Azure Project: Setting up a honeypot + Sentinel and log analysis using KQL

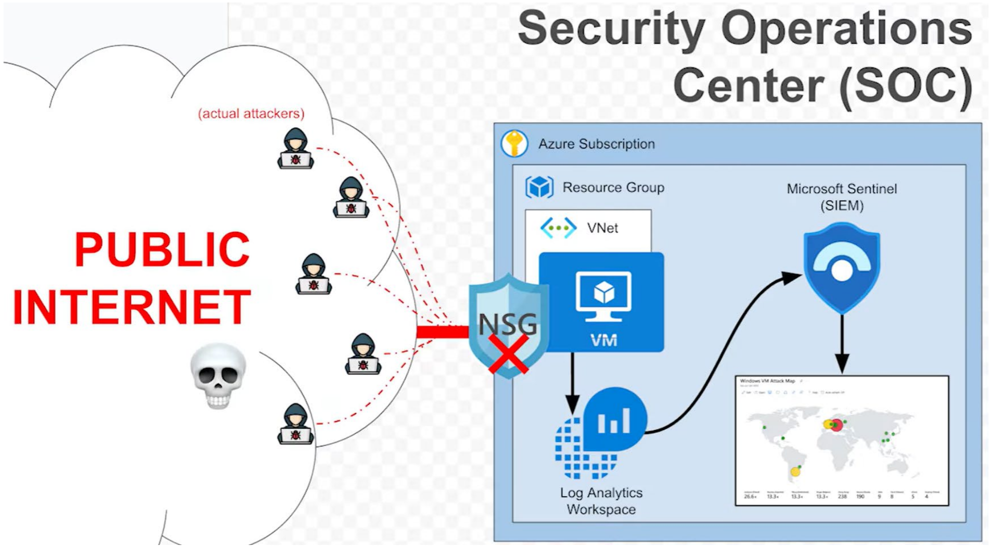
Objectives:

- Set up a honeypot to collect attack logs globally.
- Analyze and filter logs using KQL.
- Configure Microsoft Sentinel to view a comprehensive map of where the attacks are coming from.

Prerequisites:

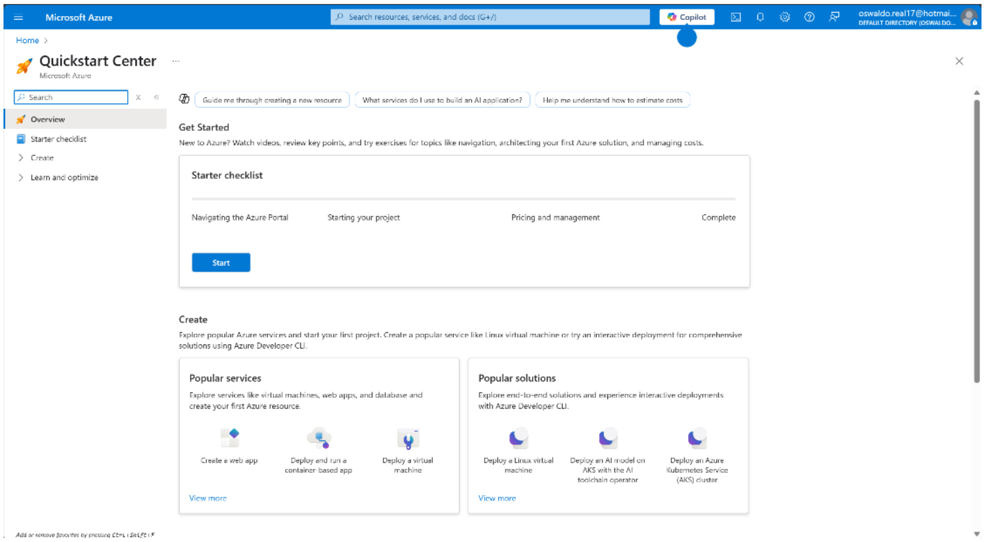
- Azure Portal
- Azure Sentinel
- Kusto Query Language
- Network Security groups

Project Topology:



To perform this lab, an Azure subscription is mandatory.

Once the Azure subscription was acquired, proceed to create a *Resource Group*, a Virtual Network, and a Virtual Machine. As is shown in the following pictures:


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
oswaldo.real17@hotmai...
DEFAULT DIRECTORY (OSWALDO...
Home
Search
Overview
Starter checklist
Create
Learn and optimize
Guide me through creating a new resource
What services do I use to build an AI application?
Help me understand how to estimate costs
Start
Create a web app
Deploy and run a container-based app
Deploy a virtual machine
Deploy a Linux virtual machine
Deploy an AI model on AKS with the AI toolchain operator
Deploy an Azure Kubernetes Service (AKS) cluster
View more
View more
Add or remove favorites by pressing Ctrl+Shift+F

Quickstart Center

Microsoft Azure

Get Started

New to Azure? Watch videos, review key points, and try exercises for topics like navigation, architecting your first Azure solution, and managing costs.

Starter checklist

Navigating the Azure Portal · Starting your project · Pricing and management · Complete

Create

Explore popular Azure services and start your first project. Create a popular service like Linux virtual machine or try an interactive deployment for comprehensive solutions using Azure Developer CLI.

