

Building a Cloud Honeypot for Real-World Threat Intelligence via Azure Sentinel

Deployed a deliberately exposed Windows VM honeypot in Azure to simulate a vulnerable asset, attracting real-world brute-force attacks. Integrated with Microsoft Sentinel and Log Analytics Workspace to collect, enrich, and visualize threat data in near real-time.

Key Achievements:

- Captured over **6,000+ RDP brute-force attempts** (Event ID 4625) within 40 minutes
- Enriched attacker IPs with **GeoIP data** via Sentinel Watchlists
- Built a **live attack map** showing global threat origin using KQL and Sentinel Workbooks
- Created scheduled detection rules to trigger incidents for high-volume login failures

SOC & Detection Engineering Skills:

- SIEM data ingestion (Azure Monitoring Agent → LAW → Sentinel)
- Threat analysis using **Kusto Query Language (KQL)**
- MITRE ATT&CK mapping: T1110, T1078.003, T1083
- SOC use case development and enrichment workflows

Threat Intel Insights:

- Attacks sourced from **2 countries** (Top:  Poland and  Brazil)
- Accounts targeted: Administrator, admin, svcuser
- Botnet-like behavior via **rapid IP rotation**

 This project replicates real SOC detection workflows and showcases my skills in threat collection, telemetry processing, and adversary analysis — all critical for modern security operations.

Step-by-Step Honeypot Deployment & Monitoring in Azure Sentinel

1. Azure Subscription Setup

- Navigate to **Azure Free Trial**
- Sign up with **personal email** (non-work/school)
- Verify identity with **credit card**
- Access portal: <https://portal.azure.com>

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a banner with the text "Hi ohh, see what more you can get from your Azure free account." Below it, a message says "You've got 29 days left to use the remaining \$200.00 of your free credit. [See what's included.](#)". There are four cards with icons: a laptop for learning, a video camera for demos, a person icon for support, and a magnifying glass for resources. Below these are sections for "Azure services" with icons for various services like Compute, Storage, Databases, and Machine Learning.

2.Resource Group Creation 📦

- **Portal search:** Resource groups
- Click **Create**
- Configure:
 - **Subscription:** Your subscription
 - **Name:** Kali-SOC-Lab
 - **Region:** East US 2
- Click **Review + Create → Create**

Click Review + Create → Create

The screenshot shows the Microsoft Azure Resource Groups page. At the top, there is a navigation bar with links like Home, OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. Below the navigation bar, the main title is "Resource groups". A message at the top says, "You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience." There are filter options for "Subscription equals all" and "Location equals all". The table below lists two resource groups:

Name	Subscription	Location
Kali-SOC-Lab	Azure subscription 1	East US 2
testresourcegroup	Azure subscription 1	West US

At the bottom, there is a "Display count" dropdown set to 10 and a "Give feedback" link.

The screenshot shows the Microsoft Azure "Create virtual network" wizard on the "Security" step. The title is "Create virtual network". The tabs at the top are Basics, Security (which is selected), IP addresses, Tags, and Review + create. A note says, "Enhance the security of your virtual network with these additional paid security services. Learn more." Under "Virtual network encryption", there is a checkbox labeled "Virtual network encryption". In the "Azure Bastion" section, it says, "Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. Learn more." At the bottom, there are "Previous" and "Next" buttons, and a "Review + create" button.

3. Virtual Network Setup

- Portal search: Virtual networks
- Click **Create**
- Configure:

- **Resource group:** kali-soc-lab
- **Name:** vnet-soc-lab
- **Region:** East US 2
- Accept defaults → **Review + Create** → **Create**

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The 'IP addresses' tab is active. A single subnet named 'default' is configured with an IP address range of 10.0.0.0/16, covering 65,536 addresses. The range 10.0.0.0 - 10.0.255.255 is listed below. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons.

4.Honeypot VM Deployment 🖥🎯

- Portal search: Virtual machines
- Click **Create** → **Azure virtual machine**
- Configure:
 - **Resource group:** kali-soc-lab
 - **VM name:** CORP-NET-East2
 - **Region:** East US 2
 - **Image:** Windows 10 Pro
 - **Size:** Standard_D2s_v3
 - **Username:** labuser
 - **Password:** ComplexPassword!
 - **Public inbound ports:** Allow selected ports → RDP (3389)

💡 Networking tab:

- **Virtual network:** vnet-soc-lab
- **Subnet:** default

→ **Review + Create** → **Create**

Screenshot of the Microsoft Azure portal showing the creation of a virtual network named "Vnet-SOC-Lab".

Create virtual network - 4

https://portal.azure.com/?ocid=AI Dcmmfq865whp_SEM_k_EAlaIQobChMI99rX5NWSjgMVUcfUAR25jBBfEAA

Microsoft Azure | Private browsing | 13:04 | +

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Microsoft Azure | Upgrade | Search resources, services, and docs (G+)

ohno961@gmail.com DEFAULT DIRECTORY

Home > Network foundation | Virtual networks >

Create virtual network

Review + create

Basics Security IP addresses Tags Review + create

Resource Group: Kali-SOC-Lab

Name: Vnet-SOC-Lab

Region: East US 2

Security

Azure Bastion: Disabled

Azure Firewall: Disabled

Azure DDoS Network Protection: Disabled

IP addresses

Address space: 10.0.0.0/16 (65,536 addresses)

Next Create Give feedback

Vnet-SOC-Lab-1751065506959 | Overview

Deployment successful

Deployment 'Vnet-SOC-Lab-1751065506959' to resource group 'Kali-SOC-Lab' was successful.

Go to resource Pin to dashboard

Overview

Inputs Outputs Template

Deployment is in progress

Deployment name: Vnet-SOC-Lab-1751065506959
Subscription: Azure subscription 1
Resource group: Kali-SOC-Lab

Start time: 6/27/2025, 1:05:10 PM
Correlation ID: edde6a3e-1650-4293-896b-18929abd...

Deployment details

Resource	Type	Status	Operation details
Vnet-SOC-Lab	Virtual network	Created	Operation details

Give feedback Tell us about your experience with deployment

Add or remove favorites by pressing Ctrl + Shift + F

The screenshot shows the Azure portal interface with the title "Create a virtual machine". The user is on the first step of the wizard, "Instance details".

Virtual machine name: CORP-NET-East2

Region: (US) East US 2

Availability options: Availability zone

Zone options: Self-selected zone (selected), which allows choosing up to 3 availability zones, one VM per zone.

Availability zone: Zone 1

A note at the bottom states: "You can now select multiple zones. Selecting multiple zones will create one VM per zone." with a "Learn more" link.

Navigation buttons: < Previous, Next : Disks >, Review + create, Give feedback.

The screenshot shows the Azure portal interface with the title "Create a virtual machine". The user is on the second step of the wizard, "Security type".

Security type: Trusted launch virtual machines

Image: Windows 10 Pro (ZH-CN), version 22H2 - x64 Gen2 (free services eligible)

VM architecture: x64 (selected), with a note: "Arm64 is not supported with the selected image."

Run with Azure Spot discount:

A note at the bottom states: "You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription." with a "Learn more" link.

Navigation buttons: < Previous, Next : Disks >, Review + create, Give feedback.

Create a virtual machine

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

Username * labuser

Password * Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None | Allow selected ports

Select inbound ports * RDP (3389)

⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab.

