🔐 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:

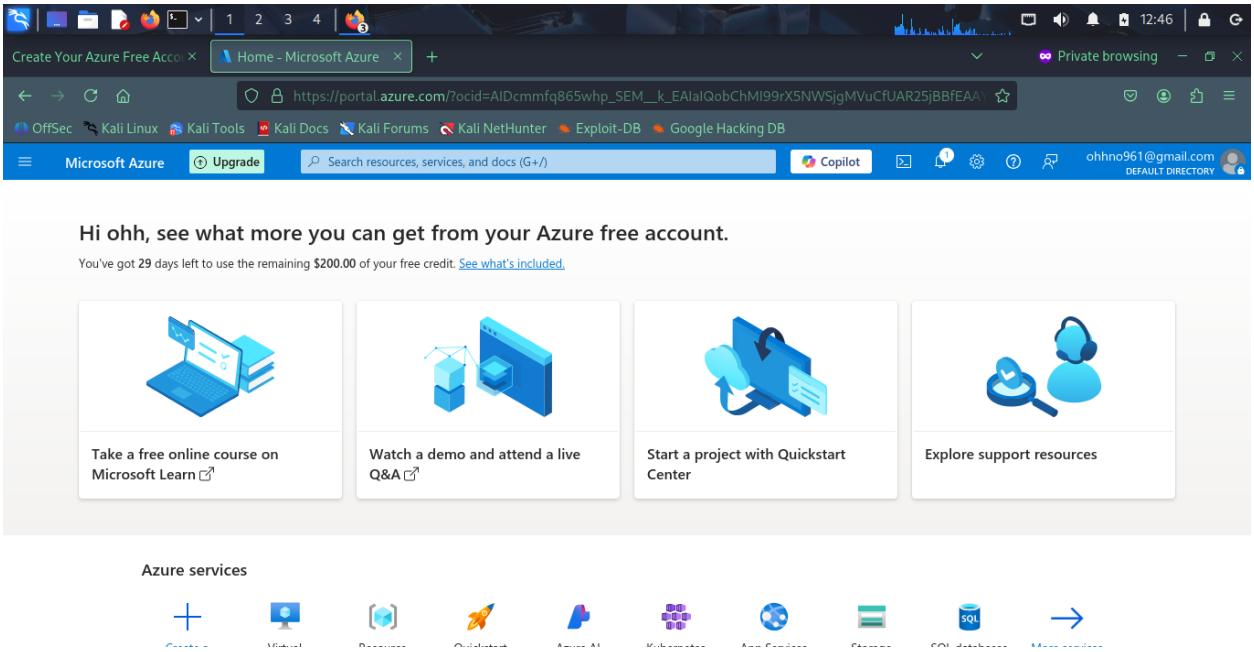
- Attacks sourced from **2 countries** (Top: 🇵🇱 Poland and 🇧🇷 Brazil)
- Accounts targeted: `Administrator`, `admin`, `svcuser`
- Botnet-like behavior via **rapid IP rotation**

✅ 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 🌐

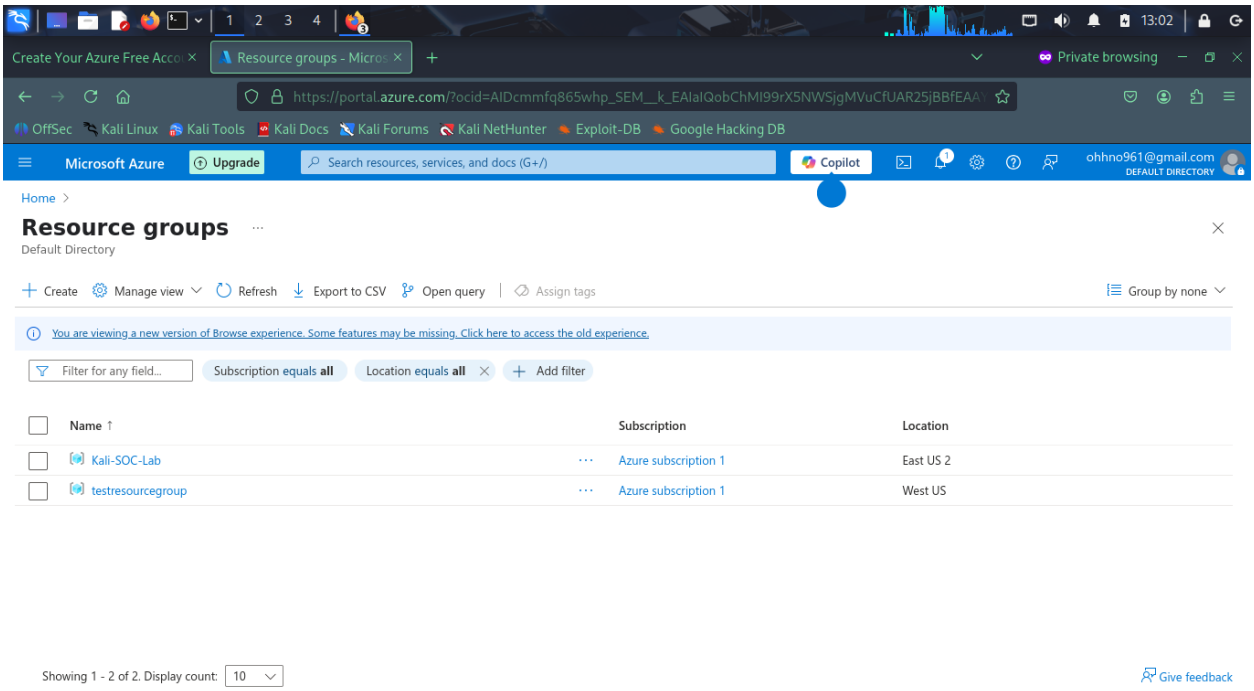
- Navigate to **Azure Free Trial**
- Sign up with **personal email** (non-work/school)
- Verify identity with **credit card**
- Access portal: https://portal.azure.com