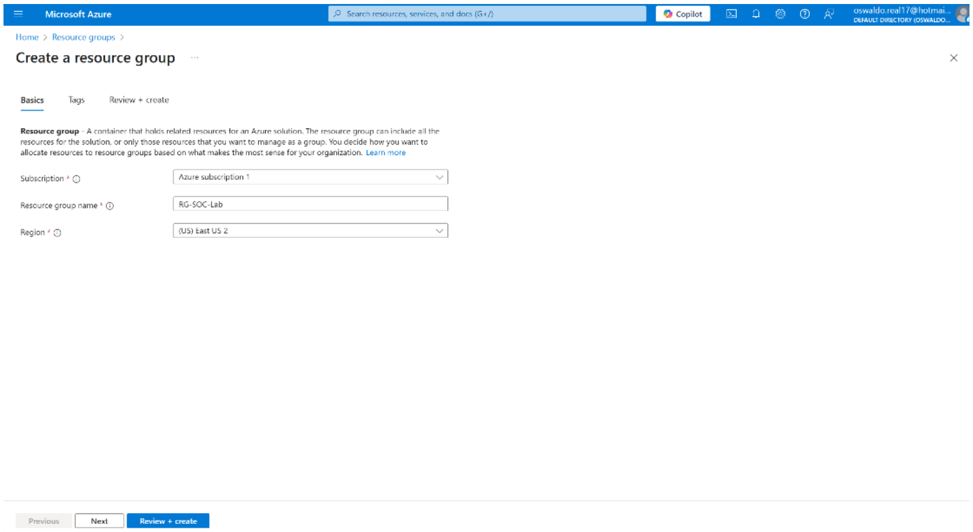
Popular services

Explore services like virtual machines, web apps, and database and create your first Azure resource.

Popular solutions

Explore end-to-end solutions and experience interactive deployments with Azure Developer CLI.

Figure1. Azure portal home page.



Create a resource group

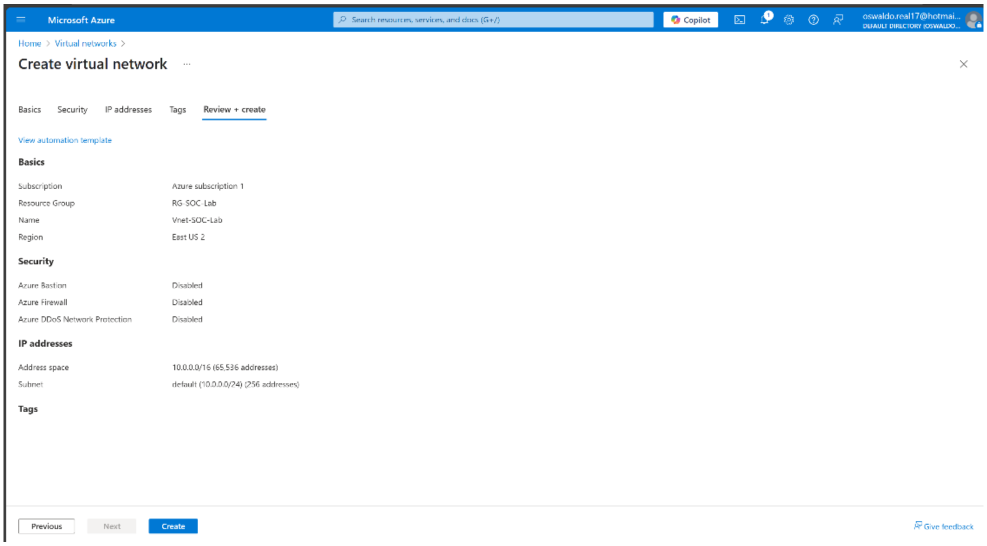
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.

Subscription *: Azure subscription 1

Resource group name *: RG-SOC-Lab

Region *: (US) East US 2

Figure2. Resource Group creation.



Create virtual network

Basics

Subscription	Azure subscription 1
Resource Group	RG-SOC-Lab
Name	Vnet-SOC-Lab
Region	East US 2

Security

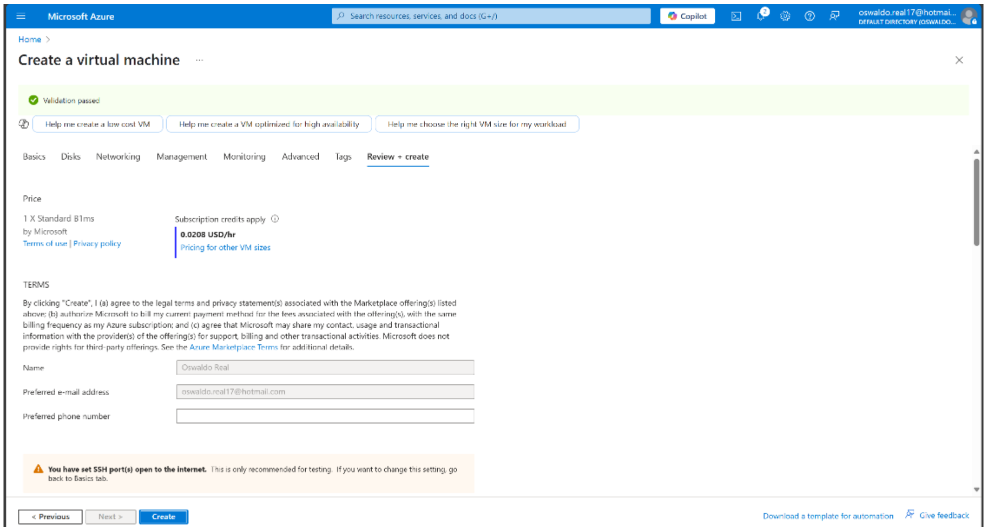
Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	default (10.0.0.0/24) (256 addresses)

