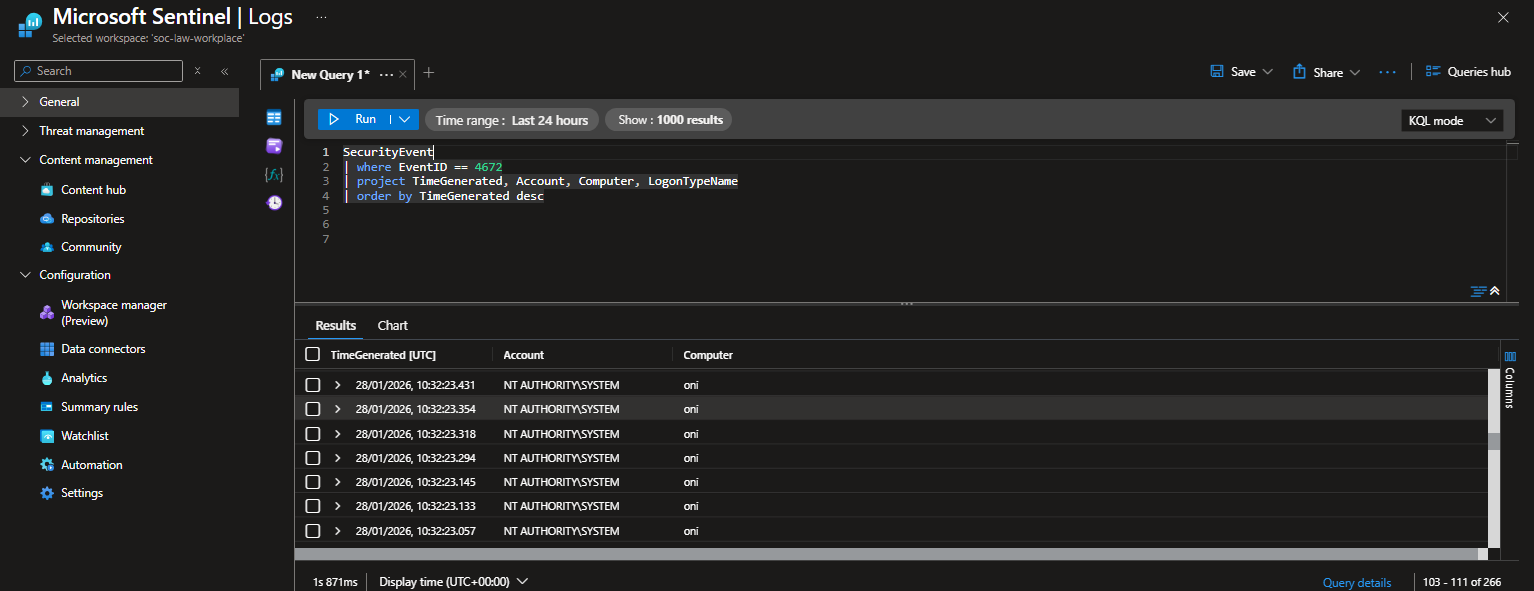
Fallback / Diagnostic Query  


### Threat Hunting – Privileged Logon (Event ID 4672) Hunting Objective

Identify **privileged logons** that may indicate:

* Administrator misuse
* Credential abuse
* Lateral movement

This hunt focuses on **Event ID 4672**, which is generated when special privileges are assigned to a new logon session.

Initial Hunt Query (Baseline

**Purpose:**

* Confirm that privileged logons are occurring
* Identify accounts receiving elevated privileges

### Advanced Hunt – Extract Privilege Details

Privilege information is not stored as a flat column in the SecurityEvent table. Instead, it is embedded in nested fields such as EventData or AdditionalFields.

### Findings

* Privileged logon events were successfully detected
* The events confirmed assignment of elevated privileges during user logon
* No anomalous or unexpected privileged activity was observed during the test window

## SOC Dashboard (Microsoft Sentinel Workbook)

### 12.1 Objective

Build a **SOC monitoring dashboard** to provide visibility into authentication activity, privilege usage, and overall security posture of the Windows endpoint.