< Previous | Next : Disks > | Review + create | Give feedback

Kali-SOC-Lab Resource group

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Name ↑

- Kali-SOC-Lab
- NetworkWatcherRG
- testresourcegroup

Showing 1 - 3 of 3. Display 10 count:

Name	Type	Location
CORP-NET-East2	Virtual machine	East US 2
CORP-NET-East2-ip	Public IP address	East US 2
CORP-NET-East2-nsg	Network security group	East US 2
corp-net-east2204_z1	Network Interface	East US 2
CORP-NET-East2_OsDisk_1_d69f2a99173b481fbab...	Disk	East US 2
Vnet-SOC-Lab	Virtual network	East US 2

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBal...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Priority	Name	Port	Protocol	Source	Destination	Action
100	This_is_DANGER_...	Any	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBal...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

5. Security Hardening (Intentional Exposure) ! 🚨

- Post-deployment → VM resource → **Networking**
- Locate **NSG name** → Click link

💡 Modify inbound rules:

- Delete default **RDP** rule
- Add new rule:
 - **Source:** Any
 - **Source ports:** *
 - **Destination:** Any
 - **Service:** Custom
 - **Destination ports:** *
 - **Protocol:** Any
 - **Action:** Allow
 - **Priority:** 100
 - **Name:** THIS_IS_DANGER

→ Click **Add** → **Save**

 RDP into VM:

- Use **public IP** from VM overview
- Credentials: labuser / ComplexPassword!

 Inside VM:

- Open Windows Search → wf.msc
- Turn off firewall for all profiles (Domain / Private / Public)

The screenshot shows two separate views of the Microsoft Azure portal.

Top View (Virtual Machine):

- Title:** CORP-NET-East2 - Microsoft Azure
- Region:** East US 2 (Zone 1)
- Status:** Running
- Subscription:** Azure subscription 1
- Tags:** None
- Networking:** Public IP address: 20.55.248.27, Virtual network/subnet: vnet-SOC-Lab/default, DNS name: Not configured
- Health state:** Not configured
- Time created:** 6/27/2025, 11:21 PM UTC

Bottom View (Log Analytics Workspaces):

- Title:** Log Analytics workspaces - Microsoft Azure
- Message:** You are viewing a new version of the Browse experience. Some features may be missing. Click here to access the old experience.
- Filter:** Subscription equals all, Resource Group equals all, Location equals all
- Result:** No log analytics workspaces to display.
- Buttons:** Create, Learn more, Give feedback.

6. Log Analytics Workspace

- **Portal search:** Log Analytics workspaces
- **Click Create**
- **Configure:**
 - **Resource group:** kali-soc-lab

- **Region:** East US 2
→ Review + Create → Create

The screenshot shows the Microsoft Log Analytics OMS Overview page in a browser. The URL is https://portal.azure.com/?ocid=AI0Cmmfq865whp_SEM_k_EAlalQobChMI99rX5NWSjgMVuCfUAR25jBBfp. The page displays a deployment status message: "Your deployment is complete". It shows deployment details: Deployment name: Microsoft.LogAnalyticsOMS, Subscription: Azure subscription 1, Resource group: Kali-SOC-Lab. The start time was 6/27/2025, 2:28:26 PM, and the Correlation ID is 0bf767b2-6b01-42f7-b157-a3d072678... Below the main content, there are sections for "Cost management", "Microsoft Defender for Cloud", "Free Microsoft tutorials", and "Work with an expert". A sidebar on the left lists "Overview", "Inputs", "Outputs", and "Template". At the bottom, there are links for "Give feedback" and "Tell us about your experience with deployment".

7. Microsoft Sentinel Deployment 🔎

- Portal search: Microsoft Sentinel
- Click **Create** → Select law-soc-lab-0001 workspace → **Add**

No Microsoft Sentinel to display

See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise.

[+ Create](#) [Learn more](#)

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
LAW-SOC-Lab-0001	eastus2	kali-soc-lab	Azure subscription 1	Default Directory

Add Microsoft Sentinel to a workspace

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Add

8.Log Collection Configuration

- In Sentinel → Content hub → Search: **Windows Security Events**
- Click **Install**
- Post-install → **Manage** → Open connector page

 Create data collection rule:

- **Name:** dcr-windows-secevents
- **Resources:** Select corp-net-east2 VM
- **Collect:** All Security Events
→ Review + Create → Create

Screenshot of Microsoft Azure Microsoft Sentinel Content hub page showing the 'Content hub' section. The search bar shows 'Search...' and the search term 'security events'. The results table shows one item: 'Windows Security Events' by Microsoft Provider, status 'In progress', and source 'Solution'. A message box indicates 'Install in progress' and 'Installing 1 item.'

Content title	Status	Content source
Windows Security Events	In progress	Solution

Microsoft Sentinel | Content hub

Selected workspace: 'faw-soc-lab-0001'

Search...

397 Solutions | 310 Standalone contents | 0 Installed | 0 Updates

Content title Status Content source

Windows Security Events In progress Solution

No solution selected
Select a solution to view more details

Install in progress
Installing 1 item.

Screenshot of Microsoft Azure portal showing the Windows Security Events page and the CORP-NET-East2 VM extensions + applications page.

Windows Security Events

74 Installed content items | **22** Configuration needed

Windows Security Events

Microsoft Provider | Microsoft Support | Version 3.0.9

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

Manage | Actions | View details

No templates selected
Select templates to view more details

CORP-NET-East2 | Extensions + applications

Virtual machine

Search | Overview | Activity log | Access control (IAM) | Tags | Diagnose and solve problems | Resource visualizer | Extensions + applications | Operating system | Configuration

What extensions can help me keep my virtual machine secure? | What is the difference between VM applications and extensions? | What are the types of VM extensions available?

Extensions | VM Applications

+ Add | Refresh | Update | Enable automatic upgrade | Disable automatic upgrade | Feedback

Name	Type	Version	Latest Version	Status	Automat
enablevmAccess	Microsoft.Compute.VM...	2.4.14	2.4.14.0	Provisioning succeeded	Not supp

Add or remove favorites by pressing **Ctrl + Shift + F**

Screenshot of Microsoft Azure Portal showing the creation of a Data Collection Rule for Windows Security Events via AMA.

Create Data Collection Rule

Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other applications. [Learn more](#)

Subscriptions	Resource Groups	Resource Types	Locations
Selected: All	Selected: All	Selected: All	Selected: All

Search to filter items... Show Selected

Scope	Resource Type	Location
Azure subscription 1		
kali-soc-lab		
CORP-NET-East2	microsoft.compute/virtualmachines	East US 2

< Previous Next: Collect >

Windows Security Events via AMA

Disconnected Status Microsoft Provider Last Log Received

Description: You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received: --

Content source: Windows Security Events Version: 1.0.0

Author: Microsoft Supported by: Microsoft Corporation | Email

CORP-NET-East2 | Extensions + applications

Virtual machine

Search: What extensions can help me keep my virtual machine secure? What is the difference between VM applications and extensions? What are the types of VM extensions available?

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer

Extensions VM Applications

+ Add Refresh Update Enable automatic upgrade Disable automatic upgrade Feedback

Search to filter items...

Showing all 2 items

Name	Type	Version	Latest Version	Status	Automat
AzureMonitorWindowsA...			1.36.0.0	(unavailable)	Not supp
enablevmAccess	Microsoft.Compute.VM...	2.4.14.0		Provisioning succeeded	Not supp

Extensions + applications Operating system Configuration

Add or remove favorites by pressing Ctrl + Shift + F

The screenshot shows the Microsoft Azure Log Analytics workspace overview page for 'LAW-SOC-Lab-0001'. The page includes a search bar, a delete button, and a message about the transition to Azure Monitor Agent. It displays workspace details such as name, resource group, status, location, subscription, and operational issues. A 'Logs' section is open, showing a 'New Query 1' editor with the query 'SecurityEvent'. The results pane shows an error message: 'Query could not be parsed at " on line [2,2]'. The left sidebar lists various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Resource visualizer, Settings, Classic, Monitoring, Automation, Help, and Get Started.