Tags

Figure3. Virtual network creation.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
oswaldo.real17@hotmai...
DEFAULT DIRECTORY (OSWALDO...
Home >
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
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next >
Create
Download a template for automation
Give feedback

Create a virtual machine

Validation passed

Price

1 X Standard B1ms
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
0.0208 USD/hr
Pricing for other VM sizes

TERMS

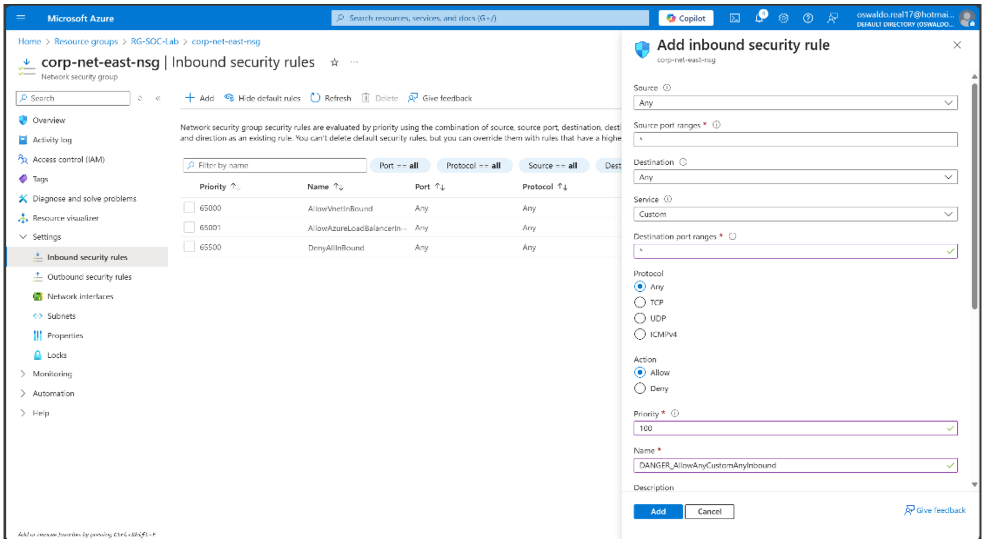
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (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.

Name	Oswaldo Real
Preferred e-mail address	oswaldo.real17@hotmail.com
Preferred phone number	

You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Figure4. Virtual machine creation.

After creating the virtual machine, configure it as a honeypot; the firewall rules or inbound security rules need to be changed so that any user from any location can access the instance over any protocol.



corp-net-east-nsg | Inbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, desti
and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a highe

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerIn...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule

corp-net-east-nsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: *

Protocol
● Any
○ TCP
○ UDP
○ ICMPv4

Action
● Allow
○ Deny

Priority *: 100

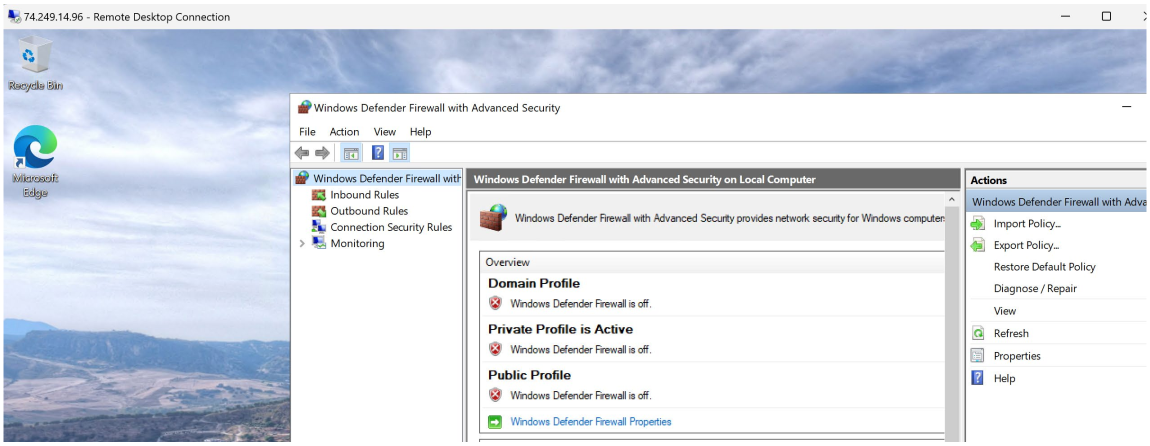
Name *: DANGER_AllowAnyCustomAnyInbound

Description

Figure5. Inbound security rules edit.

Remote Desktop Protocol is used to log on to the virtual machine that has a public IP 74.249.19.***.

To increase the likelihood of attackers on this honeypot, the firewall on the VM was shut off, and a ping was sent to prove that the new inbound security rule was applied correctly.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computer

Overview

Domain Profile

Windows Defender Firewall is off.