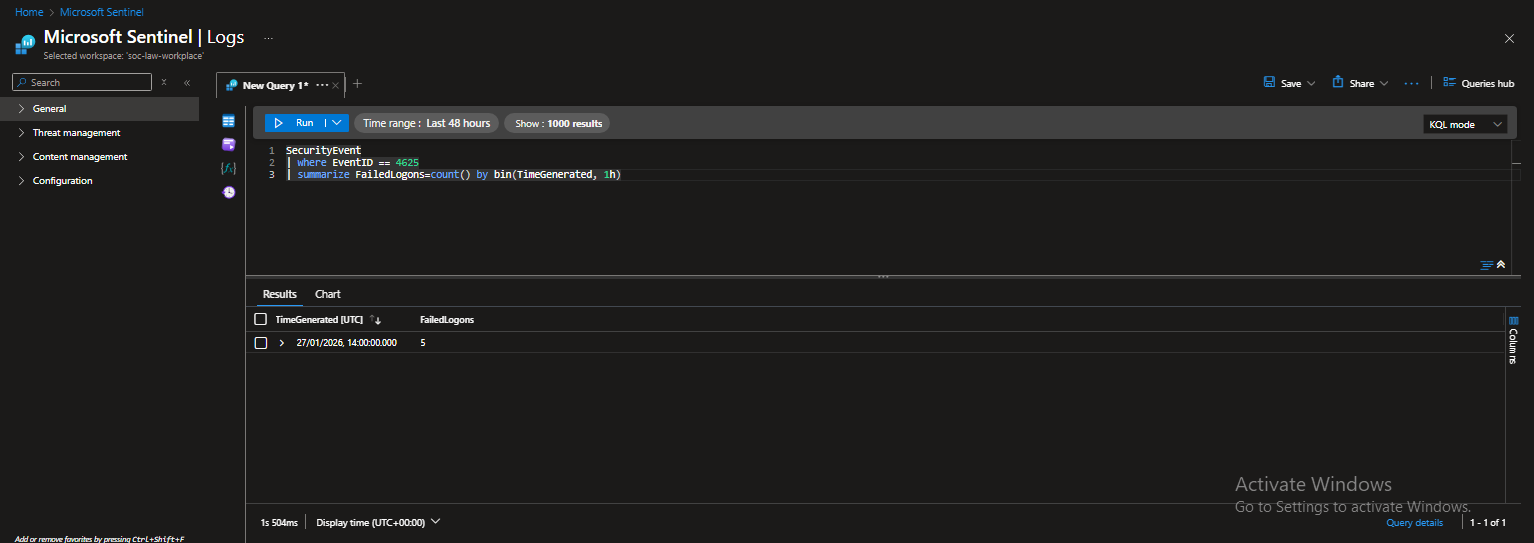
The dashboard is designed for **Tier-1 and Tier-2 SOC analysts** to quickly assess:

* Suspicious authentication behavior
* Privileged account usage
* Event volume trends

### Dashboard Components

The following visual components were created using **Microsoft Sentinel Workbooks**:

#### A. Failed Logons Over Time

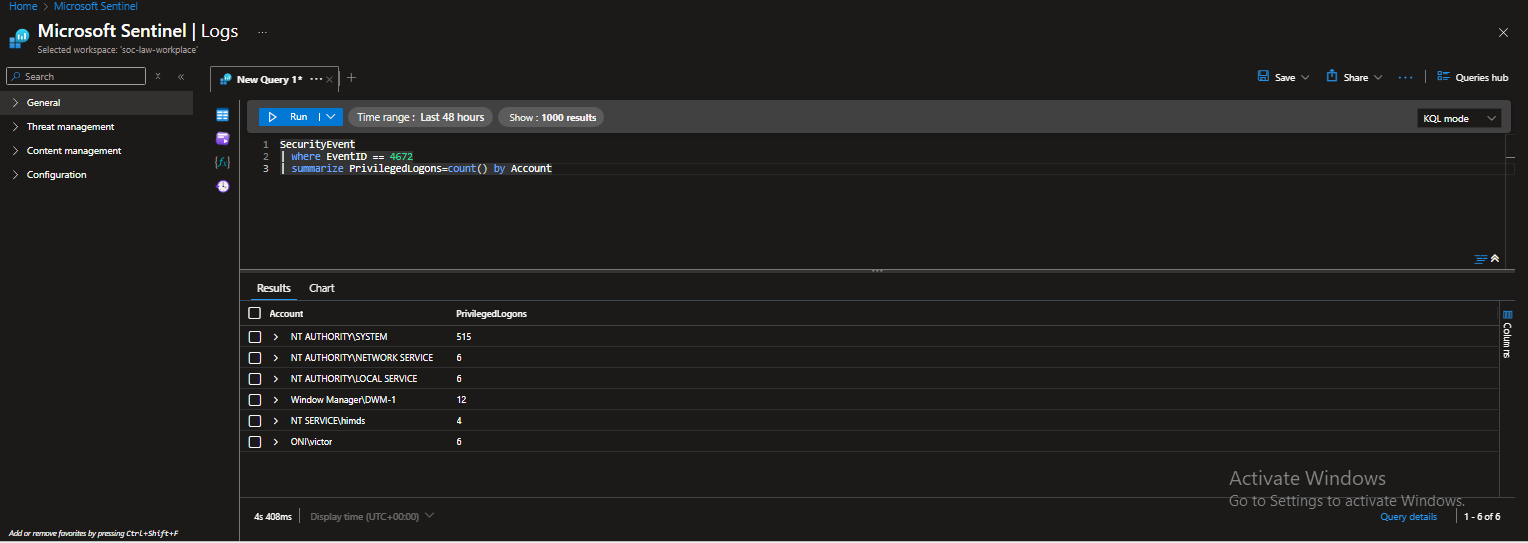
  
**Purpose:**

* Identify brute-force or password-spraying patterns

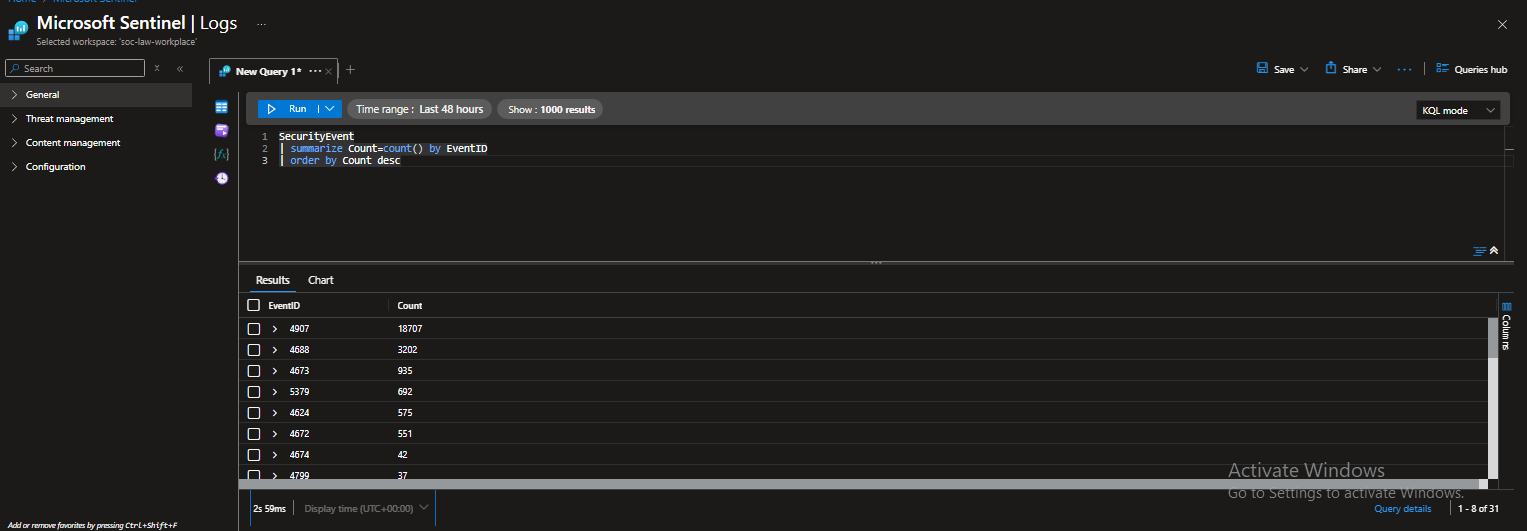
#### B. Successful Logons Over Time

**Purpose:**

* Establish authentication baseline
* Detect abnormal login activity