Log Analytics ...

LAW-SOC-Lab-0001

Log Analytics workspace

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Resource visualizer

Settings

Classic

Monitoring

Automation

Help

Get Started

Recommendations

New Query 1*

Run

Time range : Last 24 hours

Show : 1000 results

KQL mode

1 SecurityEvent

2 |

Results

Chart

Query could not be parsed at " on line [2,2]

Line: 2

Position: 2

Request id: 81bf0f80-1b59-440d-b012-23f230614334

Screenshot of Microsoft Azure Portal showing the Extensions + applications page for a virtual machine named CORP-NET-East2.

The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, and Disks. The Extensions + applications tab is selected.

The main content area displays two extensions listed:

Name	Type	Version	Latest Version	Status
AzureMonitorWindowsAgent	Microsoft.Azure.Monitor...	1.36.0.0	1.36.0.0	Provisioning succeeded
enableVmAccess	Microsoft.Compute.VM...	2.4.14	2.4.14.0	Provisioning succeeded

Below the table, there is a search bar labeled "Search to filter items..." and a "Feedback" link.

Log Analytics workspaces section:

The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, and Logs. The Logs tab is selected.

The main content area shows a "New Query 1" pane with the following query:

```
SecurityEvent
```

The results table shows the following data:

TimeGenerated [UTC]	Account	AccountType	Computer
6/28/2025, 12:55:08.828 AM	CORP-NET-East2\labuser	User	CORP-NET-East2
6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2
6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2
6/28/2025, 12:39:57.684 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2
6/28/2025, 12:39:57.684 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2

Screenshot of Microsoft Azure Log Analytics workspace (LAW-SOC-Lab-0001) showing the Logs page.

The left sidebar shows navigation links: Home, Log Analytics workspaces, LAW-SOC-Lab-0001, Create, Open recycle bin, and three dots.

A message box indicates: "You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience."

The main area displays the title "LAW-SOC-Lab-0001 | Logs" and "Log Analytics workspace".

The left sidebar under "Logs" includes: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Classic, Monitoring, Automation, and Help.

The search bar contains "Search" and a magnifying glass icon.

The results table shows 1 SecurityEvent:

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
6/28/2025, 12:26:15.923 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:26:15.919 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:26:13.615 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:26:13.614 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:26:13.614 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:26:13.604 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:26:13.602 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:26:11.337 AM	WORKGROUP\CORP-NE...	Machine	CORP-NET-East2	Microsoft-Windows-Security

Details: 0s 856ms | Display time (UTC+00:00) | Query details | 11 - 20 of 20

Screenshot of Microsoft Azure Log Analytics workspace (LAW-SOC-Lab-0001) showing the Logs page with a custom query.

The left sidebar shows navigation links: Home, Log Analytics workspaces, LAW-SOC-Lab-0001, Create, Open recycle bin, and three dots.

The main area displays the title "LAW-SOC-Lab-0001 | Logs" and "Log Analytics workspace".

The left sidebar under "Logs" includes: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Classic, Monitoring, Automation, and Help.

The search bar contains "Search" and a magnifying glass icon.

The results table shows 1 SecurityEvent:

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
6/28/2025, 12:56:36.373 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:56:36.373 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:56:35.175 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:56:35.175 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:56:34.606 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:56:34.606 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security
6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-East2	Microsoft-Windows-Security

Details: 0s 856ms | Display time (UTC+00:00) | Query details | 11 - 20 of 20

Query details: New Query 1* | Run | Time range : Last 24 hours | Show : 1000 results | QL mode | Save | Share | ... | Queries hub

```
1 SecurityEvent
2 | where Account == "NT AUTHORITY\SYSTEM"
```

Microsoft Azure | Upgrade | Search resources, services, and docs (G+) | Copilot | ohno961@gmail.com | DEFAULT DIRECTORY (OHHN096...)

Home > Log Analytics workspaces > LAW-SOC-Lab-0001

LAW-SOC-Lab-0001 | Logs

New Query 1* Time range : Last 24 hours Show : 1000 results KQL mode

```
1 SecurityEvent
2 | where Account == "NT AUTHORITY\SYSTEM"
3 | project TimeGenerated, Account, Computer, EventID, Activity,IpAddress
```

Results Chart

TimeGenerated [UTC]	Account	Computer	EventID	Activity	IpAddress
> 6/28/2025, 12:56:36.373 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:56:36.373 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-
> 6/28/2025, 12:56:35.175 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:56:35.175 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-
> 6/28/2025, 12:56:34.606 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:56:34.606 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-
> 6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-

0s 864ms | Display time (UTC+00:00) | Query details | 7 - 16 of 16

Microsoft Azure | Upgrade | Search resources, services, and docs (G+) | Copilot | ohno961@gmail.com | DEFAULT DIRECTORY (OHHN096...)

Home > Log Analytics workspaces > LAW-SOC-Lab-0001

LAW-SOC-Lab-0001 | Logs

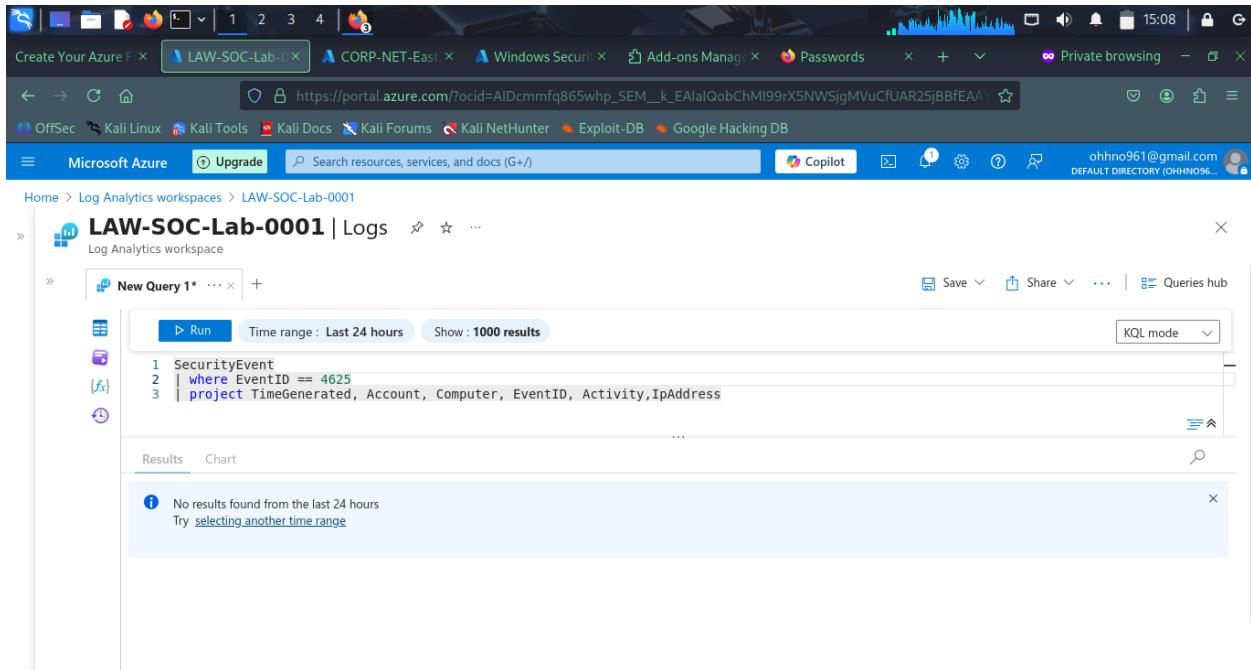
New Query 1* Time range : Last 24 hours Show : 1000 results KQL mode

```
1 SecurityEvent
2 | where Account == "NT AUTHORITY\SYSTEM"
3 | project TimeGenerated, Account, Computer, EventID, Activity,IpAddress
```