Private Profile is Active

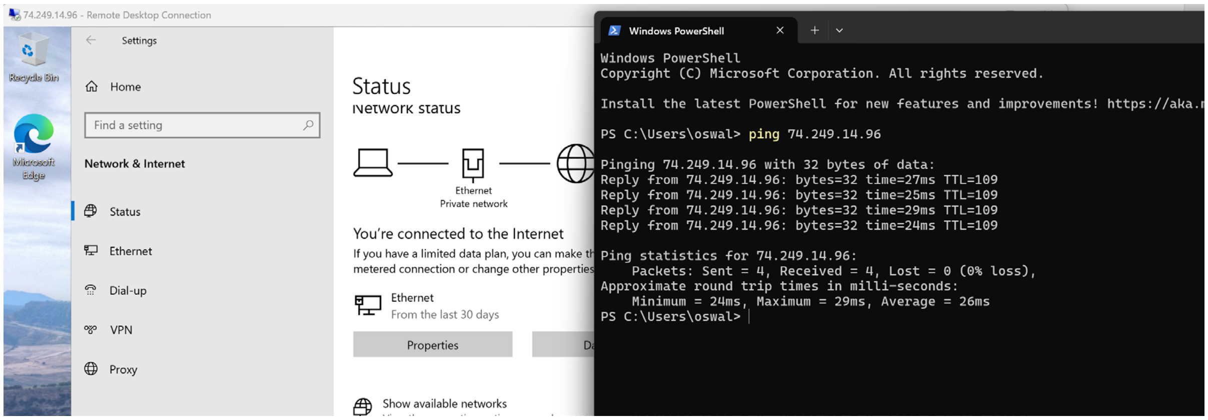
Windows Defender Firewall is off.

Public Profile

Windows Defender Firewall is off.

Windows Defender Firewall Properties

Figure6. Firewall turned off.



Status
Network status

You're connected to the Internet

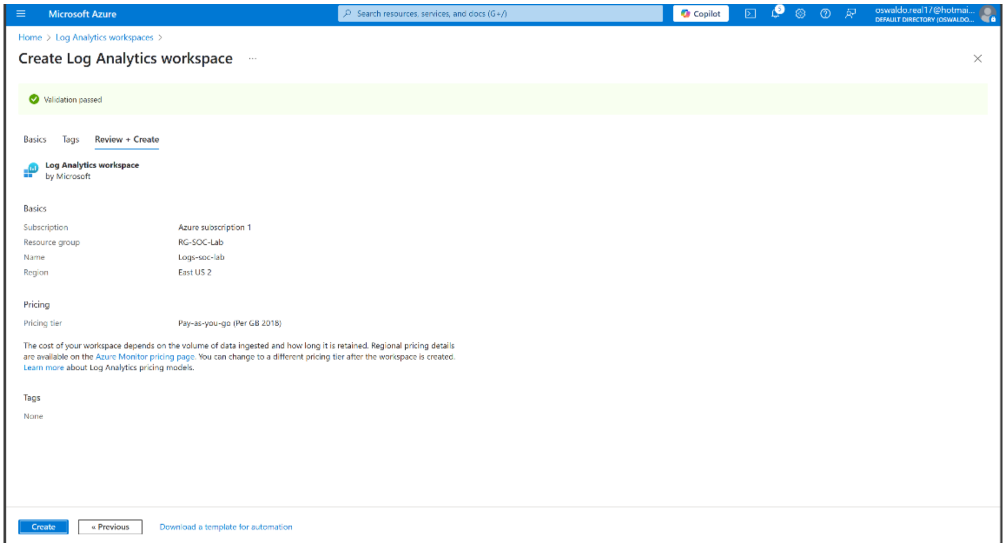
If you have a limited data plan, you can make th
metered connection or change other properties

Ethernet
From the last 30 days

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.m

PS C:\Users\oswal> ping 74.249.14.96

Pinging 74.249.14.96 with 32 bytes of data:
Reply from 74.249.14.96: bytes=32 time=27ms TTL=109
Reply from 74.249.14.96: bytes=32 time=25ms TTL=109
Reply from 74.249.14.96: bytes=32 time=29ms TTL=109
Reply from 74.249.14.96: bytes=32 time=24ms TTL=109