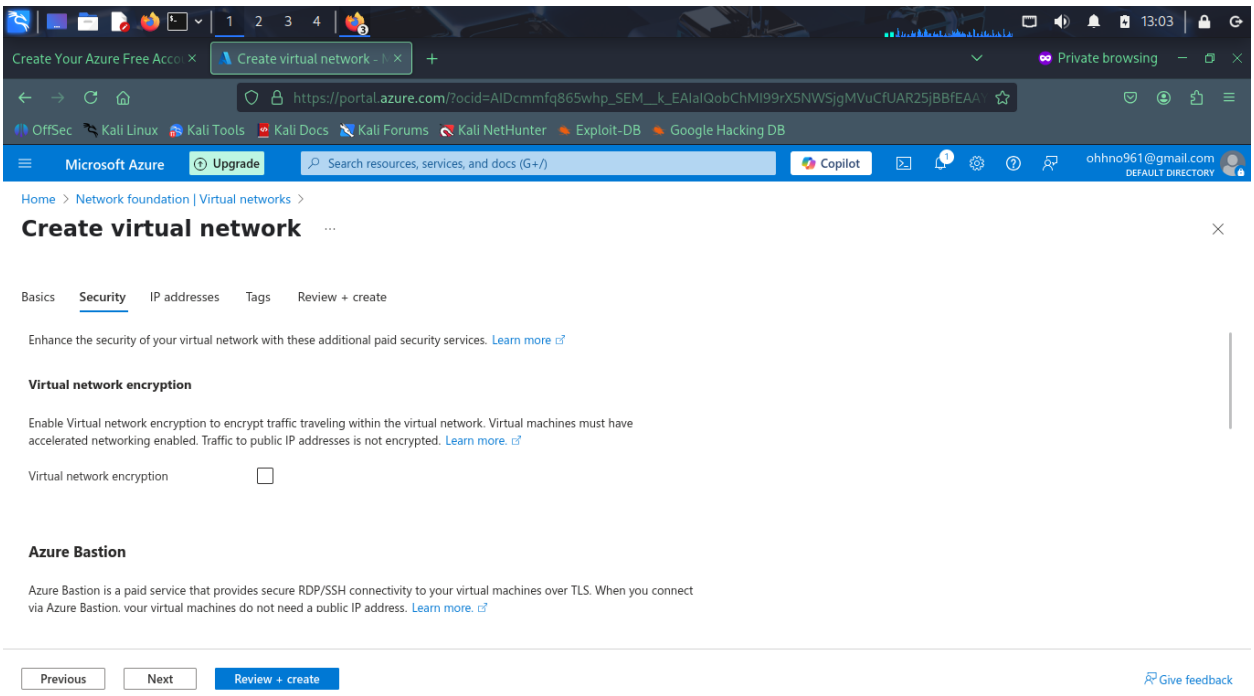


2.Resource Group Creation 📦

- 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

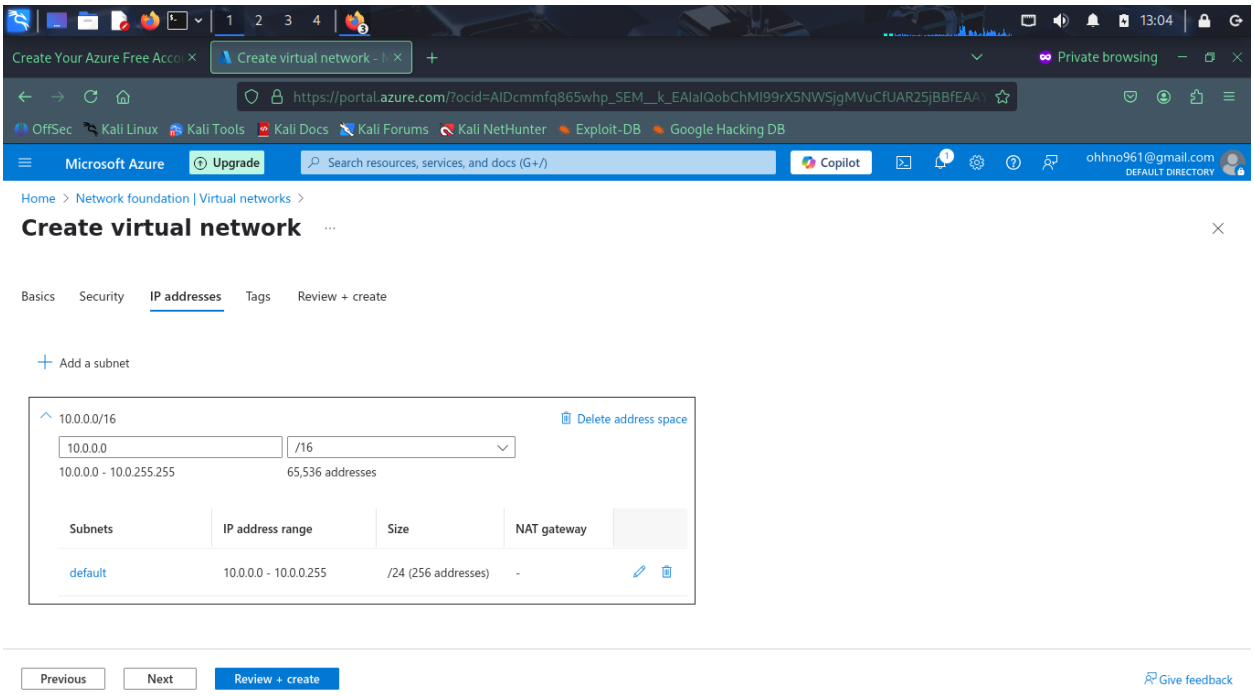




3.Virtual Network Setup 🌐

- 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**



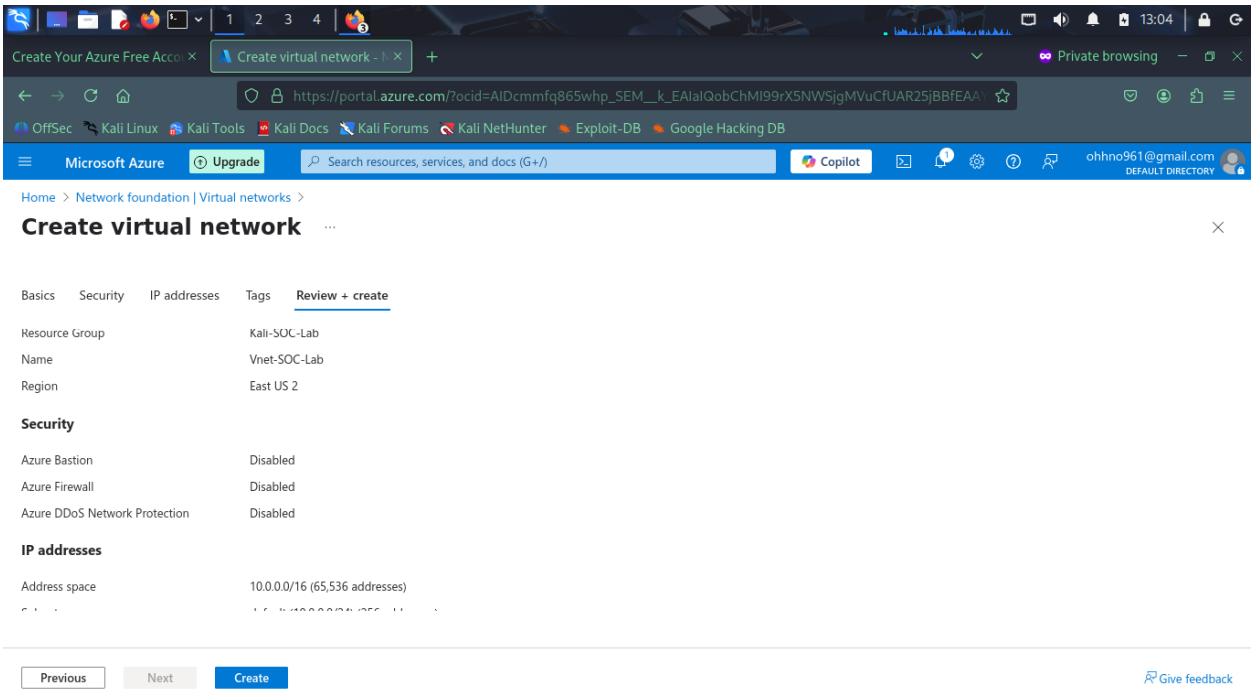
4.Honeypot VM Deployment 🖥️🎯

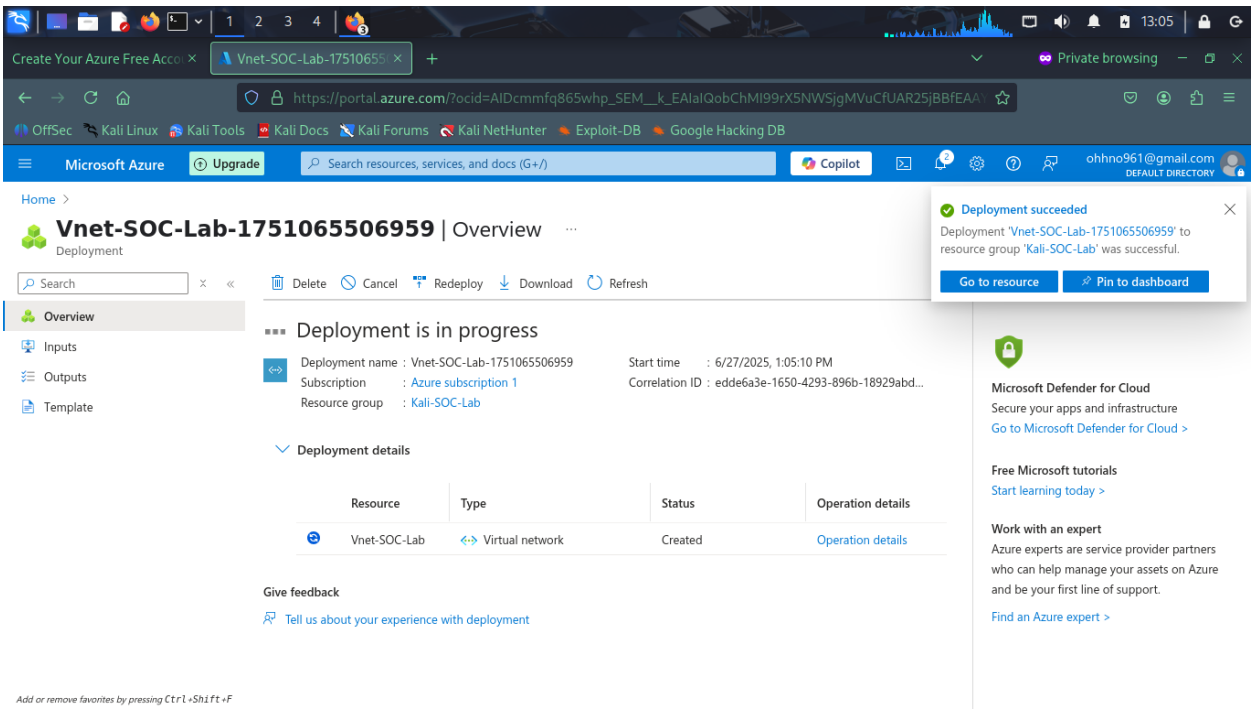
- Portal search: `Virtual machines`
- Click **Create → Azure virtual machine**
- Configure:
    - **Resource group:** `kali-soc-lab`
    - **VM name:** `CORP-NET-East2`
    - **Region:** East US 2
    - **Image:** Windows 10 Pro
    - **Size:** `Standard_D2s_v3`
    - **Username:** `labuser`
    - **Password:**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

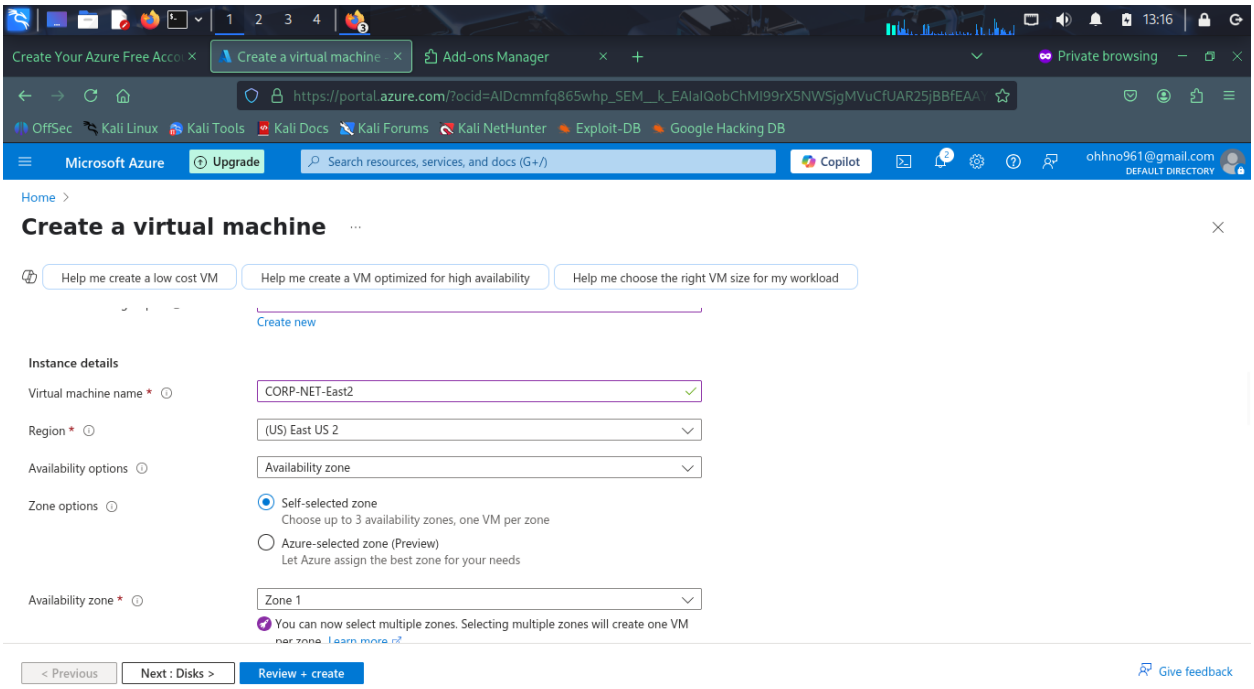
🔌 Networking tab:

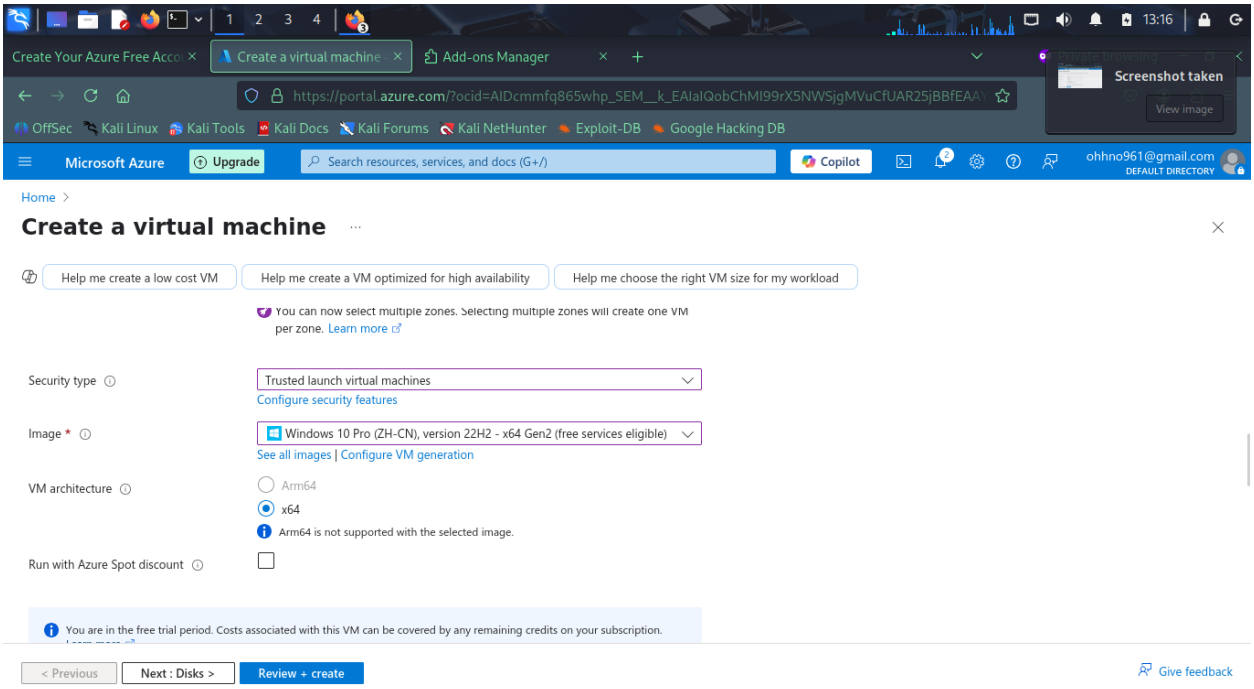
- **Virtual network:** `vnet-soc-lab`
- **Subnet:** `default`

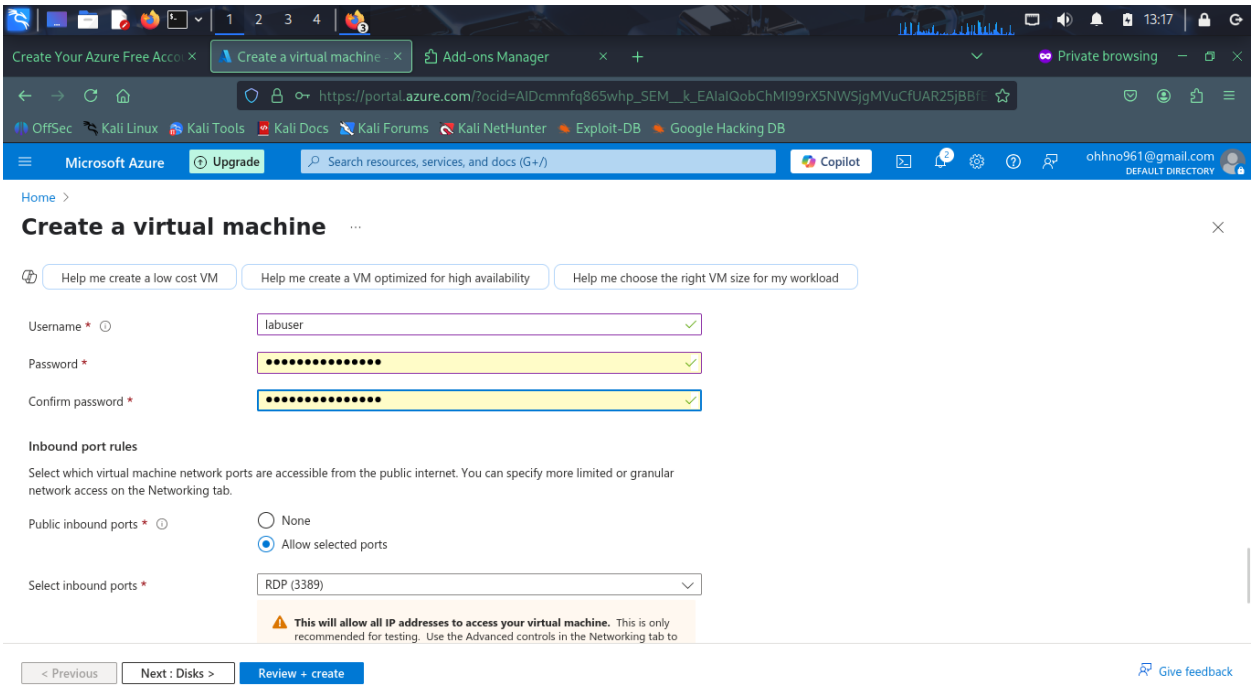
→ Review + Create → Create

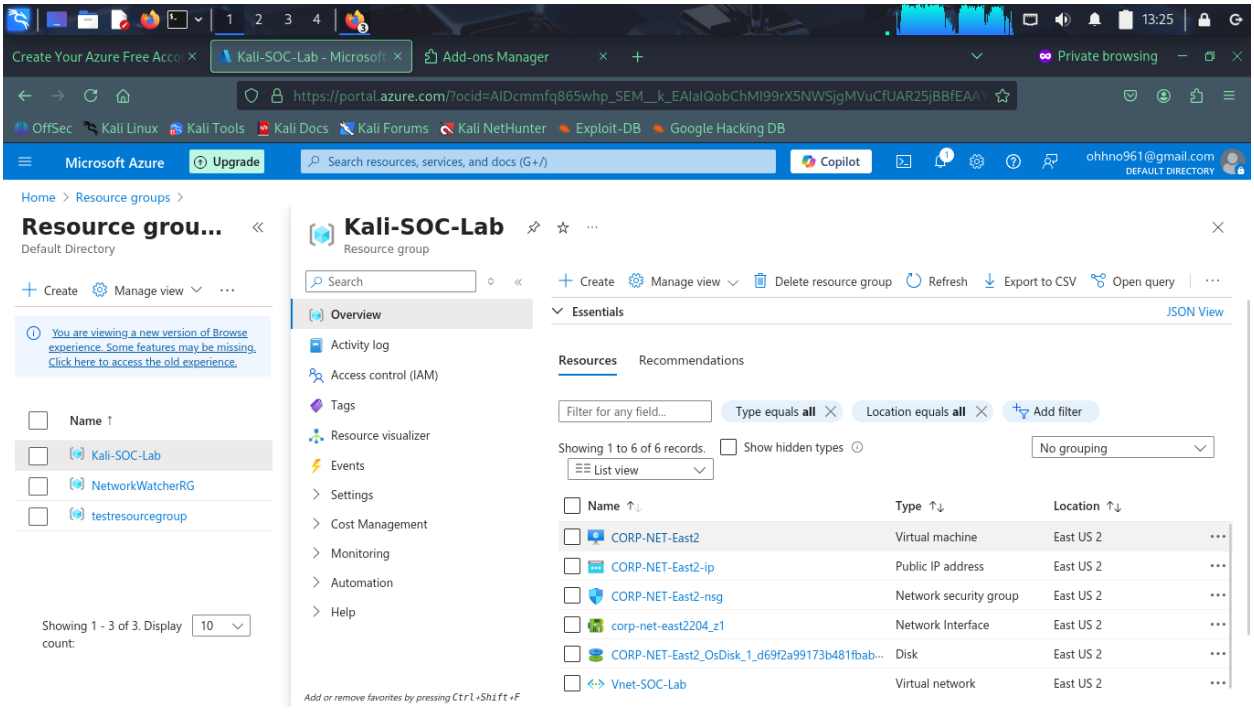

Create virtual network
Basics
Security
IP addresses
Tags
Review + create
Resource Group
Kali-SOC-Lab
Name
Vnet-SOC-Lab
Region
East US 2
Security
Azure Bastion
Disabled
Azure Firewall
Disabled
Azure DDoS Network Protection
Disabled
IP addresses
Address space
10.0.0.0/16 (65,536 addresses)
Previous
Next
Create
Give feedback