Results Chart

TimeGenerated [UTC]	Account	Computer	EventID	Activity	IpAddress
> 6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:50:20.610 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-
> 6/28/2025, 12:39:57.684 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:39:57.684 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-
> 6/28/2025, 12:31:12.610 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:31:12.610 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-
> 6/28/2025, 12:31:10.958 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:31:10.958 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-
> 6/28/2025, 12:30:06.765 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4672	4672 - Special privileges assign...	-
> 6/28/2025, 12:30:06.765 AM	NT AUTHORITY\SYSTEM	CORP-NET-East2	4624	4624 - An account was successf...	-

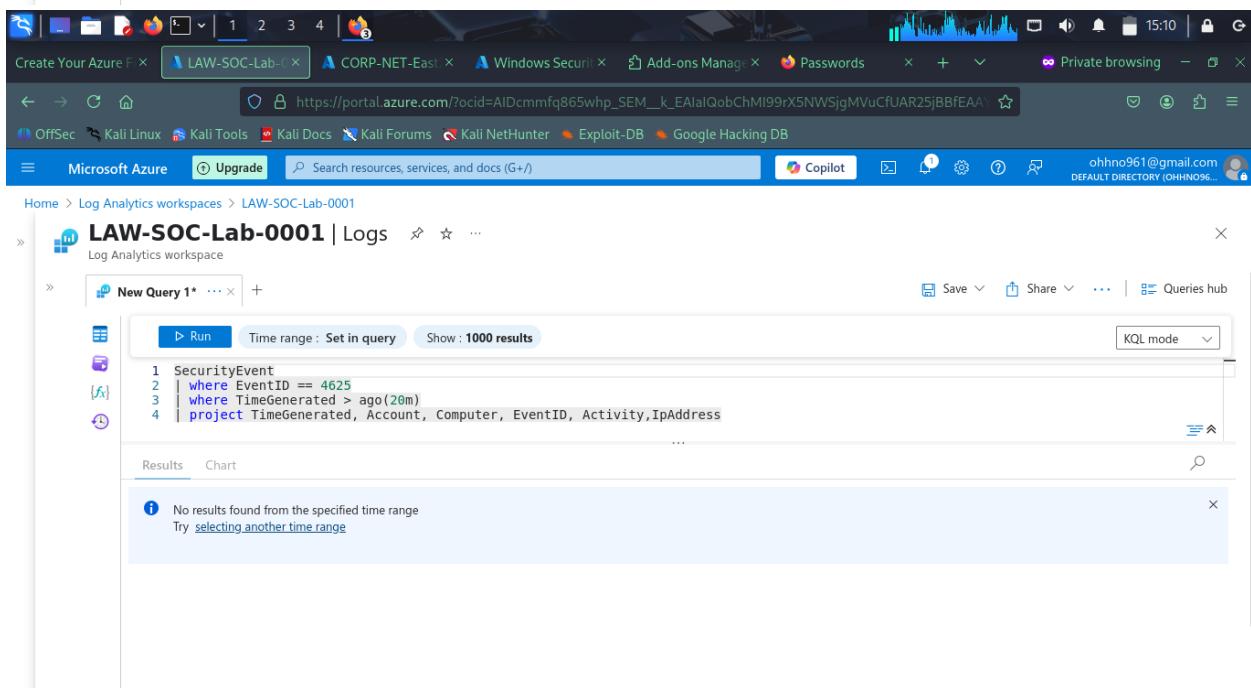
0s 864ms | Display time (UTC+00:00) | Query details | 7 - 16 of 16



LAW-SOC-Lab-0001 | Logs

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

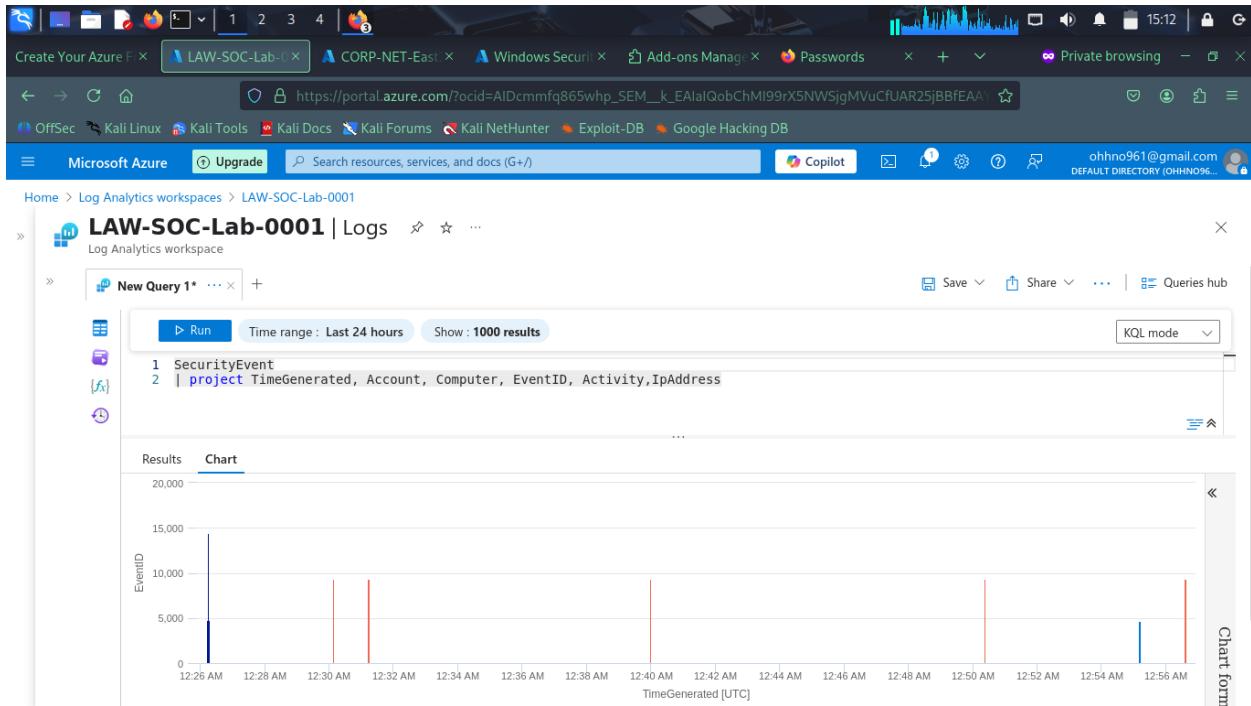
No results found from the last 24 hours
Try [selecting another time range](#)



LAW-SOC-Lab-0001 | Logs

```
1 SecurityEvent
2 | where EventID == 4625
3 | where TimeGenerated > ago(20m)
4 | project TimeGenerated, Account, Computer, EventID, Activity,IpAddress
```

No results found from the specified time range
Try [selecting another time range](#)



9. Geolocation Enrichment

- Download GeoIP CSV (replace with actual source)
- In Sentinel → Watchlists → **Add new**
 - **Name:** GeoIP
 - **Alias:** GeoIP
 - **Description:** "IP geolocation mapping"
 - **Upload CSV**
 - **Search key:** Network
→ **Create**

The screenshot shows the Microsoft Sentinel Watchlist wizard page. At the top, there are tabs for General, Source (which is selected), and Review + create. Under the Source tab, there is a dropdown for File type set to "CSV file with a header (.csv)" and a field for Number of lines before row with headings set to 0. Below this, there is a Blob SAS URL (Preview) section showing a preview of a CSV file named "geoip-summarized.csv" with details like file size (2788293 bytes), start date (5/15/2025), and expiry date (12/31/2029). A search key field is set to "network". A "Reset" button is visible. Below the form, there is a "File preview" section showing the first 50 rows and first 5 columns of the CSV file.