Ping statistics for 74.249.14.96:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 29ms, Average = 26ms
PS C:\Users\oswal>
```

Figure7. Pinging the VM.

At this point, an intentionally insecure virtual machine has been created. It is susceptible to any attack. To gather all the attack attempts that may occur, creating a Log Analytics Workspace, which will be linked to Microsoft Sentinel, is needed. The construction of those features is shown in the images below.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
oswaldo.real17@hotmai...
DEFAULT DIRECTORY (OSWALDO...
Home > Log Analytics workspaces >
Basics
Tags
Review + Create
Create
« Previous
Download a template for automation

Create Log Analytics workspace

Validation passed

Log Analytics workspace
by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	RG-SOC-Lab
Name	Logs-soc-lab
Region	East US 2

Pricing

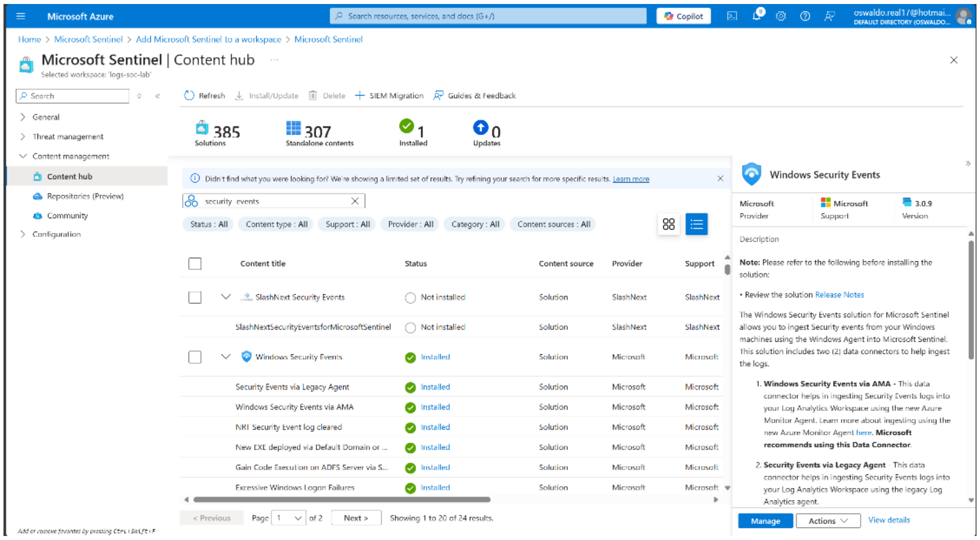
Pricing tier	Pay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the Azure Monitor pricing page. You can change to a different pricing tier after the workspace is created. Learn more about Log Analytics pricing models.

Tags

None

Figure8. Creation of Log Analysis Workspace.



Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more

security events

Status : All · Content type : All · Support : All · Provider : All · Category : All · Content sources : All

Content title	Status	Content source	Provider	Support
SlashNext Security Events	○ Not installed	Solution	SlashNext	SlashNext
SlashNextSecurityEventsforMicrosoftSentinel	○ Not installed	Solution	SlashNext	SlashNext
Windows Security Events	✓ Installed	Solution	Microsoft	Microsoft
Security Events via Legacy Agent	✓ Installed	Solution	Microsoft	Microsoft
Windows Security Events via AMA	✓ Installed	Solution	Microsoft	Microsoft
NRT Security Event log cleared	✓ Installed	Solution	Microsoft	Microsoft
New EXE deployed via Default Domain or ...	✓ Installed	Solution	Microsoft	Microsoft
Gain Code Execution on ADFS Server via S...	✓ Installed	Solution	Microsoft	Microsoft
Excessive Windows Logon Failures	✓ Installed	Solution	Microsoft	Microsoft

< Previous Page 1 of 2 Next > Showing 1 to 20 of 24 results.

Windows Security Events

Microsoft	Microsoft	3.0.9
Provider	Support	Version

Description

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

- Review the solution Release Notes

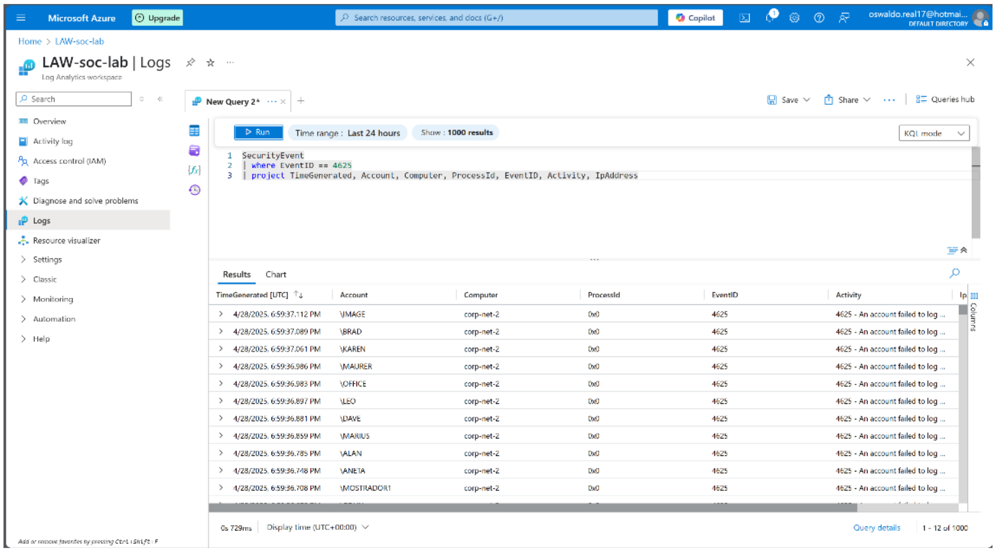
The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

1. **Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent here. **Microsoft recommends using this Data Connector**.
2. **Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

Figure9. Connection hub in Microsoft Sentinel.

