Azure SIEM Project with Microsoft Sentinel/Defender

This project demonstrates how I built and configured a Security Information and Event Management (SIEM) solution in Microsoft Azure using Log Analytics Workspace (LAW) and Microsoft Sentinel. The purpose of this lab was to simulate a vulnerable Virtual Machine (VM), observe real-world attack attempts, and visualize them through a security dashboard.

## 1. Create a Resource Group

I started by creating a Resource Group, which is a container in Azure that organizes and manages all related resources for this project.

A screenshot of a computer

AI-generated content may be incorrect.

## 2. Create a Virtual Network (VNet)

Next, I created a Virtual Network to provide secure communication and IP addressing for the VM.

A screenshot of a computer

AI-generated content may be incorrect.

## 3. Create a Virtual Machine (VM)

I deployed a Windows 10 Virtual Machine within the resource group and connected it to the virtual network.

A screenshot of a computer

AI-generated content may be incorrect.

## 4. Modify NSG Rules

I edited the Network Security Group (NSG) rules to allow inbound traffic on many unnecessary ports. This simulated a misconfigured and vulnerable system.

A screenshot of a computer

AI-generated content may be incorrect.

## 5. Configure Firewall Rules

I added a firewall rule that allowed any traffic inbound, further exposing the VM to external threats.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## 6. Remote Desktop Connection

Using RDP, I connected to the VM for further configuration.

A screenshot of a computer

AI-generated content may be incorrect.

## 7. Disable Windows Defender Firewall

Inside the VM, I turned off all protections in Windows Defender Firewall, intentionally leaving the system open.

A computer screen with a beach and water

AI-generated content may be incorrect.

## 8. Connectivity Test

I verified accessibility by pinging the VM’s public IP from my personal computer. The successful response confirmed that the VM was reachable from the internet.

A screenshot of a computer

AI-generated content may be incorrect.

## 9. Simulating Failed Logins

I closed the RDP session and attempted several failed login attempts to generate authentication failure logs.

A screenshot of a computer

AI-generated content may be incorrect.

## 10. Event Viewer Verification

After logging in successfully, I opened Event Viewer on the VM. The failed login attempts were recorded, showing timestamps and source IP addresses.

A screenshot of a computer

AI-generated content may be incorrect.

## 11. Real-Time Attacks

Within 20 minutes of exposure, the VM began receiving login attempts from automated bots across the internet.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## 12. Create a Log Analytics Workspace (LAW)

I created a Log Analytics Workspace to serve as the centralized repository for all log data collected from the VM.

A screenshot of a computer

AI-generated content may be incorrect.

## 13. Deploy Microsoft Sentinel

I enabled Microsoft Sentinel on the LAW to provide advanced monitoring, alerting, and threat analysis.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## 14. Connect VM to LAW and Sentinel

Using the Windows Security Events Connector, I created a Data Collection Rule (DCR) to forward VM security logs to the LAW and Sentinel.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a chat window

AI-generated content may be incorrect.

## 15. Verify Logs in LAW

I ran the following query inside LAW to confirm that security logs were being collected:  
  
SecurityEvent  
  
This displayed all login events, including failed attempts.

A screenshot of a computer

AI-generated content may be incorrect.

## 16. Create a GeoIP Watchlist

I uploaded a GeoIP watchlist into Microsoft Defender to map attacker IP addresses to their geographic locations.

A screenshot of a computer

AI-generated content may be incorrect.

## 17. Validate Watchlist Query

I verified the watchlist integration by running:  
  
\_GetWatchlist("geoip")  
  
This returned attacker IP addresses along with their latitude, longitude, and country details.

A screenshot of a computer

AI-generated content may be incorrect.

## 18. Build a Sentinel Workbook (Heatmap Visualization)

Finally, I created a Sentinel Workbook with a map-based visualization using a custom KQL query. This allowed me to generate a heatmap of attack origins, highlighting global sources of login attempts against the VM.

A screenshot of a computer

AI-generated content may be incorrect.

# Final Results

- Successfully simulated a vulnerable VM environment.  
- Captured and analyzed real-world brute-force login attempts.  
- Forwarded logs into a SIEM solution (Microsoft Sentinel).  
- Built visual dashboards to track attacker locations globally.  
  
This project highlights my hands-on experience with Azure Security tools, SIEM/SOC monitoring, and real-world threat analysis.