. Privileged Logons  
  
**Purpose:**

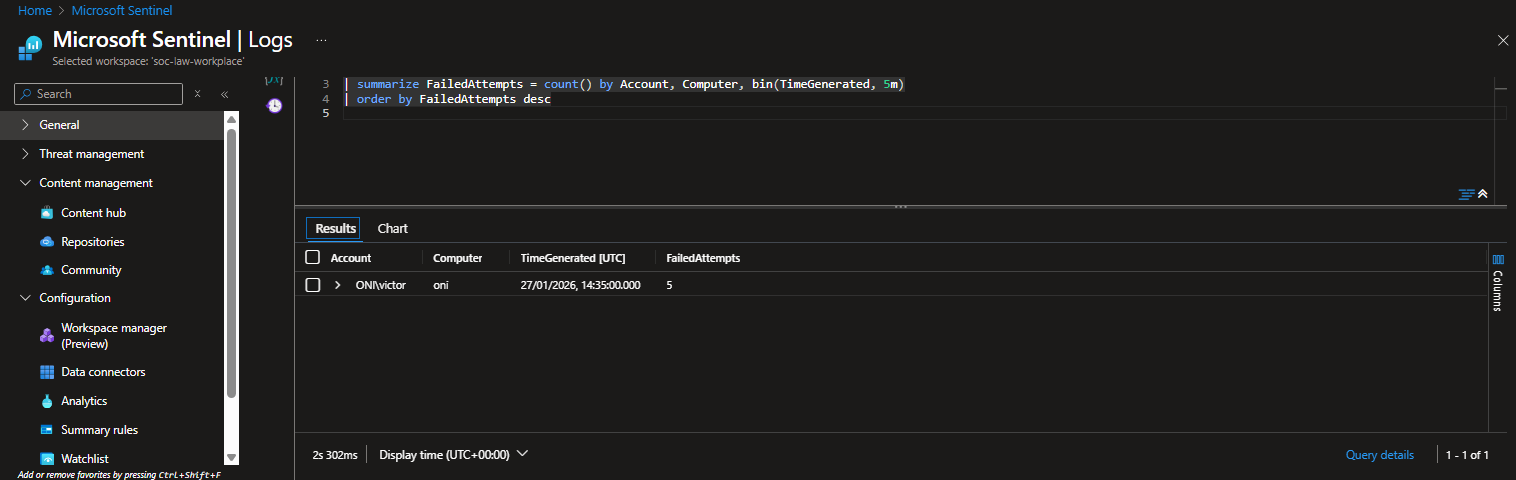
* Monitor administrator and high-privilege account usage

Top Security Event IDs  
  
**Purpose:**

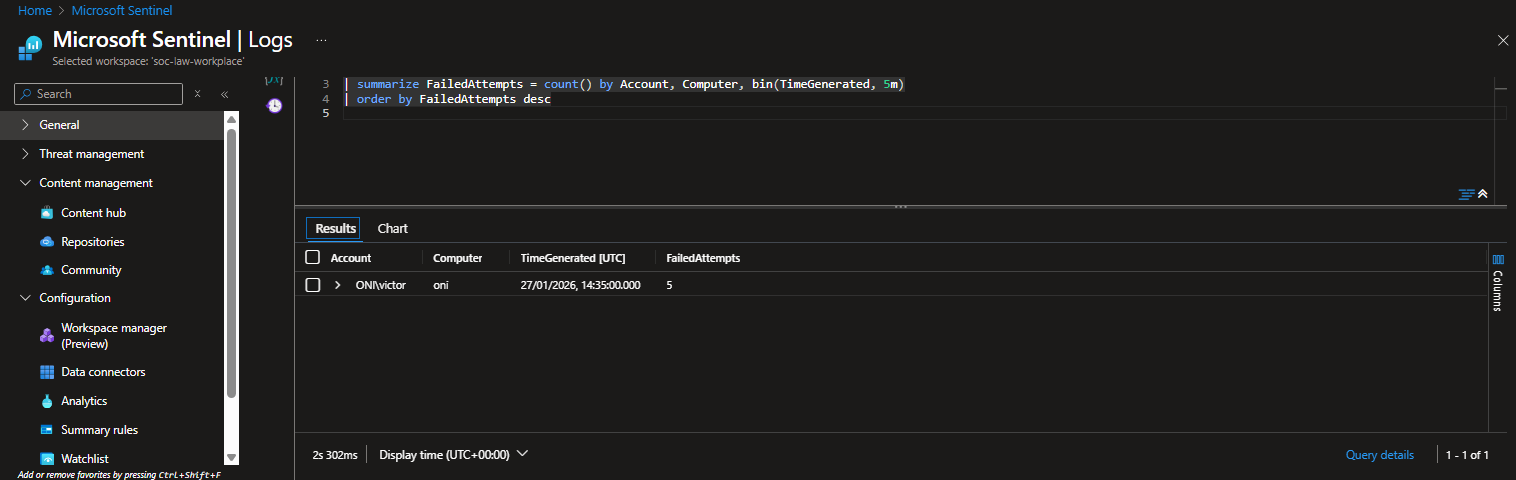
* High-level visibility into security event distribution