The desired topology involves connecting the VM to the Log Analytics Workspace, which is done by creating a connection hub via Azure Monitoring Agent. This can be seen in the image above.

Once the topology is running, in the Log Analytics Workspace, KQL can be used to perform advanced searches on the logs.



Time range : Last 24 hours · Show : 1000 results

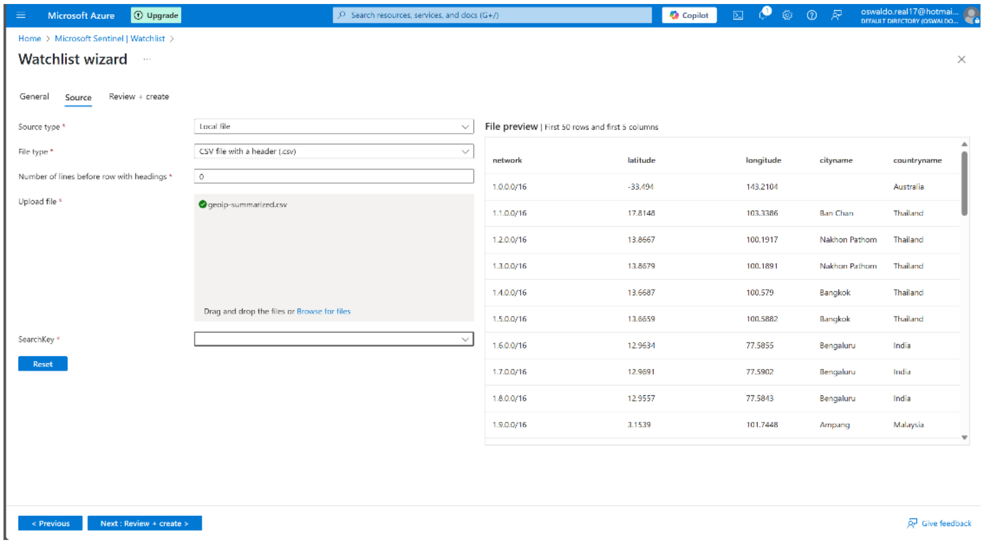
```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, Account, Computer, ProcessId, EventID, Activity, IpAddress
```

TimeGenerated [UTC]	Account	Computer	ProcessId	EventID	Activity
4/28/2025, 6:59:37.112 PM	\IMAGE	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:37.089 PM	\BRAD	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:37.061 PM	\KAREN	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.986 PM	\MAURER	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.983 PM	\OFFICE	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.897 PM	\LEO	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.881 PM	\DAVE	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.859 PM	\MARIUS	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.785 PM	\ALAN	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.748 PM	\ANETA	corp-net-2	0x0	4625	4625 - An account failed to log ...
4/28/2025, 6:59:36.708 PM	\MOSTRADOR1	corp-net-2	0x0	4625	4625 - An account failed to log ...

0s 729ms · Display time (UTC+00:00) · Query details · 1 - 12 of 1000

Figure10. Query to see the security events with the ID 4625

Since the logs gathered by the VM do not have any geographical information, an external file with all the needed geographical information was uploaded onto the Sentinel Watchlist.



Watchlist wizard

Source type * Local file

File type * CSV file with a header (.csv)

Number of lines before row with headings * 0

Upload file * geoip-summarized.csv

Drag and drop the files or Browse for files

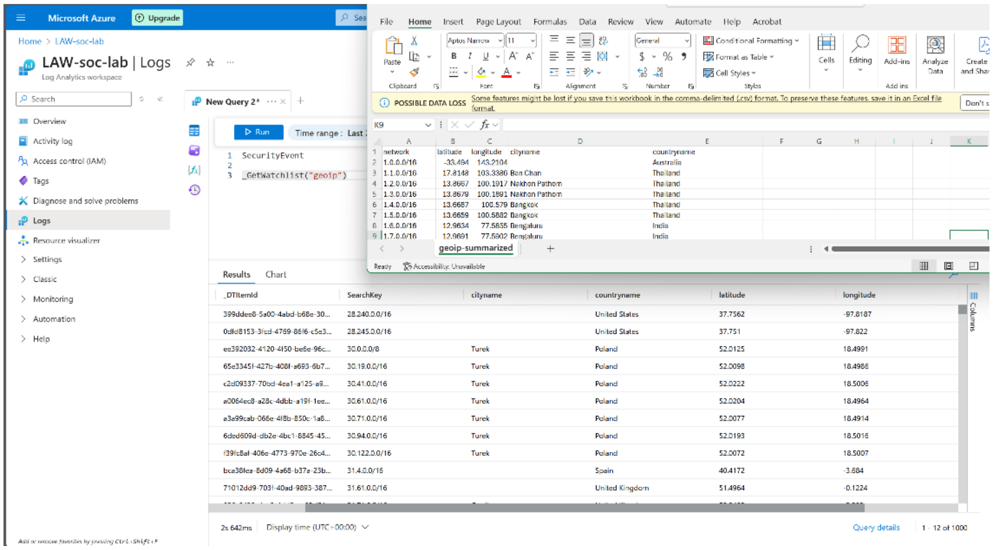
SearchKey *

File preview | First 50 rows and first 5 columns

network	latitude	longitude	cityname	countryname
1.0.0.0/16	-33.494	143.2104		Australia
1.1.0.0/16	17.8148	103.3386	Ban Chan	Thailand
1.2.0.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
1.3.0.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
1.4.0.0/16	13.6687	100.579	Bangkok	Thailand
1.5.0.0/16	13.6659	100.5882	Bangkok	Thailand
1.6.0.0/16	12.9634	77.5855	Bengaluru	India
1.7.0.0/16	12.9691	77.5902	Bengaluru	India
1.8.0.0/16	12.9557	77.5843	Bengaluru	India
1.9.0.0/16	3.1539	101.7448	Ampang	Malaysia

Figure11. Geographical information uploaded.

All the information in that file could now be used in the Log Analytics Section query to have a better understanding of the attempts that have already occurred.