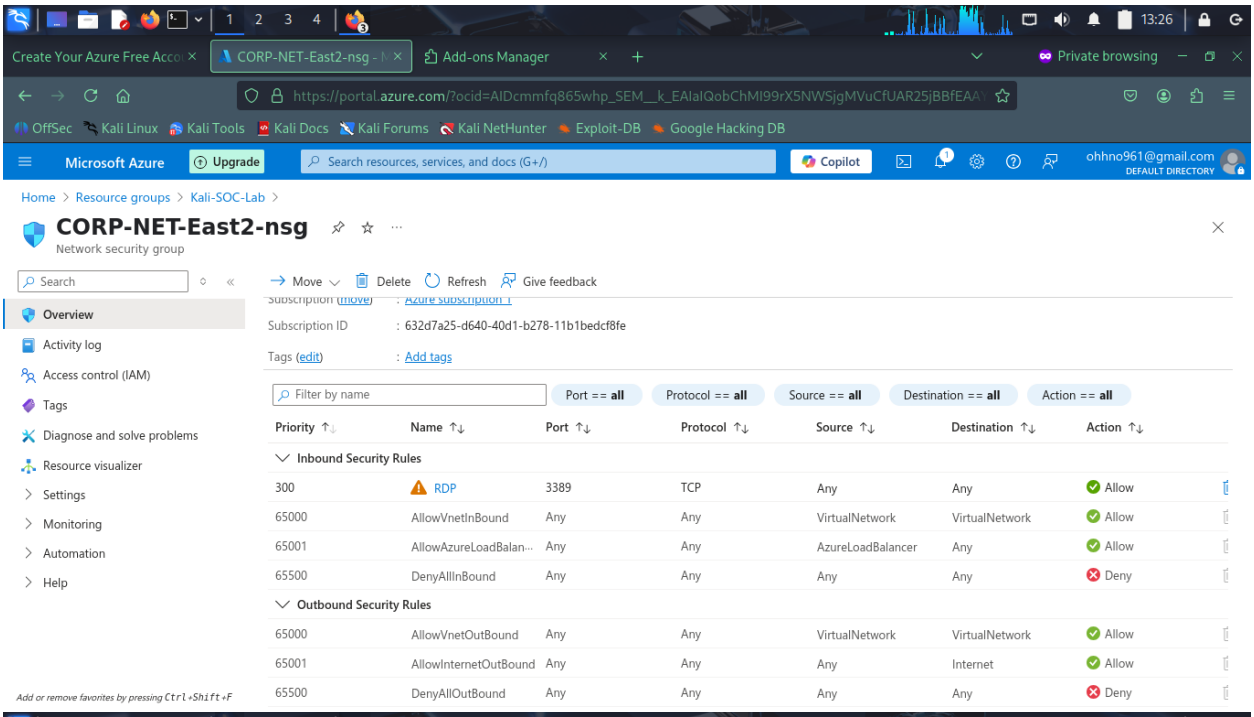

Vnet-SOC-Lab-1751065506959 | Overview
Deployment
Deployment succeeded
Deployment 'Vnet-SOC-Lab-1751065506959' to resource group 'Kali-SOC-Lab' was successful.
Go to resource
Pin to dashboard
Delete
Cancel
Redeploy
Download
Refresh
Deployment is in progress
Deployment name : Vnet-SOC-Lab-1751065506959
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
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Add or remove favorites by pressing Ctrl+Shift+F

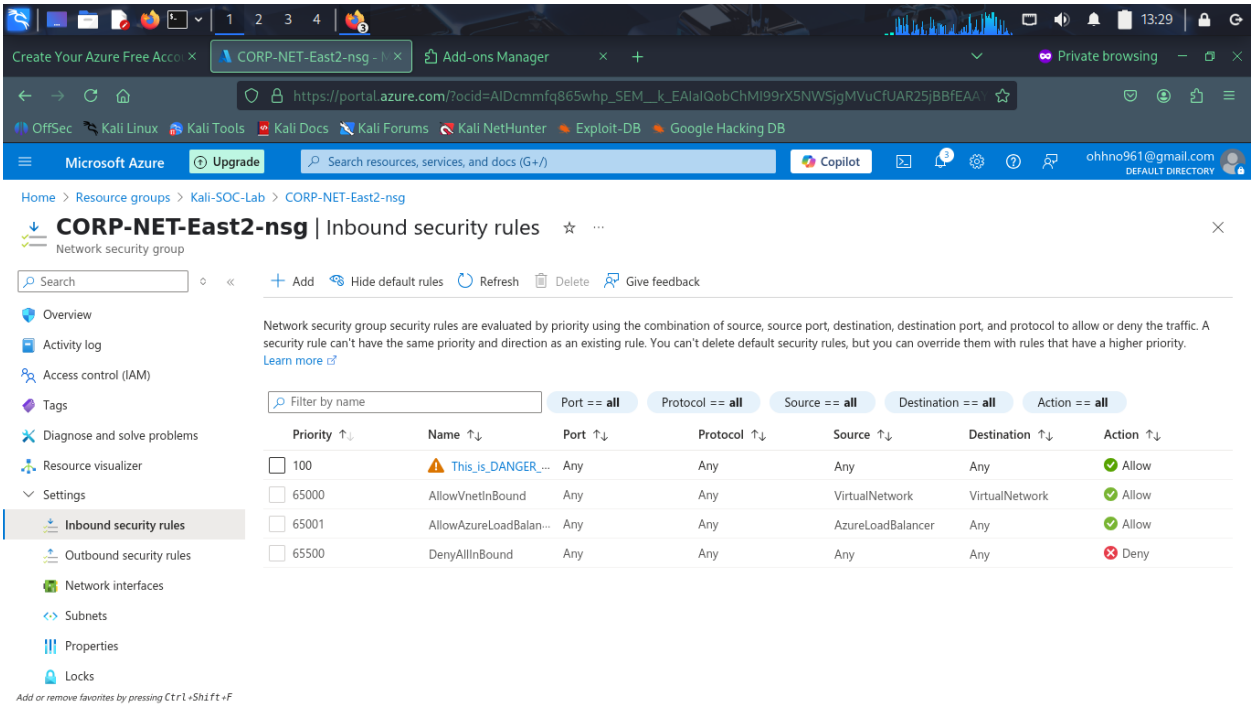

Create Your Azure Free Acco
Create a virtual machine
Add-ons Manager
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home
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
Create new
Instance details
Virtual machine name *
CORP-NET-East2
Region *
(US) East US 2
Availability options
Availability zone
Zone options
Self-selected zone
Choose up to 3 availability zones, one VM per zone
Azure-selected zone (Preview)
Let Azure assign the best zone for your needs
Availability zone *
Zone 1
You can now select multiple zones. Selecting multiple zones will create one VM
per zone. Learn more
< Previous
Next : Disks >
Review + create
Give feedback


Create Your Azure Free Acco
Create a virtual machine
Add-ons Manager
Screenshot taken
View image
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home
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
You can now select multiple zones. Selecting multiple zones will create one VM
per zone. Learn more
Security type
Trusted launch virtual machines
Configure security features
Image *
Windows 10 Pro (ZH-CN), version 22H2 - x64 Gen2 (free services eligible)
See all images | Configure VM generation
VM architecture
Arm64
x64
Arm64 is not supported with the selected image.
Run with Azure Spot discount
You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription.
< Previous
Next : Disks >
Review + create
Give feedback


Create Your Azure Free Acco
Create a virtual machine
Add-ons Manager
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBf
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home
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 to
< Previous
Next : Disks >
Review + create
Give feedback


Create Your Azure Free Acco
Kali-SOC-Lab - Microsoft
Add-ons Manager
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Resource groups
Resource grou...
Default Directory
Create
Manage view
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 count:
10
Kali-SOC-Lab
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Essentials
JSON View
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 6 of 6 records.
Show hidden types
No grouping
List view
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





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`

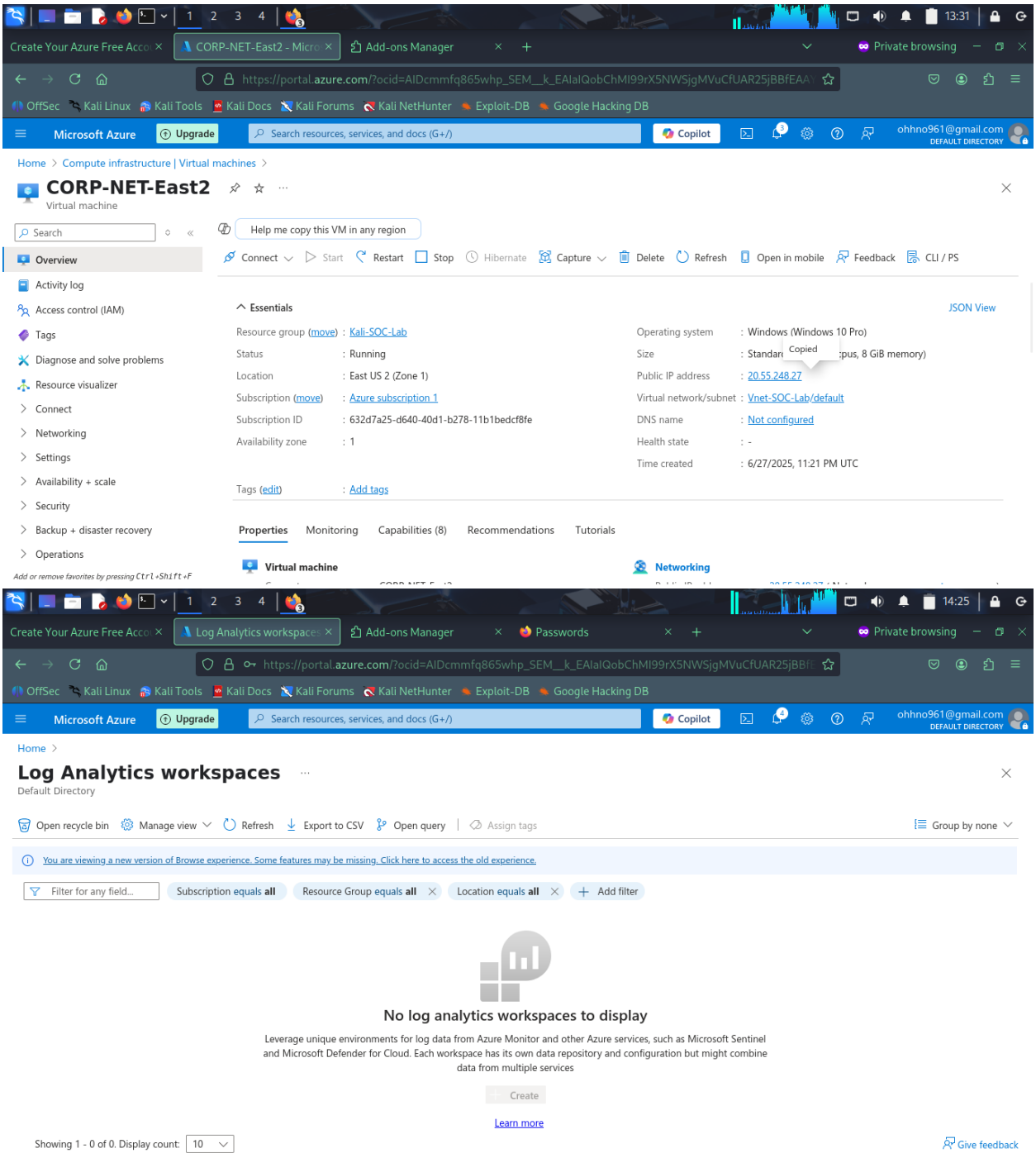
→ Click **Add → Save**

🖥️ RDP into VM:

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

⚙️ Inside VM:

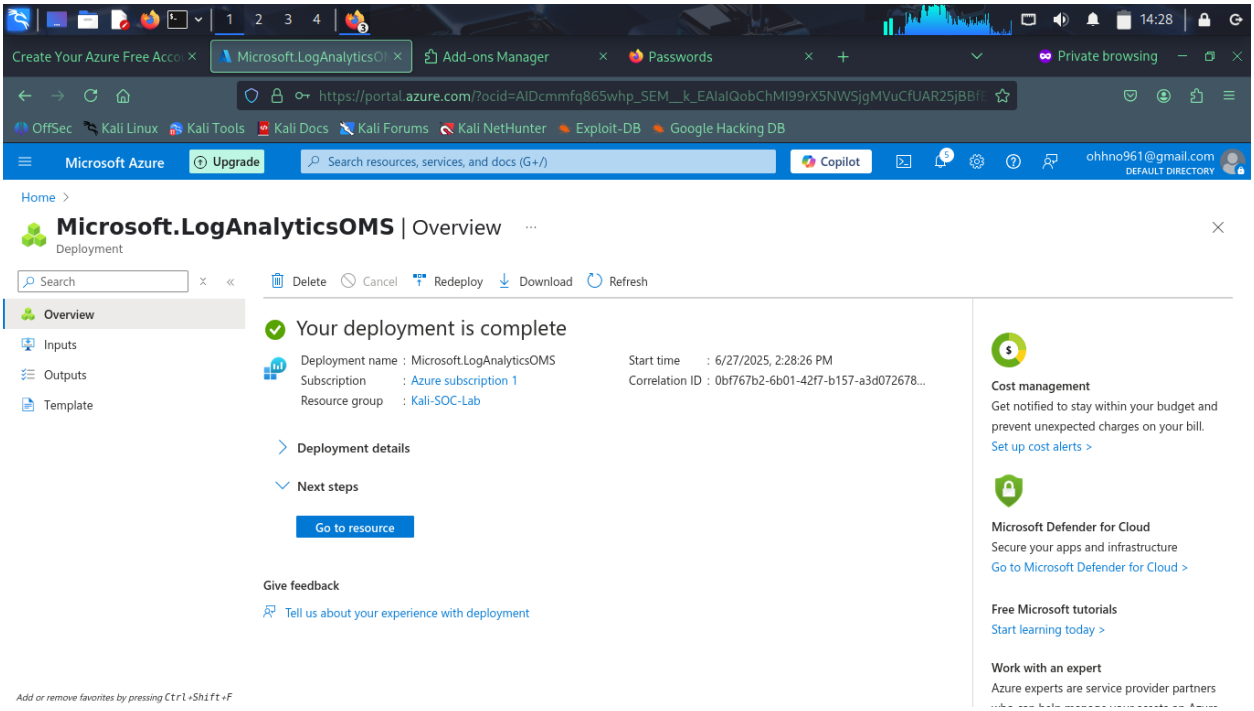
- Open Windows Search → `wf.msc`
- Turn off firewall for all profiles (Domain / Private / Public)