The screenshot shows the Microsoft Sentinel Watchlist creation confirmation page. The title bar says "Microsoft Sentinel | Watchlist". It displays two success messages: one for creating a watchlist named [geoip] and another for creating watchlist items named [geoip]. Both messages state that the submission was successful and that it may take several minutes for the items to become available. Below the messages, there are sections for "My Watchlists" and "Templates (Preview)".

The screenshot shows the Microsoft Sentinel Watchlist page. At the top, there are two sections: 'Watchlists' (0) and 'Watchlist Items' (0). Below this, the 'My Watchlists' section displays a table with one row:

Name	Alias	Source	Created time	Last updated
geoip	geoip	Remote file	6/27/2025, 3:21:09 PM	6/27/2025, 3:21

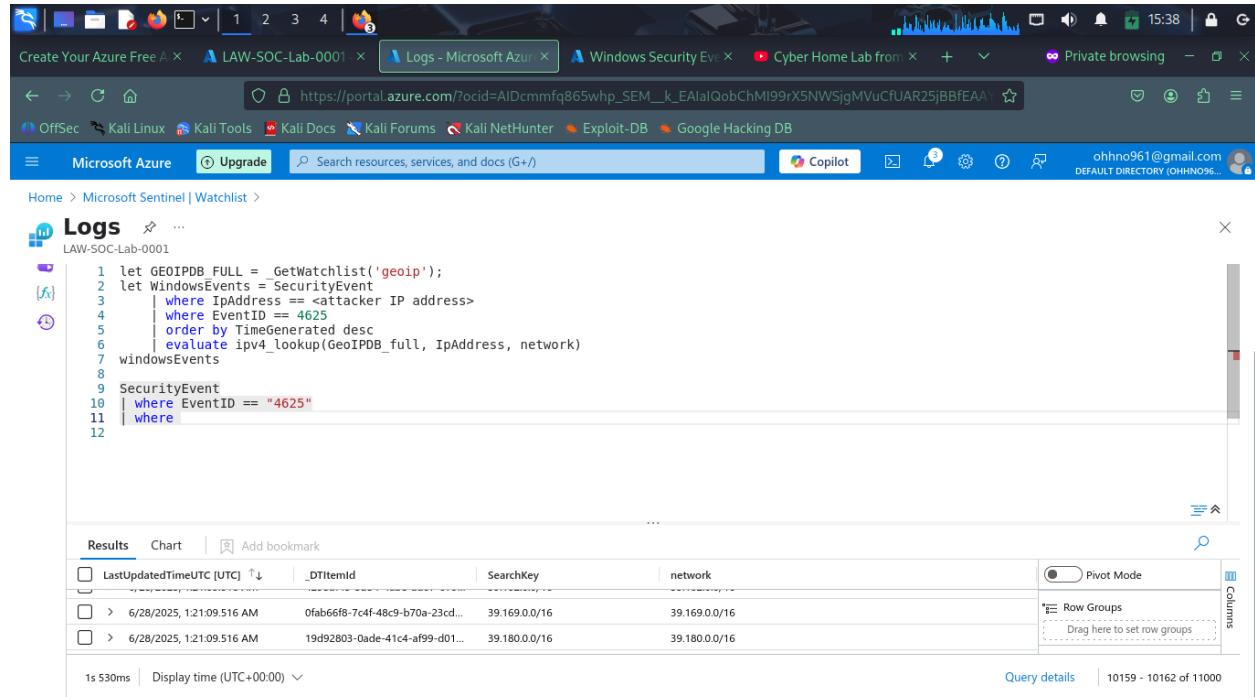
The screenshot shows the Microsoft Log Analytics interface under the 'Logs' section. A query has been run against the 'geoip' watchlist. The results table shows the following data:

LastUpdatedTimeUTC [UTC]	_DTItemId	SearchKey	cityname	countryname	latitude
6/28/2025, 1:21:09.516 AM	cd5d1b02-3b53-478a-902e-89...	24.89.0.0/16	Fort Qu'Appelle	Canada	50.7664
6/28/2025, 1:21:09.516 AM	1cca3bbc-8cda-400b-b92b-fb...	24.92.0.0/16	Mentor	United States	41.6868
6/28/2025, 1:21:09.516 AM	fedbae3-b78a-46a4-9fa7-181...	24.116.0.0/16	Idaho Falls	United States	43.4736
6/28/2025, 1:21:09.516 AM	18d091f4-c836-45c3-bd2c-ca0...	24.138.0.0/16	Dartmouth	Canada	44.6747
6/28/2025, 1:21:09.516 AM	7ac3944a-70f5-4388-a804-5ab...	24.156.0.0/16	Kingman	United States	35.1328
6/28/2025, 1:21:09.516 AM	0e07c9c5-2f38-472c-91f2-b2af...	24.180.0.0/16	San Luis Obispo	United States	35.2612
6/28/2025, 1:21:09.516 AM	14eb1351-df1-4c28-bcb3-49b...	24.198.0.0/16	Covina	United States	34.0896
6/28/2025, 1:21:09.516 AM	53ef5693-77a-4cb6-ba62-654...	24.203.0.0/16	Jonquiere	Canada	48.4294

10 KQL Threat Hunting 🧠🔍

- In Log Analytics → Logs
- Run **failed login detection**:
- SecurityEvent
- | where EventID == 4625 // Failed logon
- | join kind=inner (GetWatchlist('GeoIP')) on \$left.IpAddress == \$right.Network

- | project TimeGenerated, Computer, AttackerIP=IpAddress,
- Country=CountryName, City=CityName, Latitude, Longitude
- | summarize Attempts=count() by AttackerIP, Country, City, Latitude, Longitude



The screenshot shows the Microsoft Azure Log Analytics interface. At the top, there are several tabs: "Create Your Azure Free A", "LAW-SOC-Lab-0001", "Logs - Microsoft Azure", "Windows Security Events", "Cyber Home Lab from X", and "Private browsing". Below the tabs, the URL is https://portal.azure.com/?ocid=AIQcmmfq865whp_SEM_k_EAlalQobChMI99rX5NWSjgMVuCfUAR25jBBFEAAY. The main navigation bar includes "Microsoft Azure", "Upgrade", "Search resources, services, and docs (G+)", "Copilot", and user information "ohhno961@gmail.com" and "DEFAULT DIRECTORY (OHHN96...)".