```
SecurityEvent

_GetWatchlist("geoip")
```

POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.

	A	B	C	D	E
1	network	latitude	longitude	cityname	countryname
2	1.0.0.0/16	-33.494	143.2104		Australia
3	1.1.0.0/16	17.8148	103.3386	Ban Chan	Thailand
4	1.2.0.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
5	1.3.0.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
6	1.4.0.0/16	13.6687	100.579	Bangkok	Thailand
7	1.5.0.0/16	13.6659	100.5882	Bangkok	Thailand
8	1.6.0.0/16	12.9634	77.5855	Bengaluru	India
9	1.7.0.0/16	12.9691	77.5902	Bengaluru	India

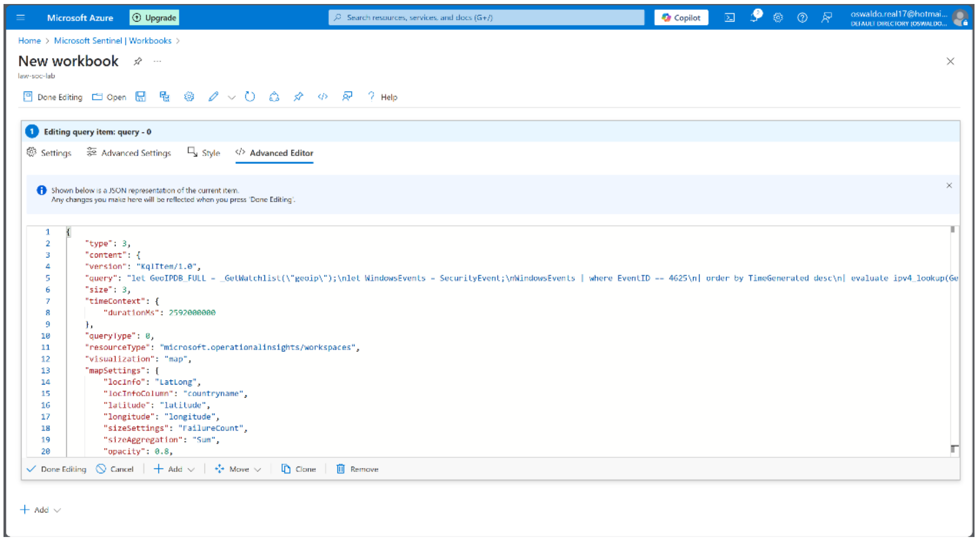
_DTItemId	SearchKey	cityname	countryname	latitude	longitude
399ddee8-5a00-4abd-b68e-30...	28.240.0.0/16		United States	37.7562	-97.8187
0dfd8153-3fcd-4769-86f6-c5e3...	28.245.0.0/16		United States	37.751	-97.822
ee392032-4120-4f50-be6e-96c...	30.0.0.0/8	Turek	Poland	52.0125	18.4991
65e3345f-427b-408f-a693-6b7...	30.19.0.0/16	Turek	Poland	52.0098	18.4986
c2d09337-70bd-4ea1-a125-a9...	30.41.0.0/16	Turek	Poland	52.0222	18.5006
a0064ec8-a28c-4dbb-a19f-1ee...	30.61.0.0/16	Turek	Poland	52.0204	18.4964
a3a99cab-066e-4f8b-850c-1a8...	30.71.0.0/16	Turek	Poland	52.0077	18.4914
6ded609d-db2e-4bc1-8845-45...	30.94.0.0/16	Turek	Poland	52.0193	18.5016
f39fc8af-406e-4773-970e-26c4...	30.122.0.0/16	Turek	Poland	52.0072	18.5007
bca38fea-8d09-4a68-b37a-23b...	31.4.0.0/16		Spain	40.4172	-3.684
71012dd9-703f-40ad-9893-387...	31.61.0.0/16		United Kingdom	51.4964	-0.1224

2s 642ms Display time (UTC+00:00)

1 - 12 of 1000

Figure12. KQL using geographical information.

Lastly, to visualize all this information on a world map, a new workbook within Sentinel needs to be created. This workbook will contain the code provided in Appendix A.

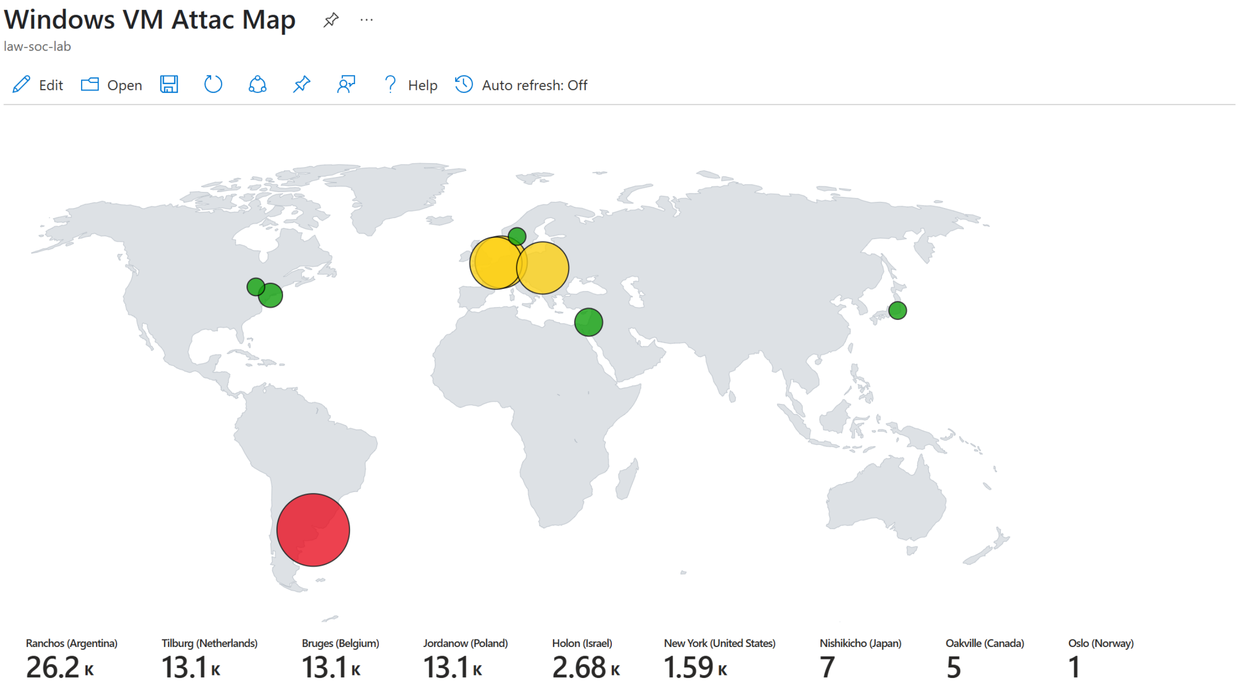


Shown below is a JSON representation of the current item.
Any changes you make here will be reflected when you press 'Done Editing'.