6.Log Analytics Workspace

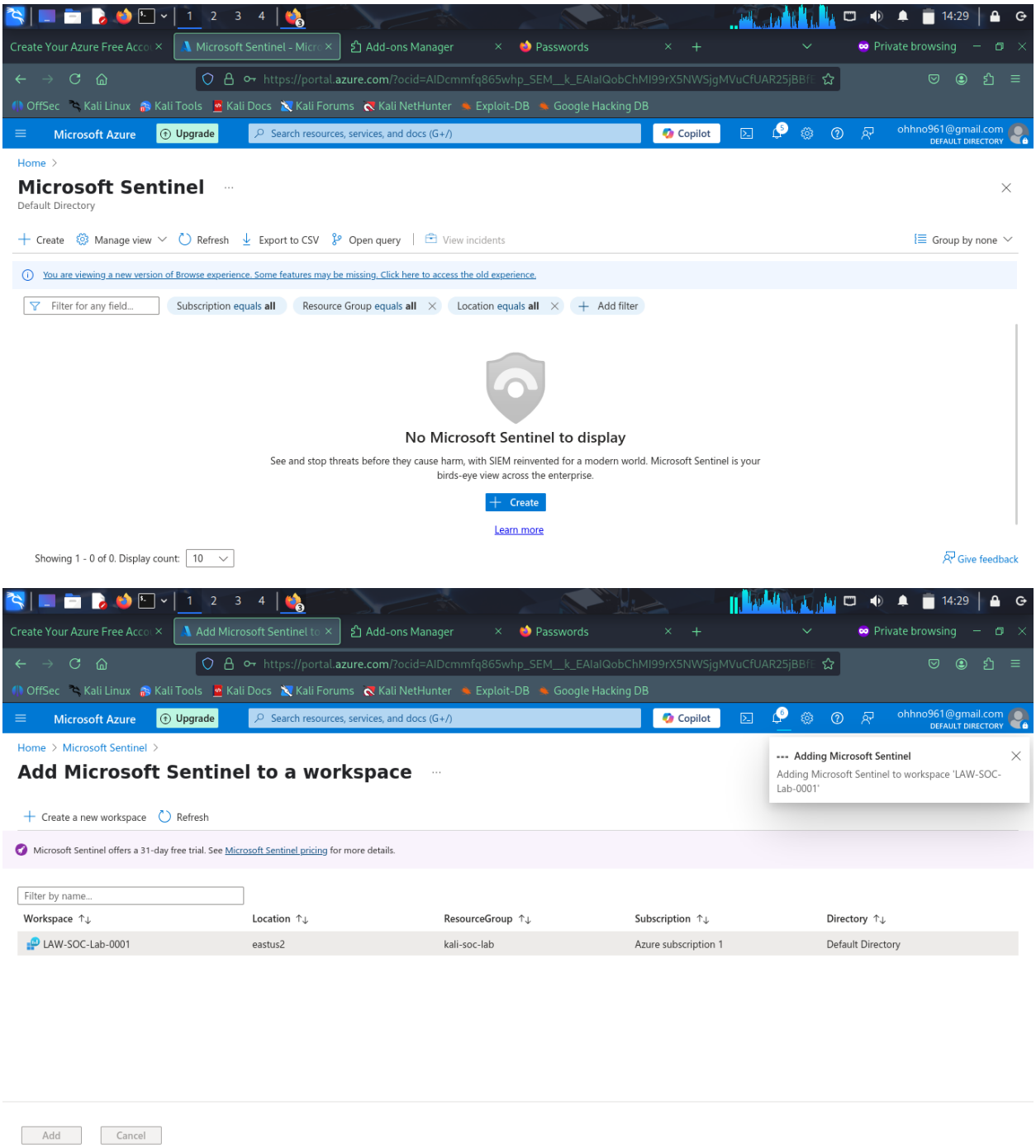
- Portal search: `Log Analytics workspaces`
- Click **Create**
- Configure:
    - **Resource group:** `kali-soc-lab`

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



7.Microsoft Sentinel Deployment 🔎

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

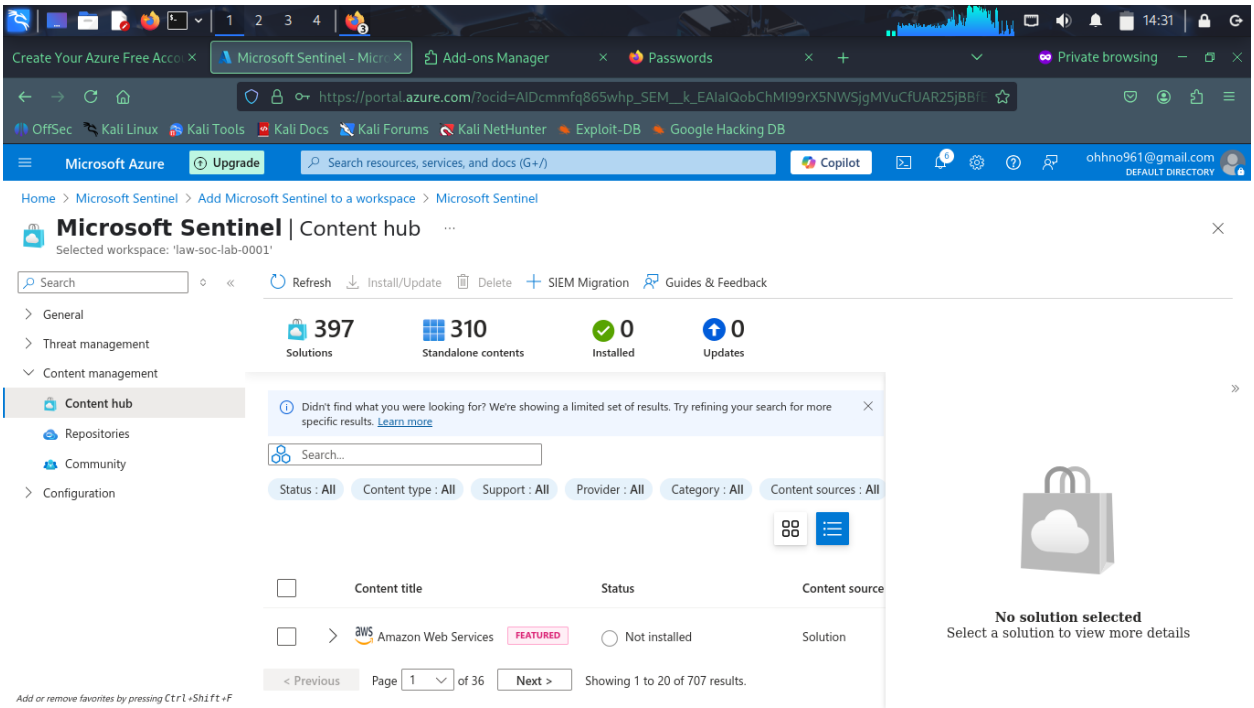


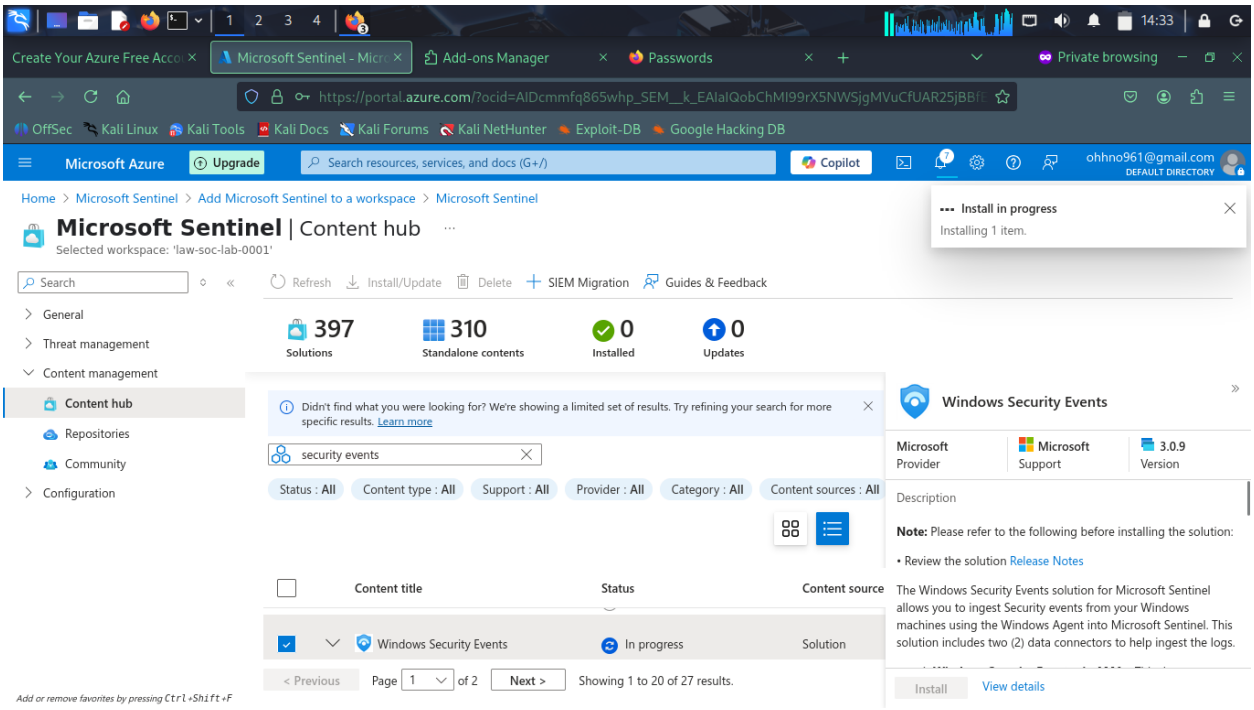
8.Log Collection Configuration 🧲

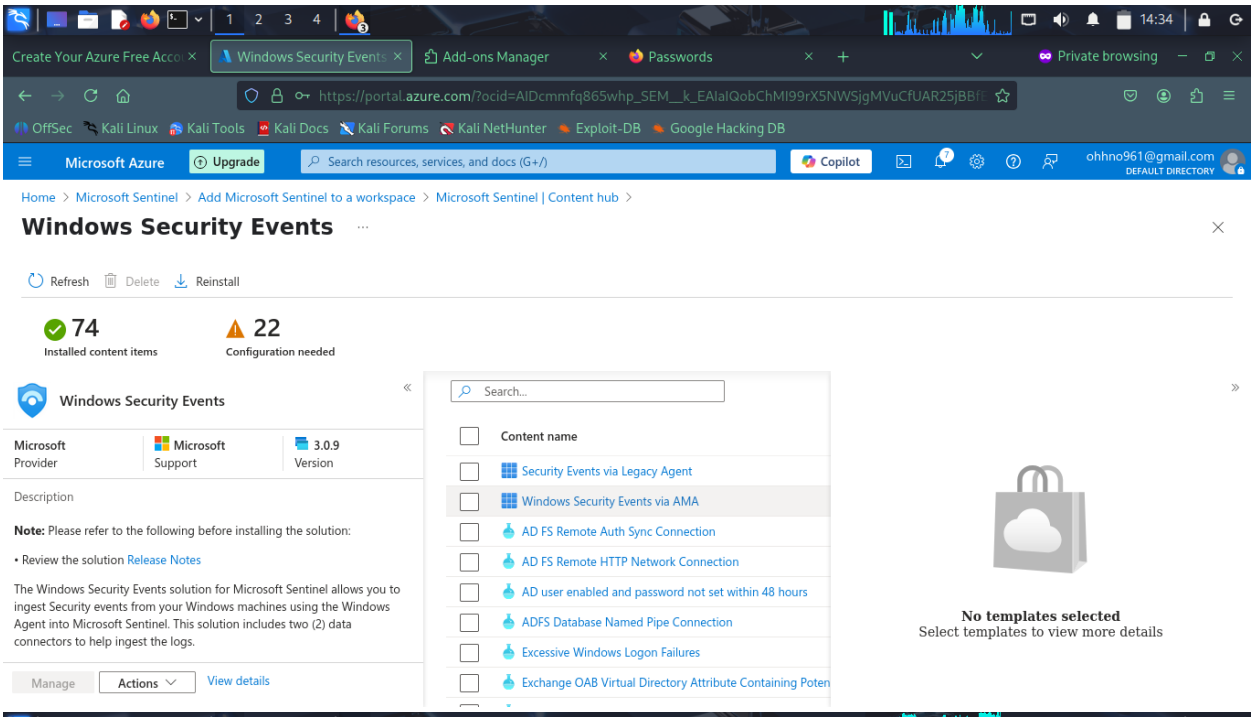
- In Sentinel → `Content hub` → Search: **Windows Security Events**
- Click **Install**
- Post-install → **Manage** → Open connector page

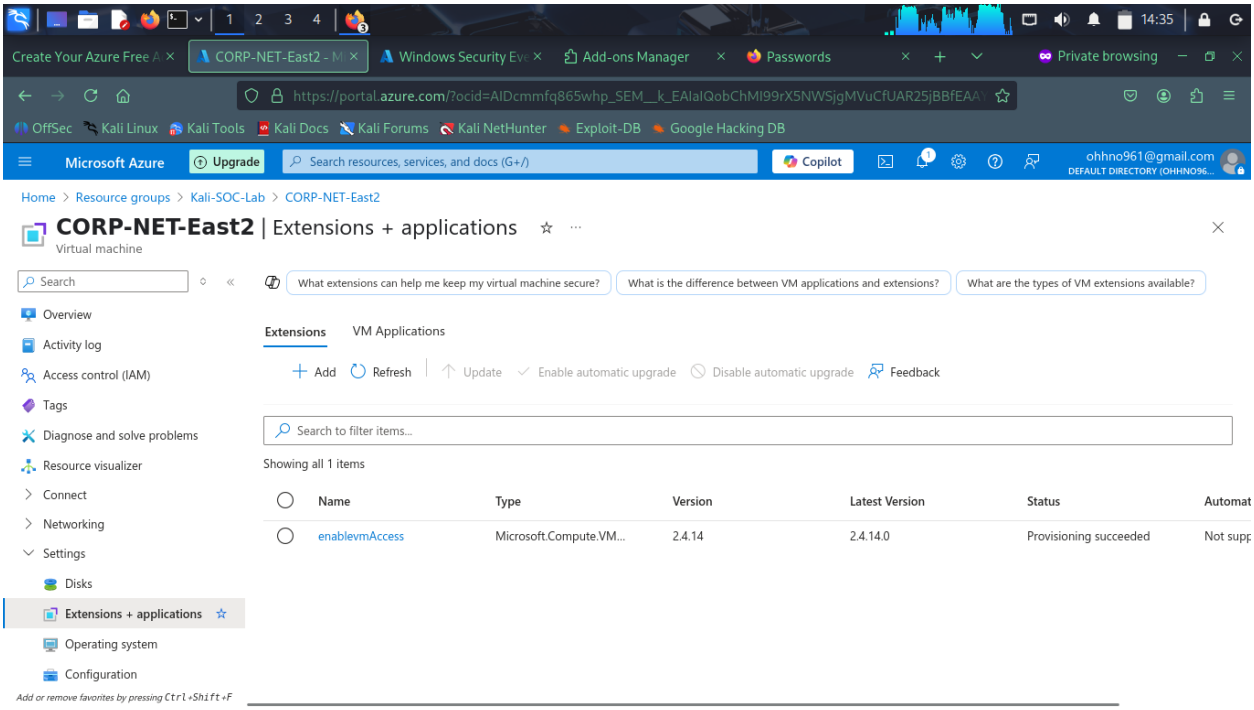
🛠️ Create data collection rule:

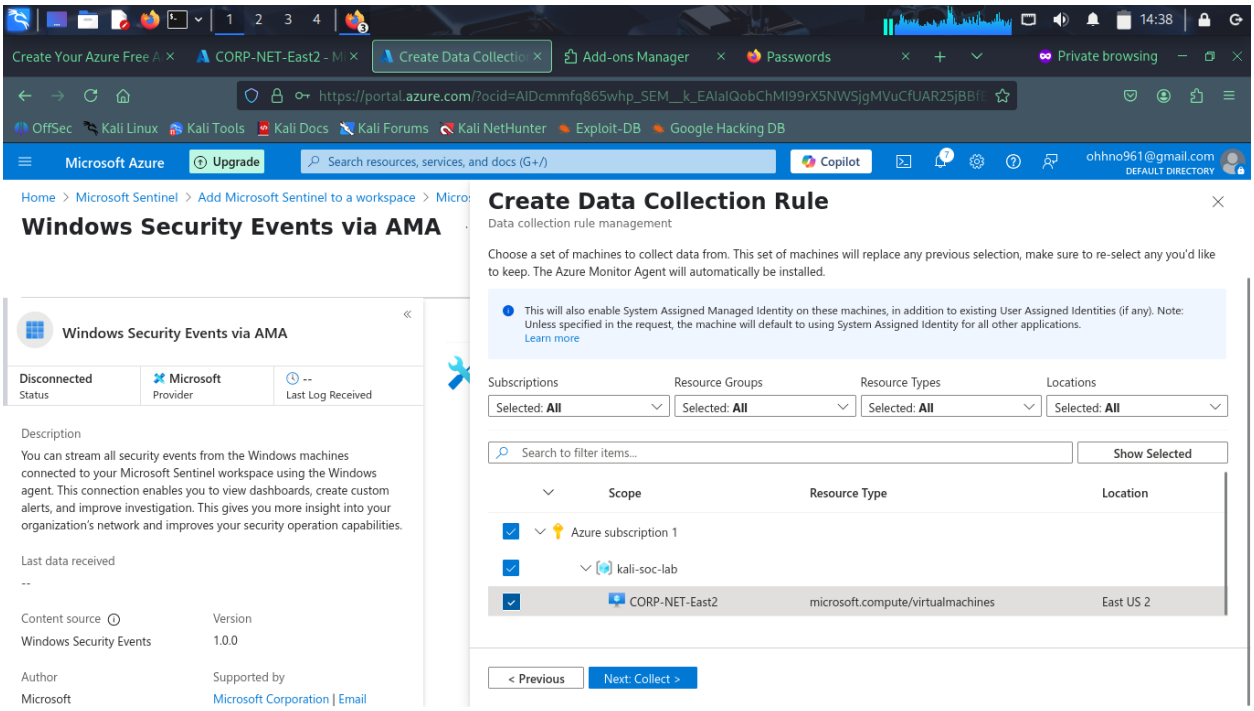
- **Name:** `dcr-windows-secevents`
- **Resources:** Select `corp-net-east2` VM
- **Collect:** All Security Events
  → **Review + Create → Create**

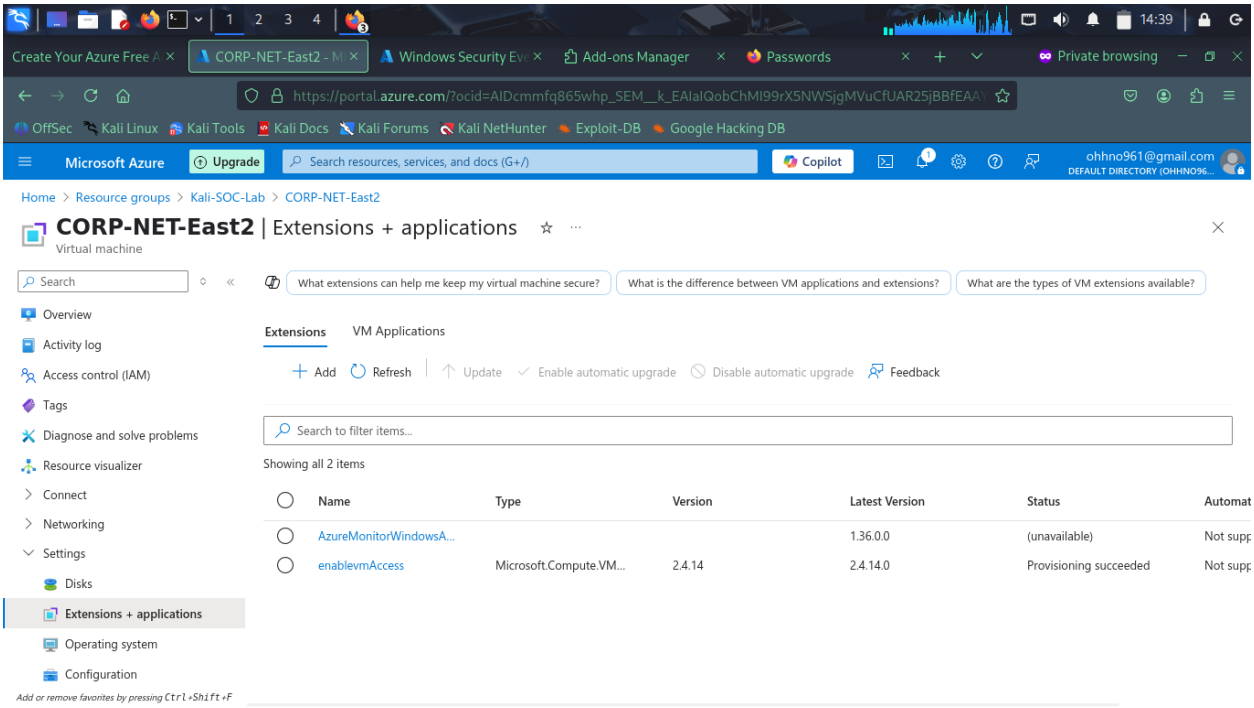


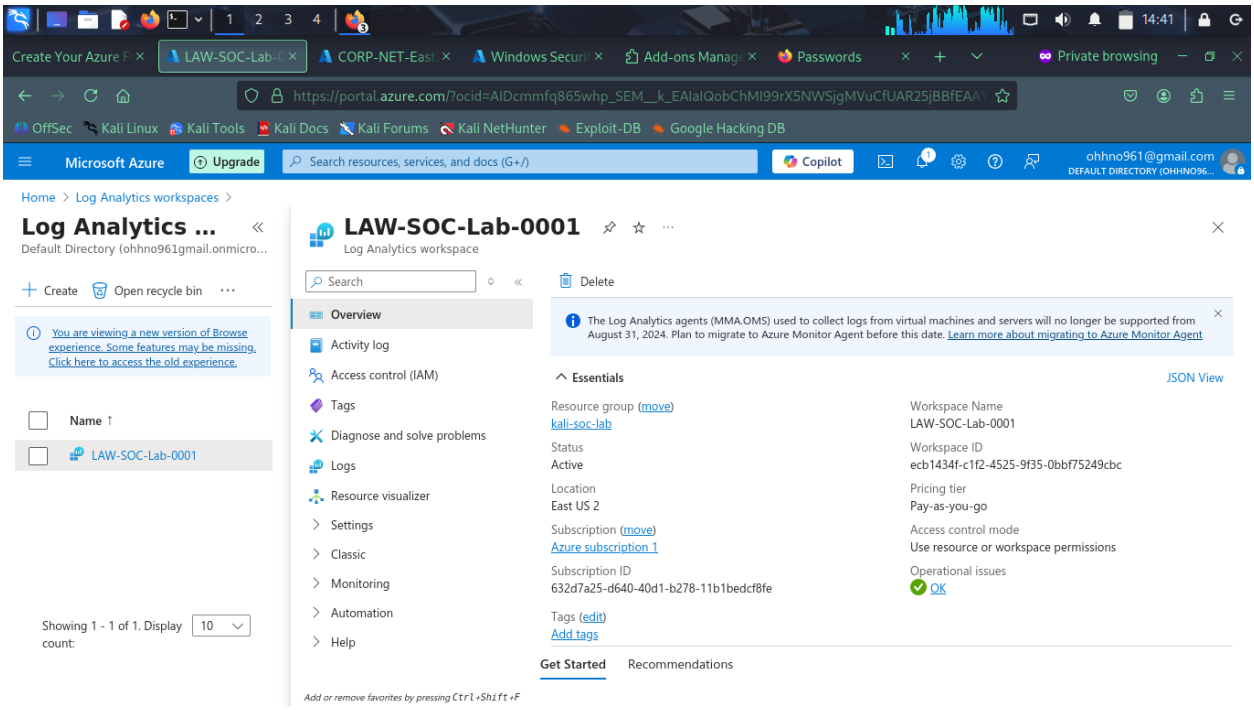


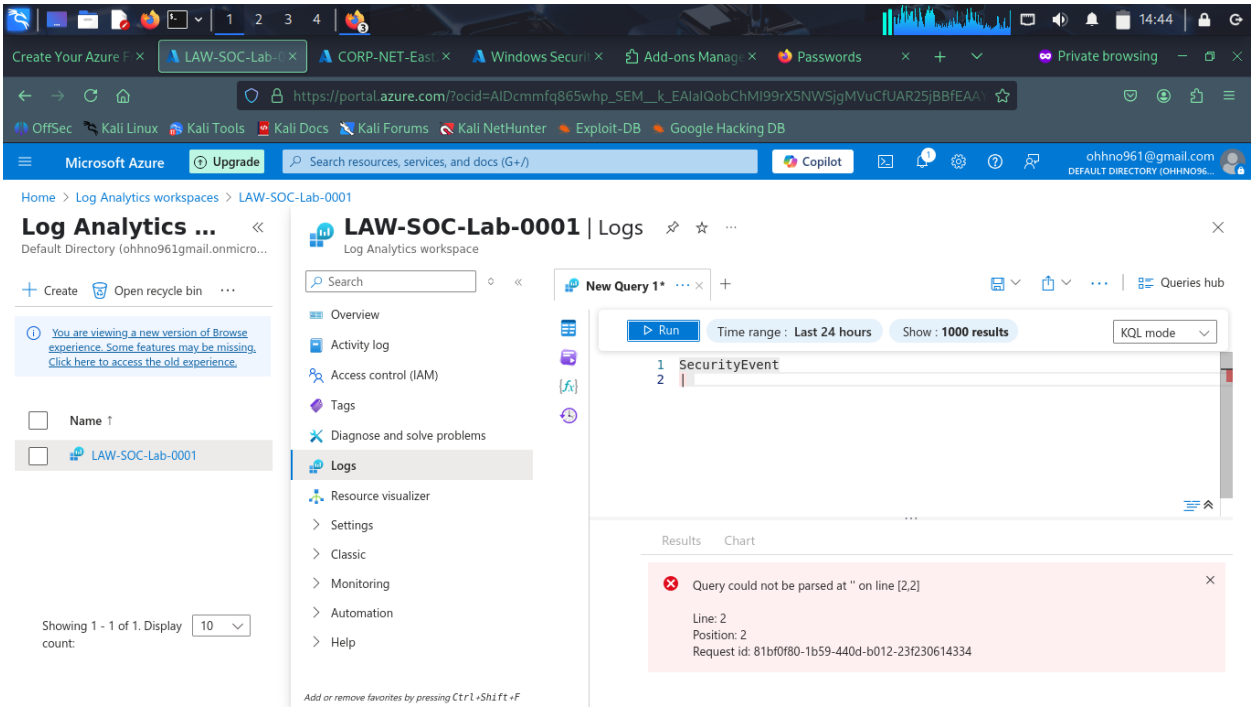

Windows Security Events
Refresh
Delete
Reinstall
74
Installed content items
22
Configuration needed
Windows Security Events
Microsoft
Provider
Microsoft
Support
3.0.9
Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The Windows 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.
Manage
Actions
View details
Search...
Content name
Security Events via Legacy Agent
Windows Security Events via AMA
AD FS Remote Auth Sync Connection
AD FS Remote HTTP Network Connection
AD user enabled and password not set within 48 hours
ADFS Database Named Pipe Connection
Excessive Windows Logon Failures
Exchange OAB Virtual Directory Attribute Containing Poten
No templates selected
Select templates to view more details