The page title is "Logs" under "LAW-SOC-Lab-0001". The query editor contains the following Kusto Query Language (KQL) code:

```

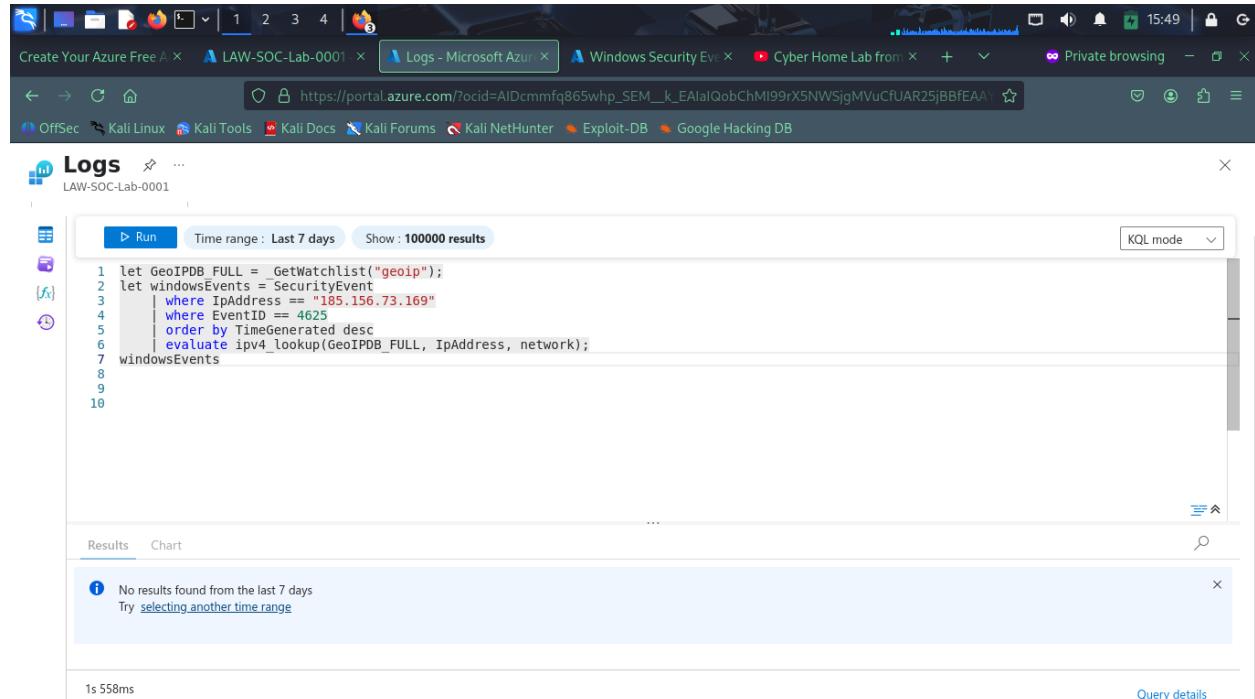
let GEOIPDB_FULL = _GetWatchlist('geoip');
let WindowsEvents = SecurityEvent
| where IPAddress == <attacker IP address>
| where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_full, IPAddress, network)
windowsEvents
SecurityEvent
| where EventID == "4625"
| where

```

The results table shows two rows of data:

LastUpdatedTimeUTC [UTC]	_DTIItemId	SearchKey	network
> 6/28/2025, 1:21:09.516 AM	0fab66f8-7c4f-48c9-b70a-23cd...	39.169.0.0/16	39.169.0.0/16
> 6/28/2025, 1:21:09.516 AM	19d92803-0ade-41c4-af99-d01...	39.180.0.0/16	39.180.0.0/16

Below the table, it says "1s 530ms | Display time (UTC+0:00)". On the right, there are "Query details" and "10159 - 10162 of 11000".



This screenshot shows the same Microsoft Azure Log Analytics interface as the previous one, but with a different query. The URL is https://portal.azure.com/?ocid=AIQcmmfq865whp_SEM_k_EAlalQobChMI99rX5NWSjgMVuCfUAR25jBBFEAAY. The results table shows a message: "No results found from the last 7 days. Try selecting another time range".

The query editor contains the following Kusto Query Language (KQL) code:

```

let Run Time range : Last 7 days Show : 100000 results
KQL mode
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
9
10

```

At the bottom, it says "1s 558ms" and "Query details".

Screenshot of Microsoft Sentinel Watchlist page:

Selected workspace: 'law-soc-lab-0001'

Watchlist items: 55K

Watchlist details for 'geoip':

- Provider: Microsoft
- Rows: 55K
- Created: 6/27/2025, 3:21:09 PM
- Status: Succeeded

Watchlist items table:

Name	Rows	Created
geoip	55K	6/27/2025, 3:21:09 PM

Log entry:

```
2025-06-27T03:21:09Z | geoip | Microsoft | 55K | Rows | 6/27/2025, 3:21:09 PM | Created time
```

Screenshot of Microsoft Sentinel Logs page:

New Query 1*

```
1 let GeoIPDB FULL = GetWatchlist("geoip");
2 let windowsEvents = SecurityEvent
3 | where countryname == Canada
4 | order by TimeGenerated desc
5 | evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
6 windowsEvents
7
8 SecurityEvent
9 | where EventID == "4625"
10
11
```

Results table:

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task
6/28/2025, 1:56:51.911 AM	WIN-OJ06LPP1P1\guest	User	CORP-NET-East2	Microsoft-Windows-Security-Audit	Security	1254
6/28/2025, 1:56:22.765 AM	WIN-OJ06LPP1P1\Administrador	User	CORP-NET-East2	Microsoft-Windows-Security-Audit	Security	1254

Logs - Microsoft Azure | Logs - Microsoft Azure | Cyber Home Lab from | Private browsing

https://portal.azure.com/?ocid=AIIDcmmfq865whp_SEM_k_EAlalQobChMI99rX5NWSjgMVuCfUAR25

Microsoft Azure | Upgrade | Search resources, services, and docs (G+)

ohno961@gmail.com | DEFAULT DIRECTORY

Home > Microsoft Sentinel | Watchlist >

Logs ...

LAW-SOC-Lab-0001

```
1 let GeoIPDB FULL = GetWatchlist("geoip");
2 let windowsEvents = SecurityEvent
3 | where countryname == Canada
4 | order by TimeGenerated desc
5 | evaluate ipv4_lookup(GeoIPDB_FULL,IpAddress, network);
6 windowsEvents
7
8 SecurityEvent
9 | where EventID == "4625"
10
11
```

Results Chart Add bookmark

PackageName	FailureReason	IpAddress	IpPort	KeyLength	LmPackageName	LogonProcessName
%%2313		177.207.233.155	59198	0	-	NtLmSsp
%%2313		177.207.233.155	56806	0	-	NtLmSsp

1s 46ms | Display time (UTC+00:00) ▾

Query details | 1 - 2 of 2

Logs - Microsoft Azure | Logs - Microsoft Azure | Cyber Home Lab from | Private browsing

https://portal.azure.com/?ocid=AIIDcmmfq865whp_SEM_k_EAlalQobChMI99rX5NWSjgMVuCfUAR25

Microsoft Azure | Upgrade | Search resources, services, and docs (G+)

ohno961@gmail.com | DEFAULT DIRECTORY

Home > Microsoft Sentinel | Watchlist >

Logs ...

LAW-SOC-Lab-0001

Run Time range : Last 24 hours Show : 100000 results KQL mode

```
1 let GeoIPDB FULL = GetWatchlist("geoip");
2 let windowsEvents = SecurityEvent
3 | where IPAddress == "177.207.233.155"
4 | where EventID == 4625
5 | order by TimeGenerated desc
6 | evaluate ipv4_lookup(GeoIPDB_FULL,IpAddress, network);
7 windowsEvents
8
9 SecurityEvent
10 | where EventID == "4625"
11
```

Results Chart Add bookmark

TimeGenerated [UTC] ↑	Account	AccountType	Computer	EventSourceName	Channel	Task
> 6/28/2025, 1:56:51.911 AM	WIN-OJ06LPP1P1\guest	User	CORP-NET-East2	Microsoft-Windows-Security-Audit	Security	125
> 6/28/2025, 1:56:22.765 AM	WIN-OJ06LPP1P1\Administrador	User	CORP-NET-East2	Microsoft-Windows-Security-Audit	Security	125