### Dashboard Value (SOC Perspective)

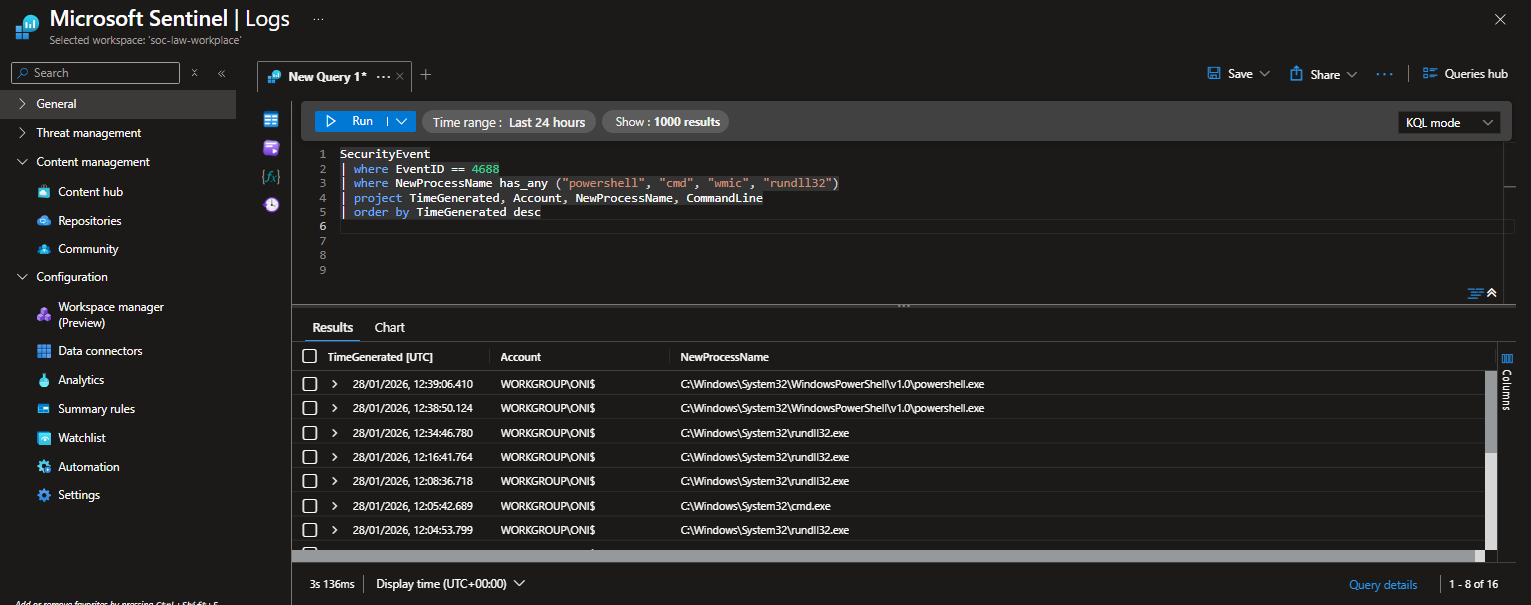
* Enables rapid triage of authentication anomalies
* Supports escalation decisions
* Provides management-friendly security visibility
* Acts as a foundation for alert-driven workflow



Failed Logon Bursts (Brute Force)



Privileged Logons

Suspicious Process Creation  
  
Logon Outside Normal Hours

Account Lockouts