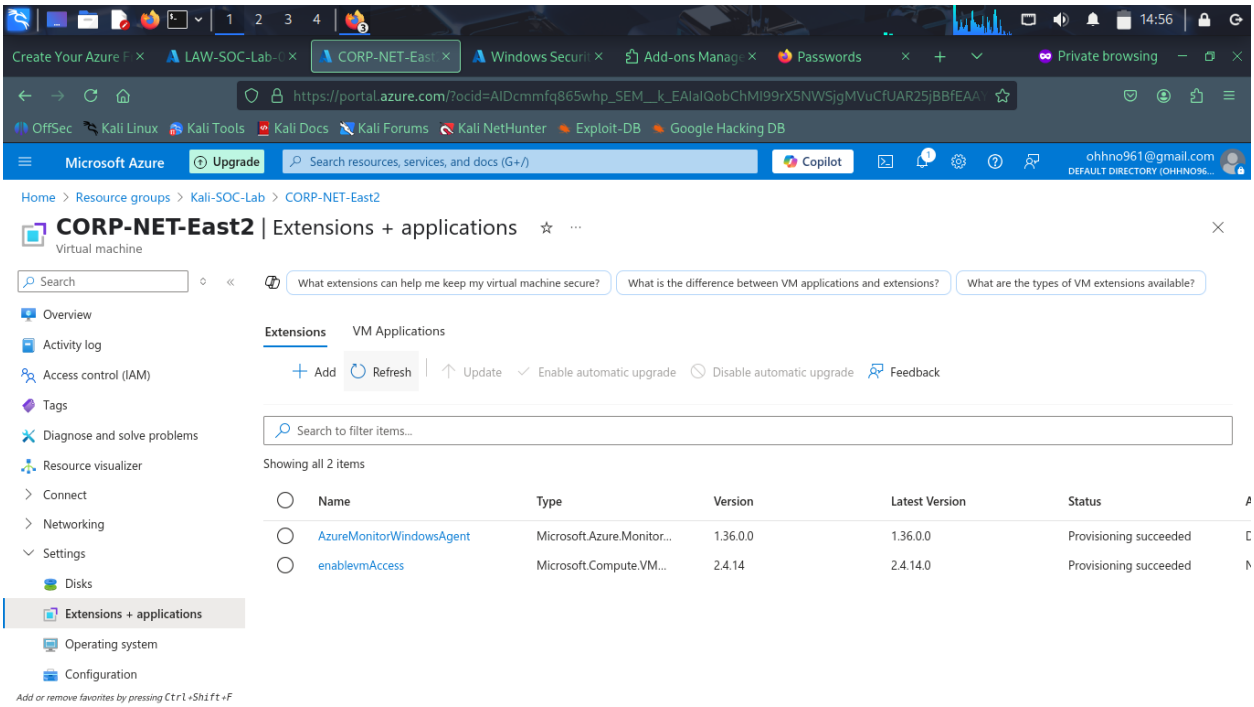

CORP-NET-East2 | Extensions + applications
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
What extensions can help me keep my virtual machine 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
Search to filter items...
Showing all 1 items
Name
Type
Version
Latest Version
Status
enablevmAccess
Microsoft.Compute.VM...
2.4.14
2.4.14.0
Provisioning succeeded

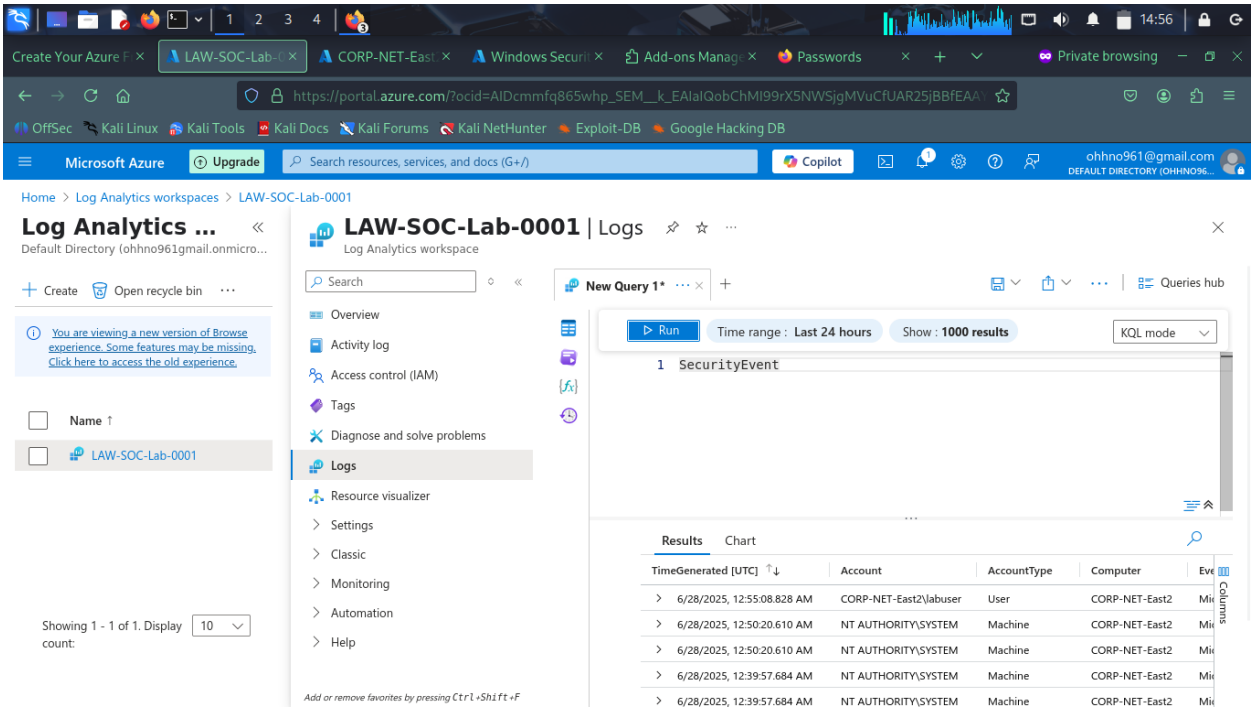

Create Your Azure Free A
CORP-NET-East2 - M
Create Data Collectio
Add-ons Manager
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBf
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Micro
Windows Security Events via AMA
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
Create Data Collection Rule
Data collection rule management
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
Selected: All
Resource Groups
Selected: All
Resource Types
Selected: All
Locations
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 >

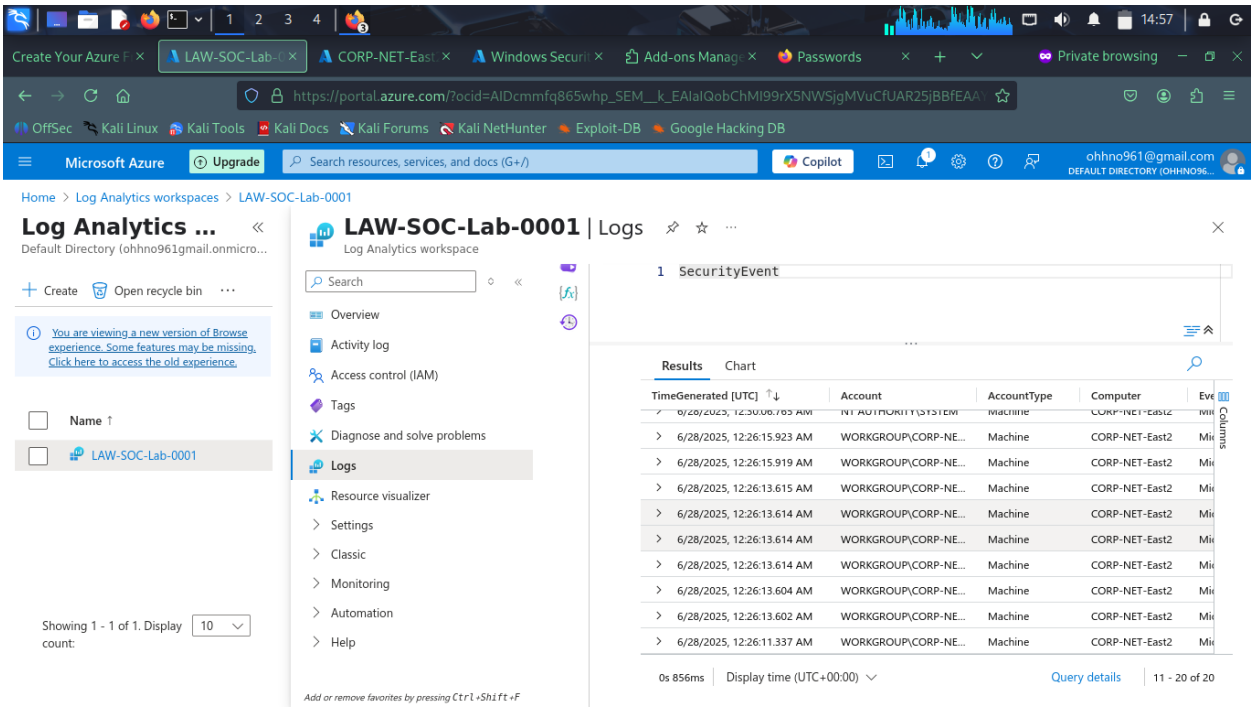

Create Your Azure Free A
CORP-NET-East2 - M
Windows Security Ev
Add-ons Manager
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Resource groups > Kali-SOC-Lab > CORP-NET-East2
CORP-NET-East2 | Extensions + applications
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Add or remove favorites by pressing Ctrl+Shift+F
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
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
2.4.14.0
Provisioning succeeded
Not supp

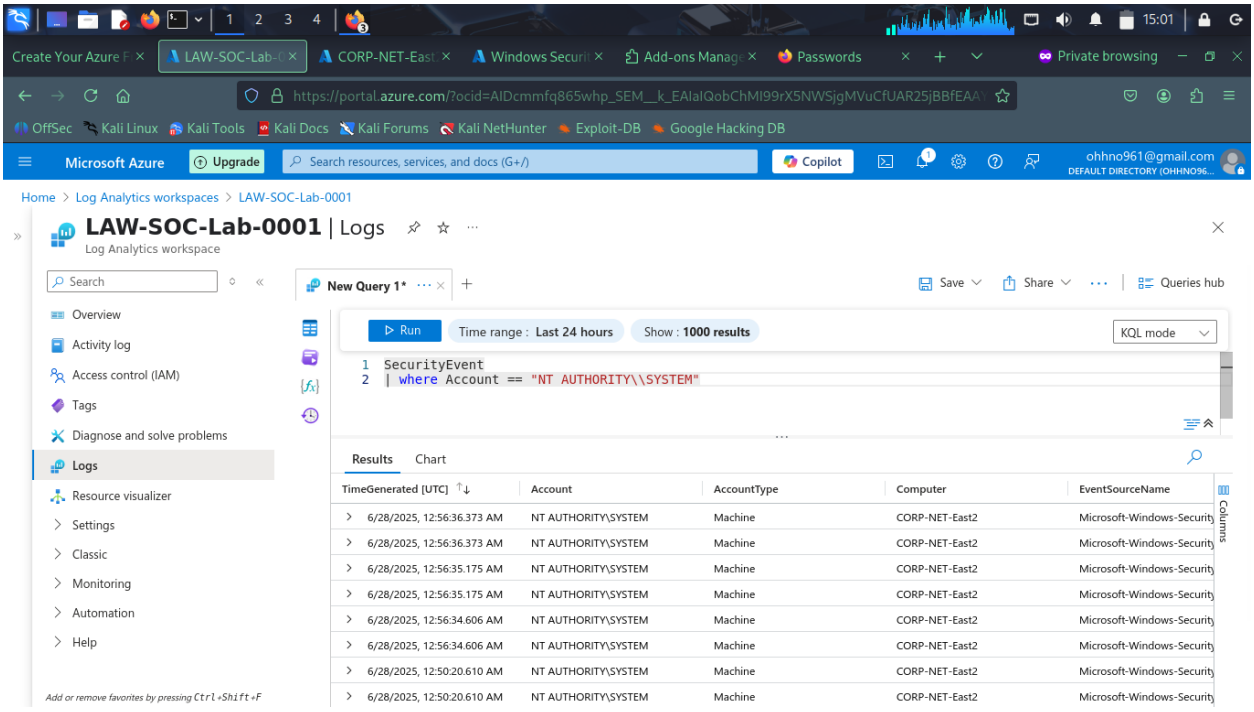

Create Your Azure F
LAW-SOC-Lab-(
CORP-NET-East
Windows Securit
Add-ons Manage
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces >
Log Analytics ...
Default Directory (ohhno961gmail.onmicro...
Create
Open recycle bin
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-SOC-Lab-0001
Showing 1 - 1 of 1. Display count:
10
LAW-SOC-Lab-0001
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Delete
The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to Azure Monitor Agent
Essentials
JSON View
Resource group (move)
kali-soc-lab
Status
Active
Location
East US 2
Subscription (move)
Azure subscription 1
Subscription ID
632d7a25-d640-40d1-b278-11b1bedcf8fe
Tags (edit)
Add tags
Workspace Name
LAW-SOC-Lab-0001
Workspace ID
ecb1434f-c1f2-4525-9f35-0bbf75249cbc
Pricing tier
Pay-as-you-go
Access control mode
Use resource or workspace permissions
Operational issues
OK
Get Started
Recommendations
Add or remove favorites by pressing Ctrl+Shift+F

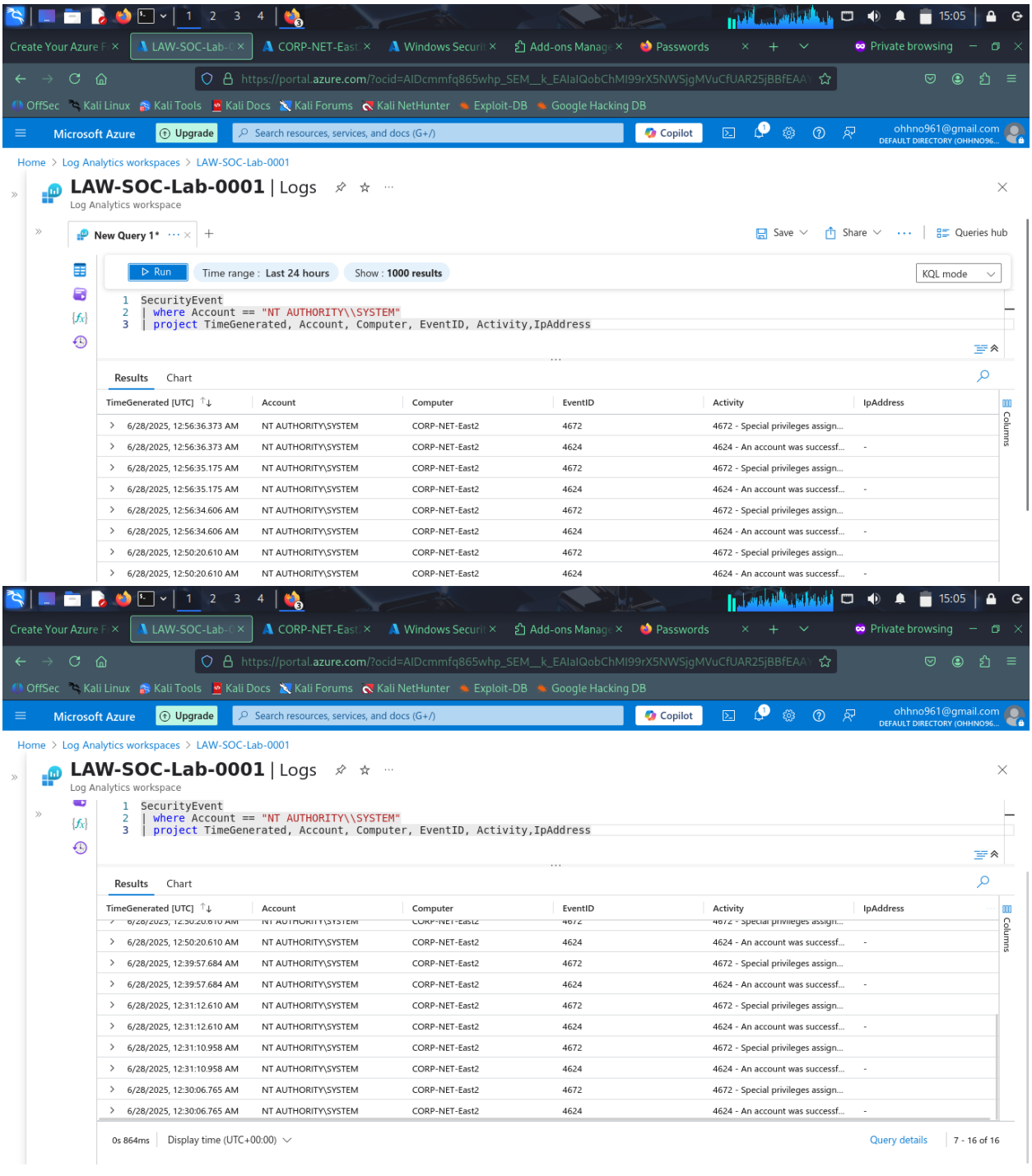

Create Your Azure F
LAW-SOC-Lab-(
CORP-NET-East
Windows Securit
Add-ons Manage
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
Log Analytics ...
Default Directory (ohhno961gmail.onmicro...
Create
Open recycle bin
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-SOC-Lab-0001
Showing 1 - 1 of 1. Display count:
10
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
New Query 1*
Queries hub
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
Add or remove favorites by pressing Ctrl+Shift+F