1s 534ms | Display time (UTC+00:00) ▾

Query details | 1 - 2 of 2

Logs

LAW-SOC-Lab-0001

```
let GeoIPDB_FULL = GetWatchlist("geoip");
let windowsEvents = SecurityEvent
| whereIpAddress == "177.207.233.155"
| where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL,IpAddress, network);
windowsEvents
SecurityEvent
| where EventID == 4625
```

Time range : Last 24 hours Show : 100000 results

KQL mode

sourcelid	_DTItemid	LastUpdatedTimeUTC [UTC]	SearchKey	cityname	countryname	latitude
bscriptions/632d7a25-d640-...	47b44616-ae10-4a70-adec-a8e...	6/28/2025, 1:21:09.516 AM	177.207.0.0/16	Carinhanha	Brazil	-14.2115
bscriptions/632d7a25-d640-...	47b44616-ae10-4a70-adec-a8e...	6/28/2025, 1:21:09.516 AM	177.207.0.0/16	Carinhanha	Brazil	-14.2115

1s 534ms | Display time (UTC+00:00) ▾

Query details | 1 - 2 of 2

Logs

LAW-SOC-Lab-0001

```
let GeoIPDB_FULL = GetWatchlist("geoip");
let windowsEvents = SecurityEvent
| whereIpAddress == "177.207.233.155"
| where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL,IpAddress, network);
windowsEvents
| project TimeGenerated, Computer,IpAddress, cityname, countryname
```

Time range : Last 24 hours Show : 100000 results

KQL mode

TimeGenerated [UTC] ↑	Computer	IpAddress	cityname	countryname
> 6/28/2025, 1:56:51.911 AM	CORP-NET-East2	177.207.233.155	Carinhanha	Brazil
> 6/28/2025, 1:56:22.765 AM	CORP-NET-East2	177.207.233.155	Carinhanha	Brazil

0s 682ms | Display time (UTC+00:00) ▾

Query details | 1 - 2 of 2

The screenshot shows the Microsoft Azure Log Analytics interface. At the top, there are several tabs: 'Create Your Azure Free A', 'LAW-SOC-Lab-0001', 'Logs - Microsoft Azur', 'Logs - Microsoft Azur', 'Cyber Home Lab from', and 'Private browsing'. Below the tabs, the URL is https://portal.azure.com/?ocid=AIcmmfq865whp_SEM_k_EAlaIQobChMI9rX5NWSjgMVUAR25. The main area is titled 'Logs' and shows a query editor with the following KQL code:

```

1 let GeoIPDB_FULL = GetWatchlist("geoip");
2 let windowsEvents = SecurityEvent
3 | whereIpAddress == "177.207.233.155"
4 | where EventID == 4625
5 | order by TimeGenerated desc
6 | evaluate ipv4_lookup(GeoIPDB_FULL, IPAddress, network);
7 windowsEvents
8 | project TimeGenerated, Computer, AttackerIp = IPAddress, cityname, countryname
9
10

```

The results table shows two rows of data:

	TimeGenerated [UTC]	Computer	AttackerIp	cityname	countryname
<input type="checkbox"/>	> 6/28/2025, 1:56:51.911 AM	CORP-NET-East2	177.207.233.155	Carinhanha	Brazil
<input type="checkbox"/>	> 6/28/2025, 1:56:22.765 AM	CORP-NET-East2	177.207.233.155	Carinhanha	Brazil

At the bottom of the interface, it says '0s 627ms | Display time (UTC+00:00) ▾' and 'Query details | 1 - 2 of 2'.

11. Attack Map Visualization

- In Sentinel → Workbooks → Add workbook
- Edit → Advanced Editor → Paste JSON template:

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the **Edit** button below each section to configure it or add more sections.

100
0

Heartbeat

SecurityEvent | Heartbeat | Usage

105 | 84 | 2

Editing query item: query - 0

Settings Advanced Settings Style Advanced Editor

Shown below is a JSON representation of the current item.
Any changes you make here will be reflected when you press 'Done Editing'.

```
1
```

Screenshot of Microsoft Azure Microsoft Sentinel Workbook interface showing a query editor and a map visualization.

Query Editor:

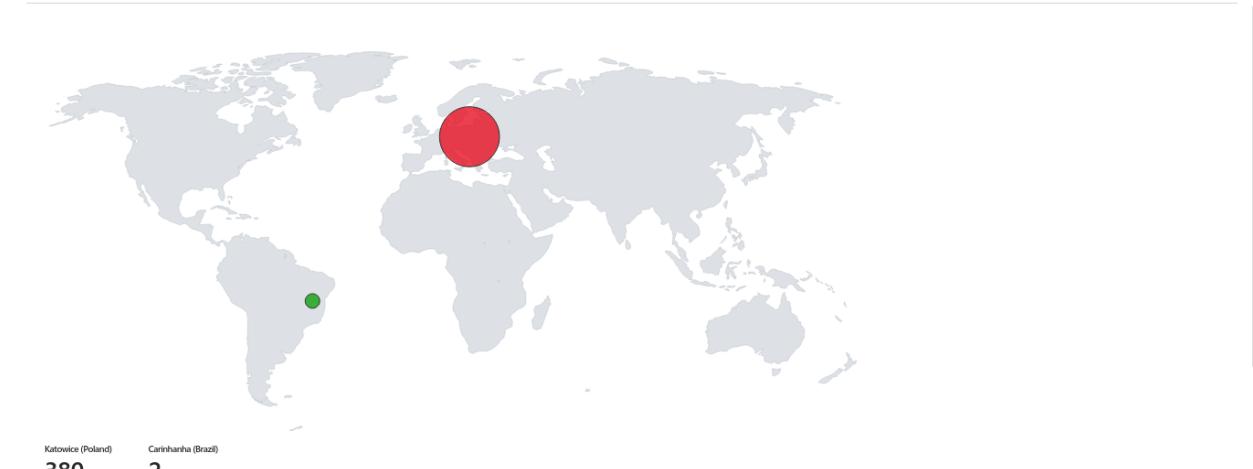
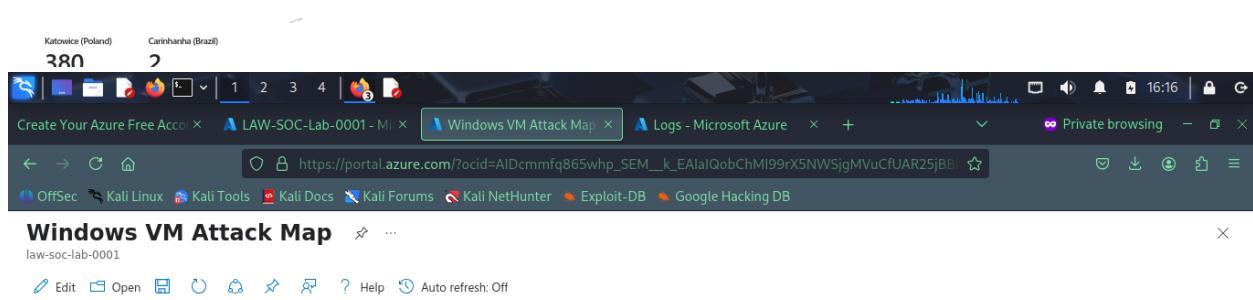
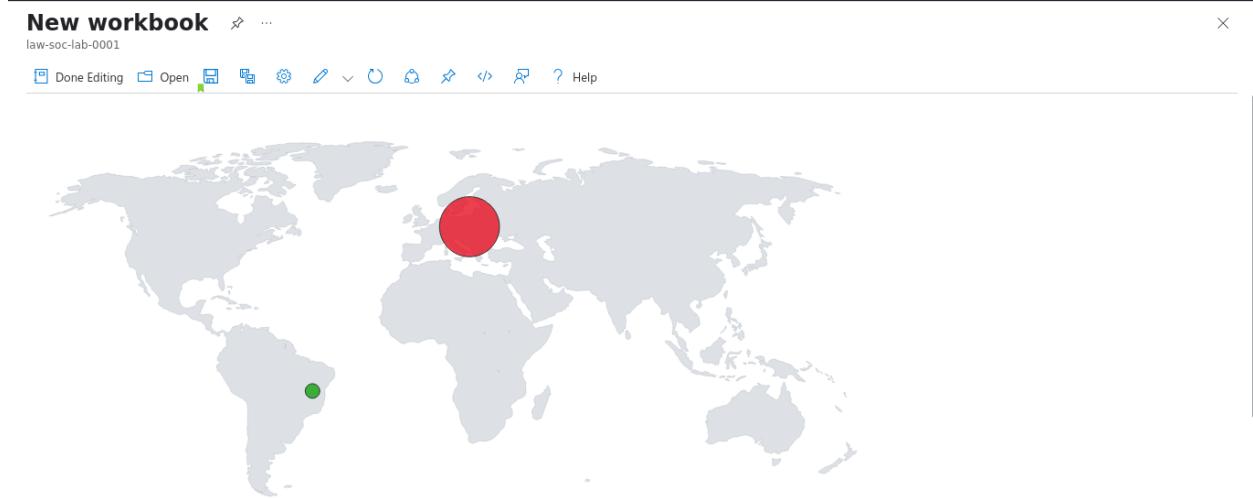
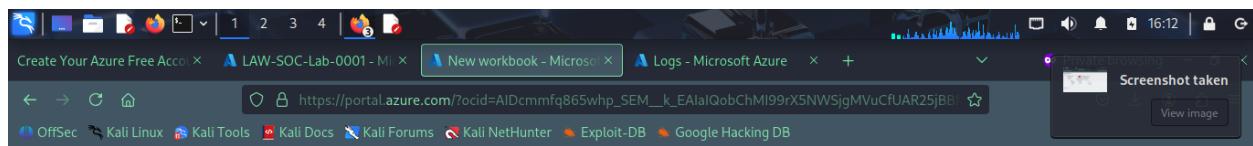
```
1 {
2   "type": 3,
3   "content": {
4     "version": "KqlItem/1.0",
5     "query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n| order by T desc\n| take 1000\n|\n  \"durationMs\": 2592000000
6     },
7     "queryType": 0,
8     "resourceType": "microsoft.operationalinsights/workspaces",
9     "visualization": "map",
10    "mapSettings": {
11      "lat": 52.2297,
12      "lon": 21.0122
13    }
14 }
```