```
{
    "type": 3,
    "content": {
    "version": "KqlItem/1.0",
    "query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n| order by TimeGenerated desc\n| evaluate ipv4_lookup(Ge
    "size": 3,
    "timeContext": {
        "durationMs": 2592000000
    },
    "queryType": 0,
    "resourceType": "microsoft.operationalinsights/workspaces",
    "visualization": "map",
    "mapSettings": {
        "locInfo": "LatLong",
        "locInfoColumn": "countryname",
        "latitude": "latitude",
        "longitude": "longitude",
        "sizeSettings": "FailureCount",
        "sizeAggregation": "Sum",
        "opacity": 0.8,
```

Figure13. Edit a workbook within Sentinel.

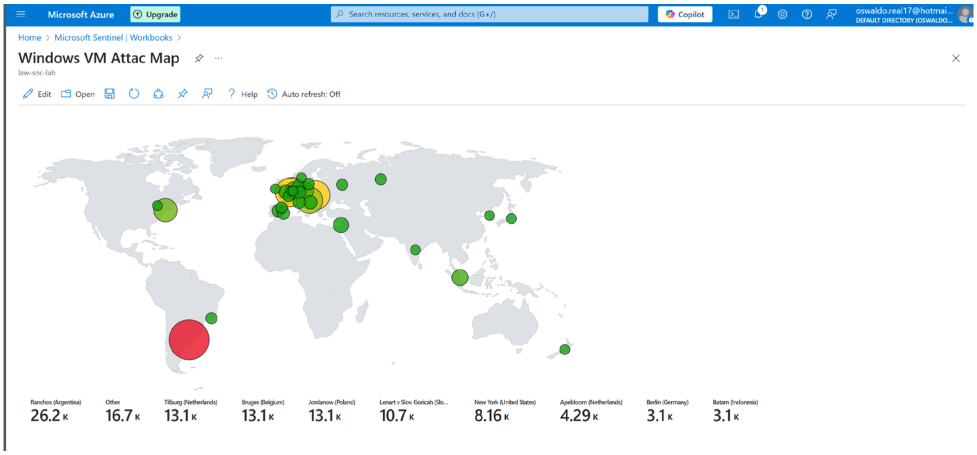
Once saved, the workbook displays a world map highlighting attack sources.



Ranchos (Argentina)	Tilburg (Netherlands)	Bruges (Belgium)	Jordanow (Poland)	Holon (Israel)	New York (United States)	Nishikicho (Japan)	Oakville (Canada)	Oslo (Norway)
26.2 K	13.1 K	13.1 K	13.1 K	2.68 K	1.59 K	7	5	1

Figure14. Attack Visualization in Microsoft Sentinel.

After 24 hours the map highlighting attack sources look like the image below.



Ranchos (Argentina)	Other	Tilburg (Netherlands)	Bruges (Belgium)	Jordanow (Poland)	Lenart v Slov. Goricah (Slo...	New York (United States)	Apeldoorn (Netherlands)	Berlin (Germany)	Batam (Indonesia)
26.2 K	16.7 K	13.1 K	13.1 K	13.1 K	10.7 K	8.16 K	4.29 K	3.1 K	3.1 K

Figure15. Attack Visualization in Microsoft Sentinel.

Results

By setting up an intentionally vulnerable virtual machine (honeypot) in Azure, I successfully attracted and collected malicious login attempts from external attackers. The logs were gathered using a Log Analytics Workspace linked to Microsoft Sentinel and enriched with geographic data through a custom Watchlist. Using KQL queries, I was able to analyze security events, correlate them with attacker locations, and visualize the origin of attack attempts on a global map within a Sentinel workbook. This project demonstrated the ability to configure cloud-based honeypots, perform log analysis, enhance security data with external intelligence, and build interactive threat visualizations.

Appendix A:

```
{
        "type": 3,
        "content": {
        "version": "KqlItem/1.0",
        "query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n| order by TimeGenerated desc\n| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)\n| summarize FailureCount = count() by IpAddress, latitude, longitude, cityname, countryname\n| project FailureCount, AttackerIp = IpAddress, latitude, longitude, city = cityname, country = countryname,\nfriendly_location = strcat(cityname, \" (\", countryname, \")\");",
        "size": 3,
        "timeContext": {
                "durationMs": 2592000000
        },
        "queryType": 0,
        "resourceType": "microsoft.operationalinsights/workspaces",
        "visualization": "map",
        "mapSettings": {
                "locInfo": "LatLong",
                "locInfoColumn": "countryname",
                "latitude": "latitude",
                "longitude": "longitude",
                "sizeSettings": "FailureCount",
                "sizeAggregation": "Sum",
                "opacity": 0.8,
                "labelSettings": "friendly_location",
                "legendMetric": "FailureCount",
                "legendAggregation": "Sum",
                "itemColorSettings": {
                "nodeColorField": "FailureCount",
                "colorAggregation": "Sum",
                "type": "heatmap",
                "heatmapPalette": "greenRed"
                }
        }
        },
        "name": "query - 0"
}
```

Code to create the graphical view of a world map with the adversaries from all over the world in it.