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Resource groups > Kali-SOC-Lab > CORP-NET-East2
CORP-NET-East2 | Extensions + applications
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Disks
Extensions + applications
Operating system
Configuration
Add or remove favorites by pressing Ctrl+Shift+F
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
Search to filter items...
Showing all 2 items
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

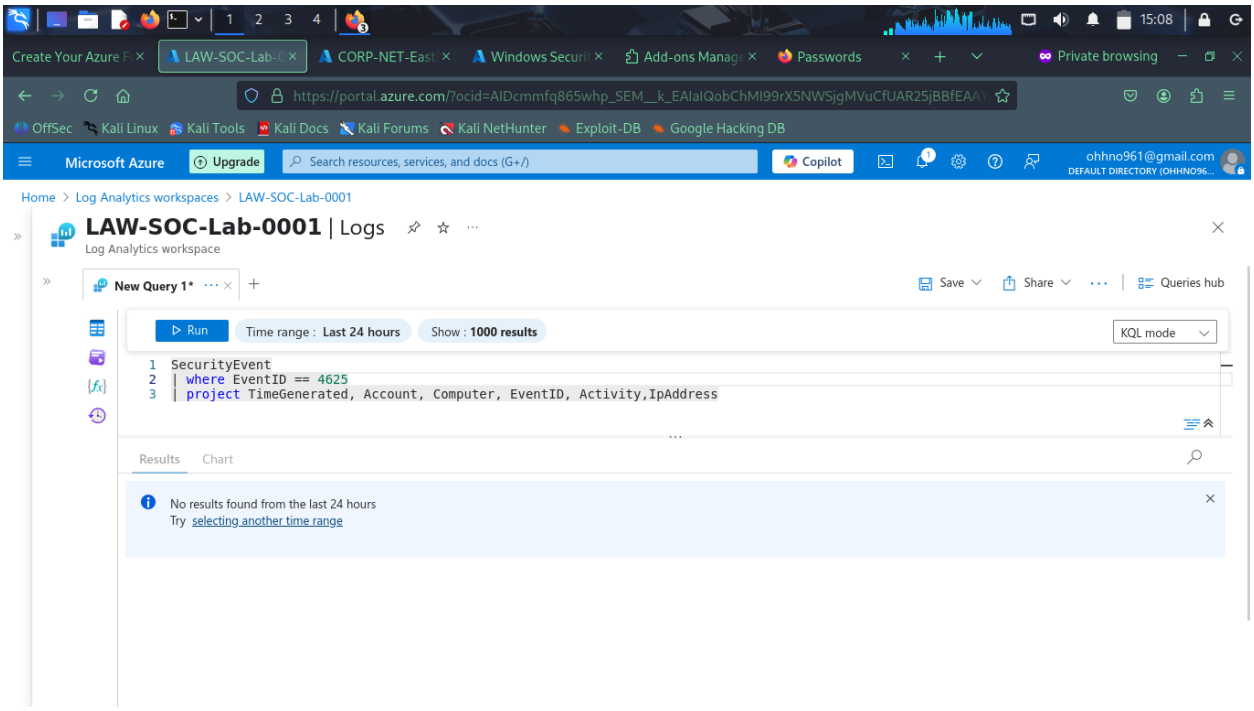

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
Log Analytics ...
Default Directory (ohhno961gmail.onmicro...
Create
Open recycle bin
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-SOC-Lab-0001
Showing 1 - 1 of 1. Display count:
10
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
New Query 1*
Queries hub
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
1 SecurityEvent
Results
Chart
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
Columns

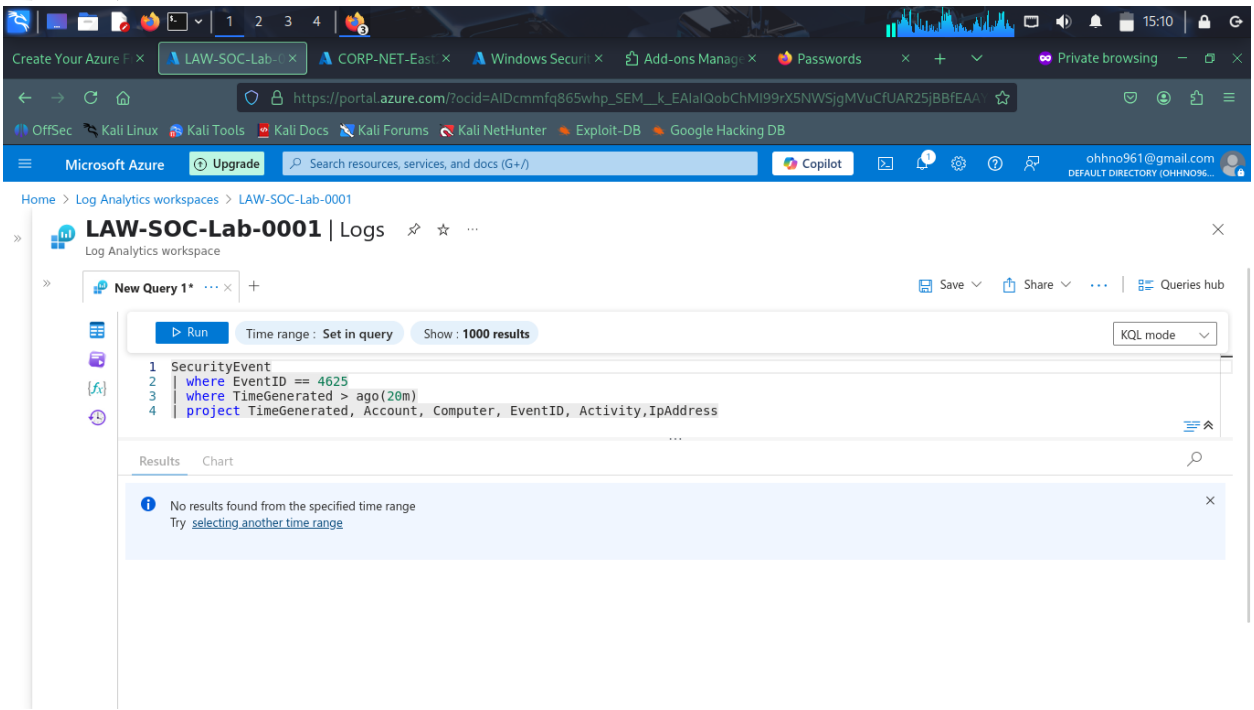

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
Log Analytics ...
Default Directory (ohhno961gmail.onmicro...
Create
Open recycle bin
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-SOC-Lab-0001
Showing 1 - 1 of 1. Display count: 10
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
1 SecurityEvent
Results
Chart
TimeGenerated [UTC]
Account
AccountType
Computer
6/28/2025, 12:26:15.923 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:15.919 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:13.615 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:13.614 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:13.614 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:13.614 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:13.604 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:13.602 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
6/28/2025, 12:26:11.337 AM WORKGROUP\CORP-NE... Machine CORP-NET-East2
Columns
0s 856ms
Display time (UTC+00:00)
Query details
11 - 20 of 20

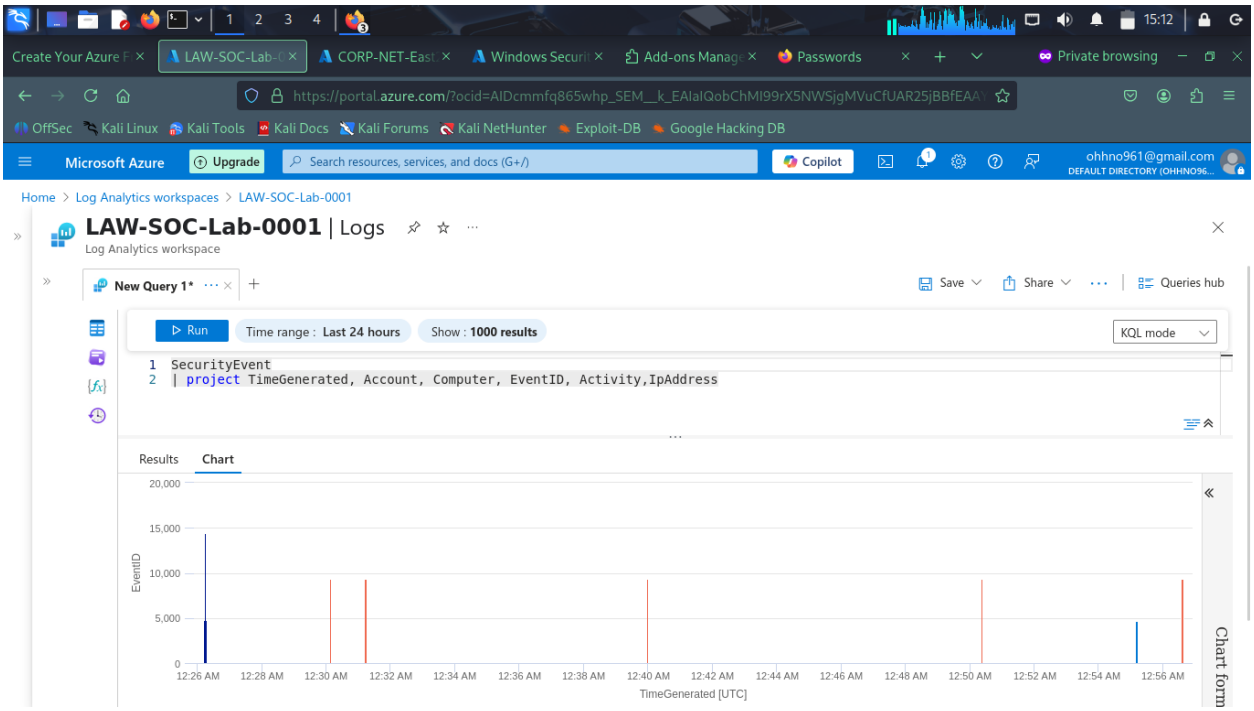

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
1 SecurityEvent
2 | where Account == "NT AUTHORITY\\SYSTEM"
Results
Chart
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
Columns


Create Your Azure F
LAW-SOC-Lab-0
CORP-NET-East
Windows Securit
Add-ons Manage
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
New Query 1*
Save
Share
Queries hub
Run
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
Columns
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... -

Create Your Azure F
LAW-SOC-Lab-0
CORP-NET-East
Windows Securit
Add-ons Manage
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
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
Columns
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

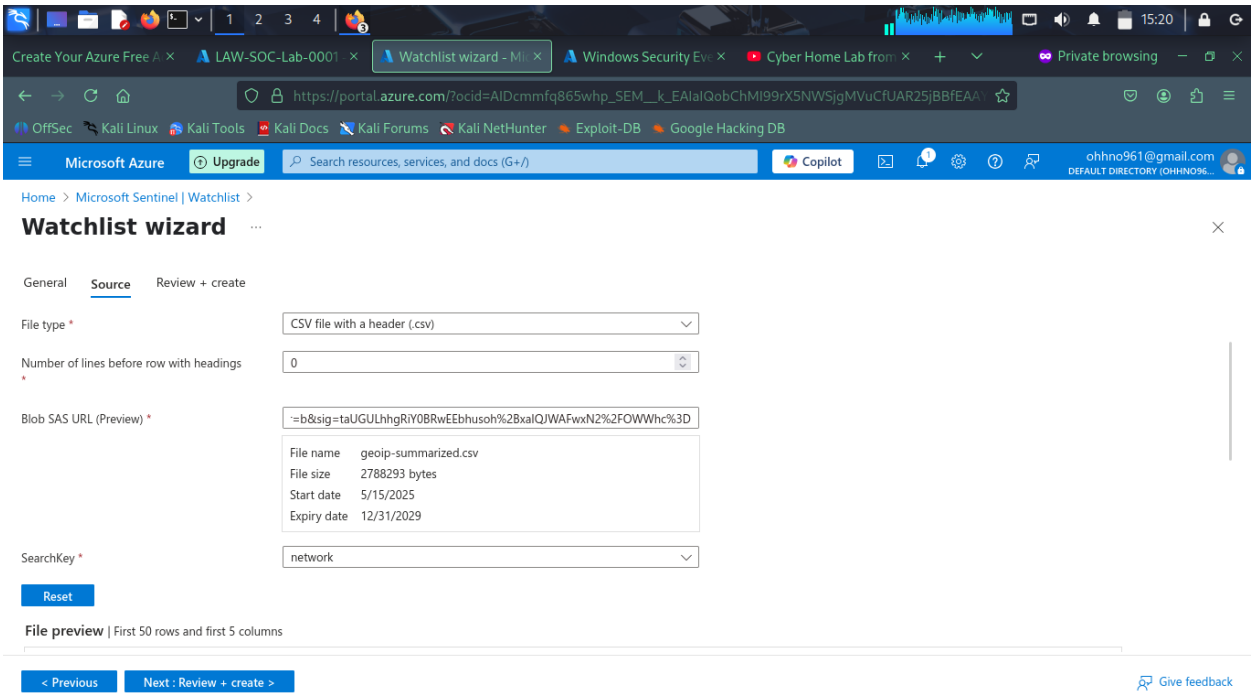

15:08
Create Your Azure F
LAW-SOC-Lab-0
CORP-NET-East
Windows Securit
Add-ons Manage
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
1 SecurityEvent
2 | where EventID == 4625
3 | project TimeGenerated, Account, Computer, EventID, Activity,IpAddress
Results
Chart
No results found from the last 24 hours
Try selecting another time range