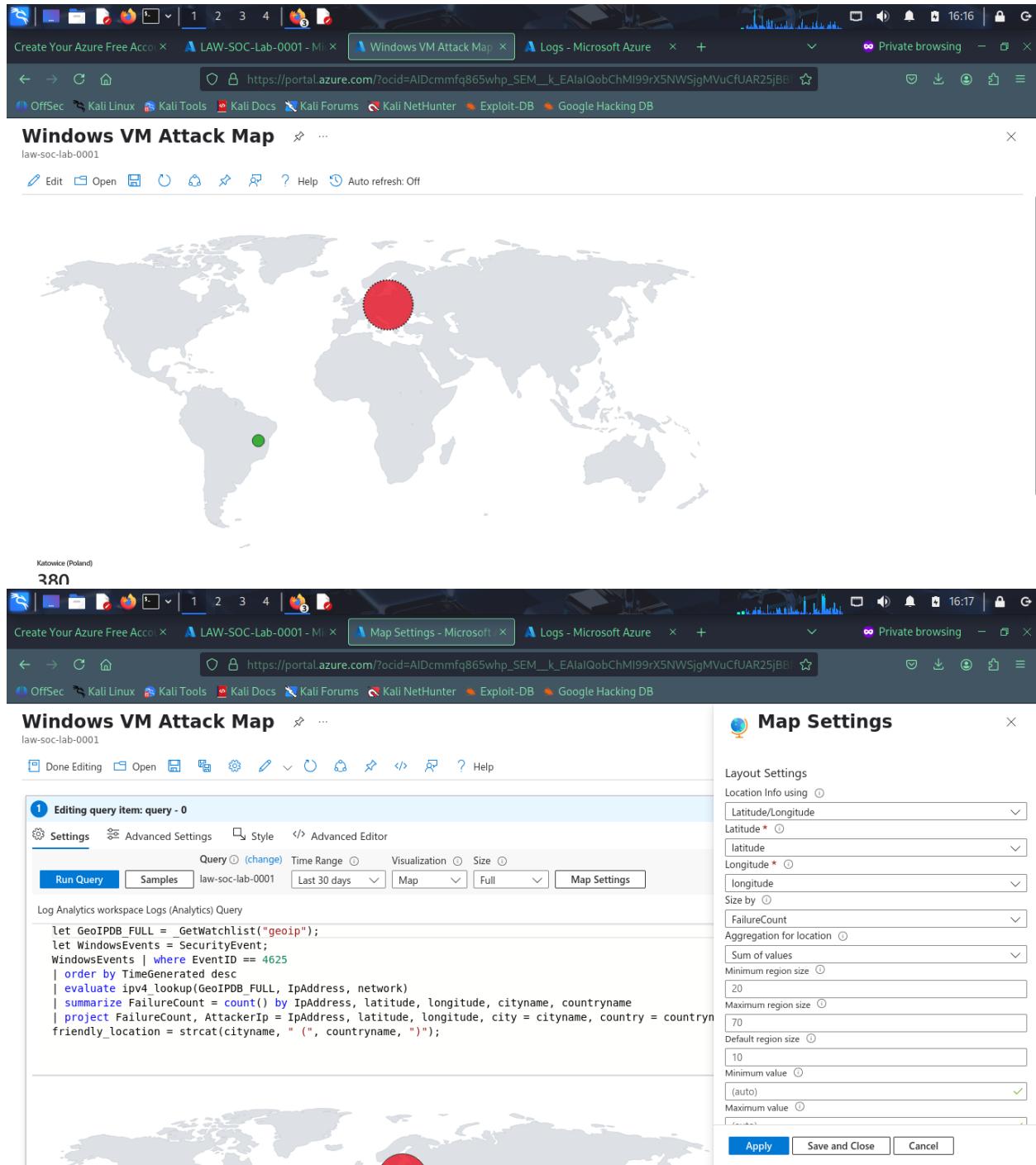
Map Visualization:

A world map with two green dots indicating event locations. One dot is labeled 'Katowice (Poland)' and the other is labeled 'Carinhanha (Brazil)'. The map shows continents and oceans in a grayscale color scheme.

Bottom Status Bar:

380 2





12.Incident Creation (Optional) 🚨🧩

- In Sentinel → Analytics → **Create scheduled rule**
- Configure:
 - **Query:**

SecurityEvent

```
| where EventID == 4625  
| where IpAddress != "Your_IP"
```

- **Threshold:** >5 events / 5m
- **Entity mapping:** IP → Address
- **Automated response:** Create incident

13.Cost Management

-  Always Stop VM when not in use
-  Delete kali-soc-lab after lab to prevent charges

Verification Checklist

-  NSG shows "Allow *" inbound rule
-  LAW populated with SecurityEvent table
-  Watchlist shows **55K+ GeoIP entries**
-  Attack map displays heat points within **60 mins**
-  Failed logons visible in KQL results (**Event ID 4625**)

Final Note: This lab demonstrates fundamental detection capabilities but lacks response workflows. In production SOCs, automate incident creation (e.g., via Sentinel playbooks) and integrate with ITSM tools like ServiceNow for end-to-end case management.