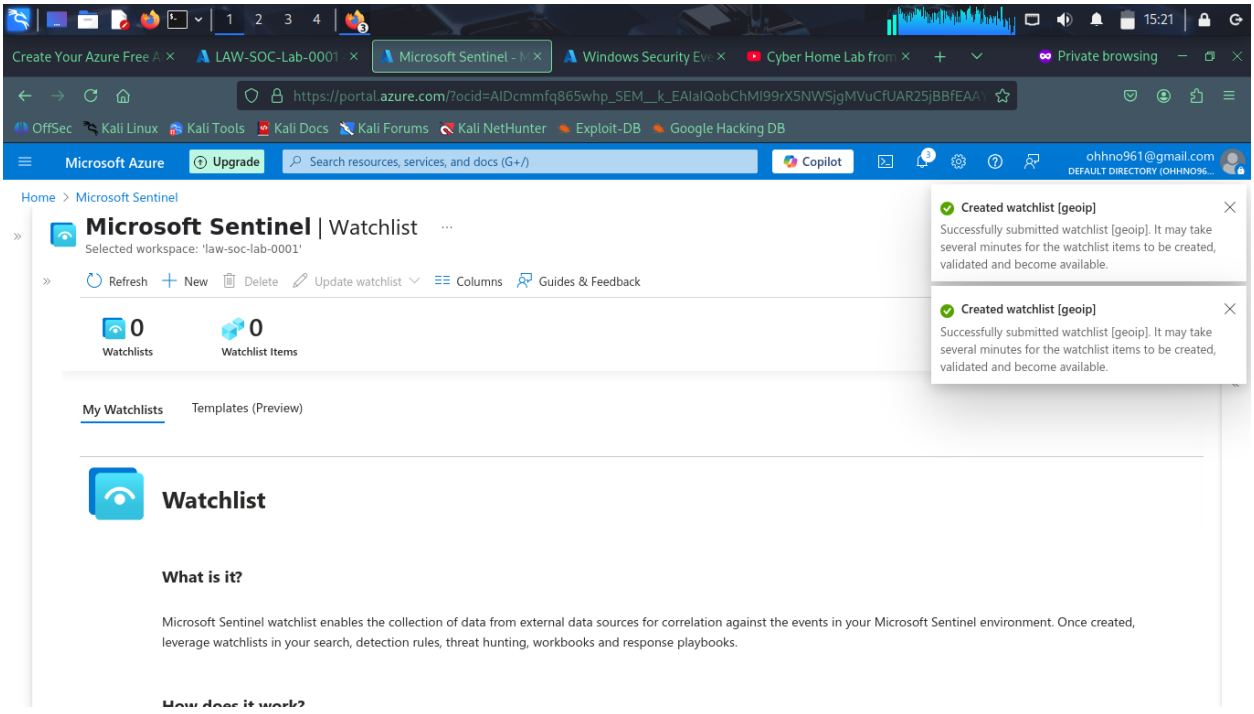

15:10
Create Your Azure F
LAW-SOC-Lab-0
CORP-NET-East
Windows Securit
Add-ons Manage
Passwords
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Log Analytics workspaces > LAW-SOC-Lab-0001
LAW-SOC-Lab-0001 | Logs
Log Analytics workspace
New Query 1*
Save
Share
Queries hub
Run
Time range : Set in query
Show : 1000 results
KQL mode
1 SecurityEvent
2 | where EventID == 4625
3 | where TimeGenerated > ago(20m)
4 | project TimeGenerated, Account, Computer, EventID, Activity,IpAddress
Results
Chart
No results found from the specified time range
Try selecting another time range

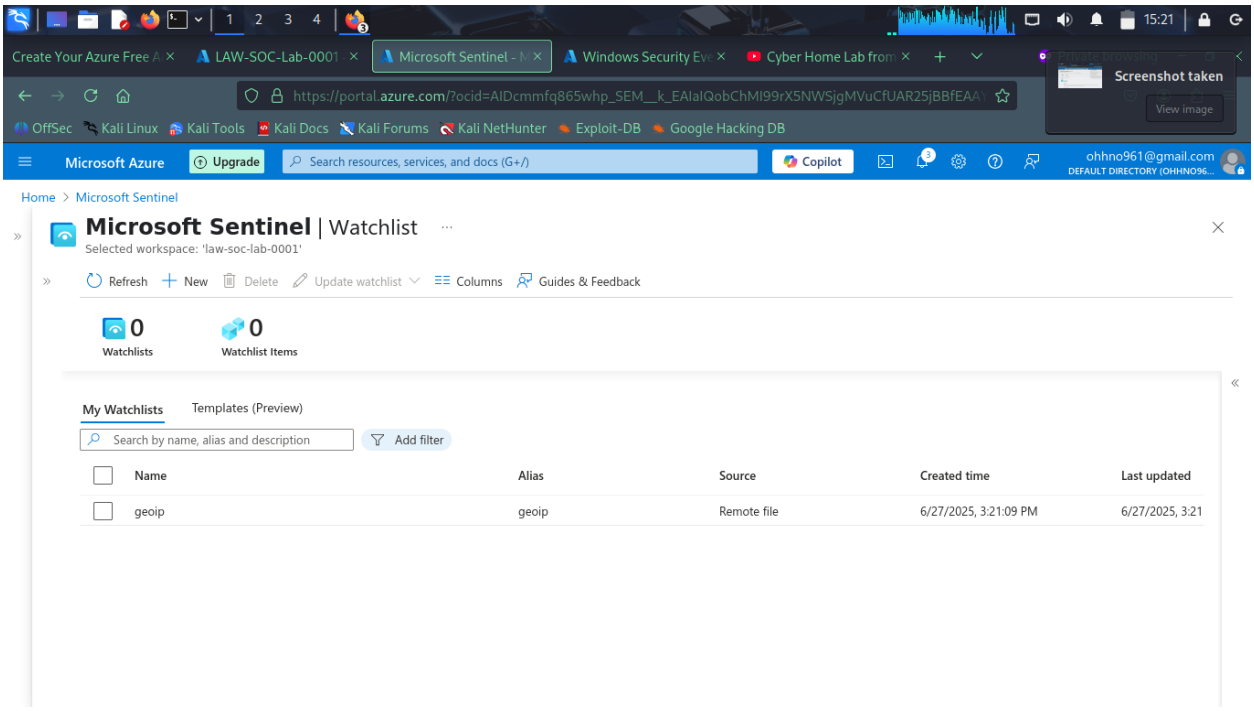


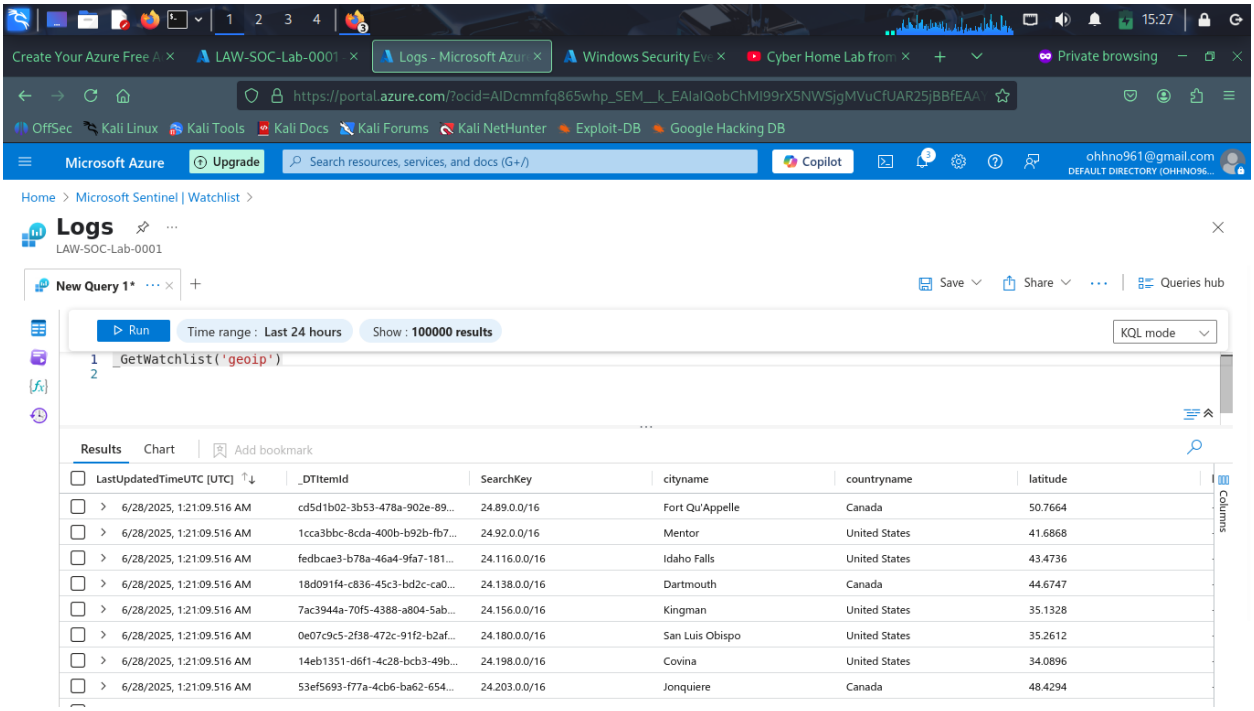
9.Geolocation Enrichment 🌍📍

- 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**


Create Your Azure Free A
LAW-SOC-Lab-0001
Watchlist wizard - Mi
Windows Security Eve
Cyber Home Lab from
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Microsoft Sentinel | Watchlist >
Watchlist wizard
General
Source
Review + create
File type *
CSV file with a header (.csv)
Number of lines before row with headings *
0
Blob SAS URL (Preview) *
:=b&sig=taUGULhhgRiY0BRwEEbhusoh%2BxaIQJWAFwxN2%2FOWWhc%3D
File name geoip-summarized.csv
File size 2788293 bytes
Start date 5/15/2025
Expiry date 12/31/2029
SearchKey *
network
Reset
File preview | First 50 rows and first 5 columns
< Previous
Next : Review + create >
Give feedback


Create Your Azure Free A
LAW-SOC-Lab-0001
Microsoft Sentinel - M
Windows Security Eve
Cyber Home Lab from
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBBfEAA
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Microsoft Sentinel
Microsoft Sentinel | Watchlist
Selected workspace: 'law-soc-lab-0001'
Refresh
New
Delete
Update watchlist
Columns
Guides & Feedback
0
Watchlists
0
Watchlist Items
My Watchlists
Templates (Preview)
Watchlist
What is it?
Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.
How does it work?
Created watchlist [geoip]
Successfully submitted watchlist [geoip]. It may take several minutes for the watchlist items to be created, validated and become available.
Created watchlist [geoip]
Successfully submitted watchlist [geoip]. It may take several minutes for the watchlist items to be created, validated and become available.

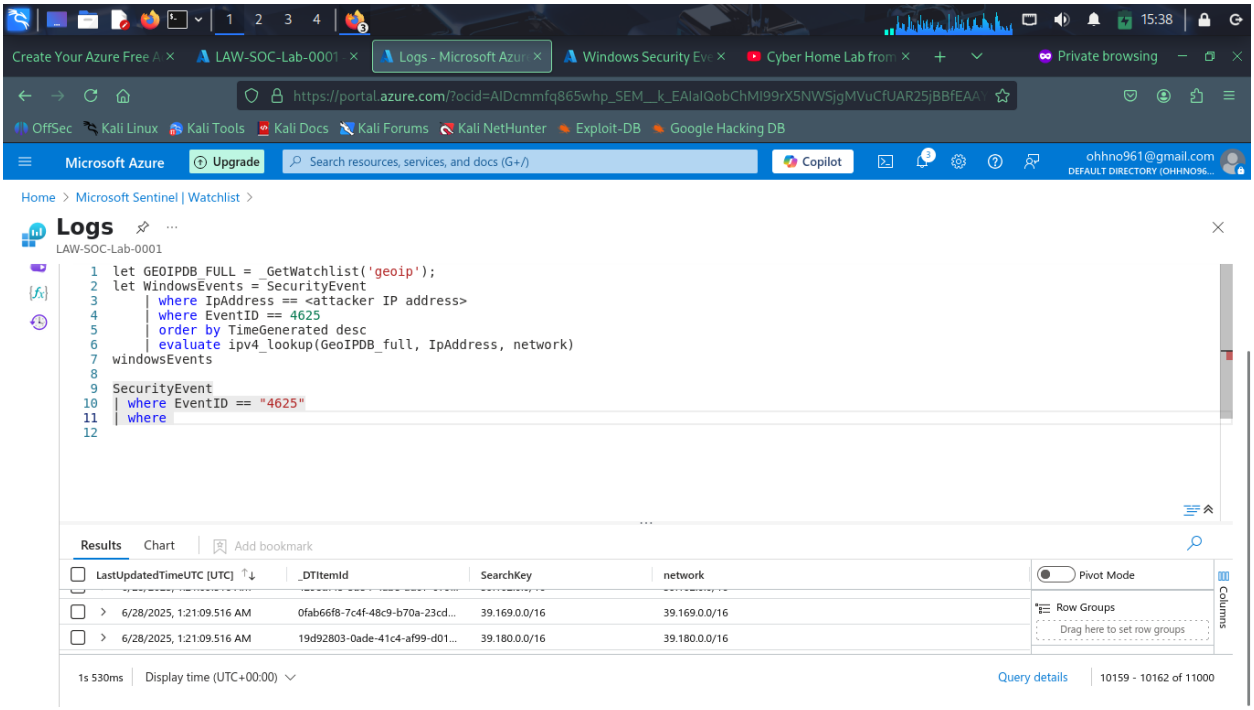


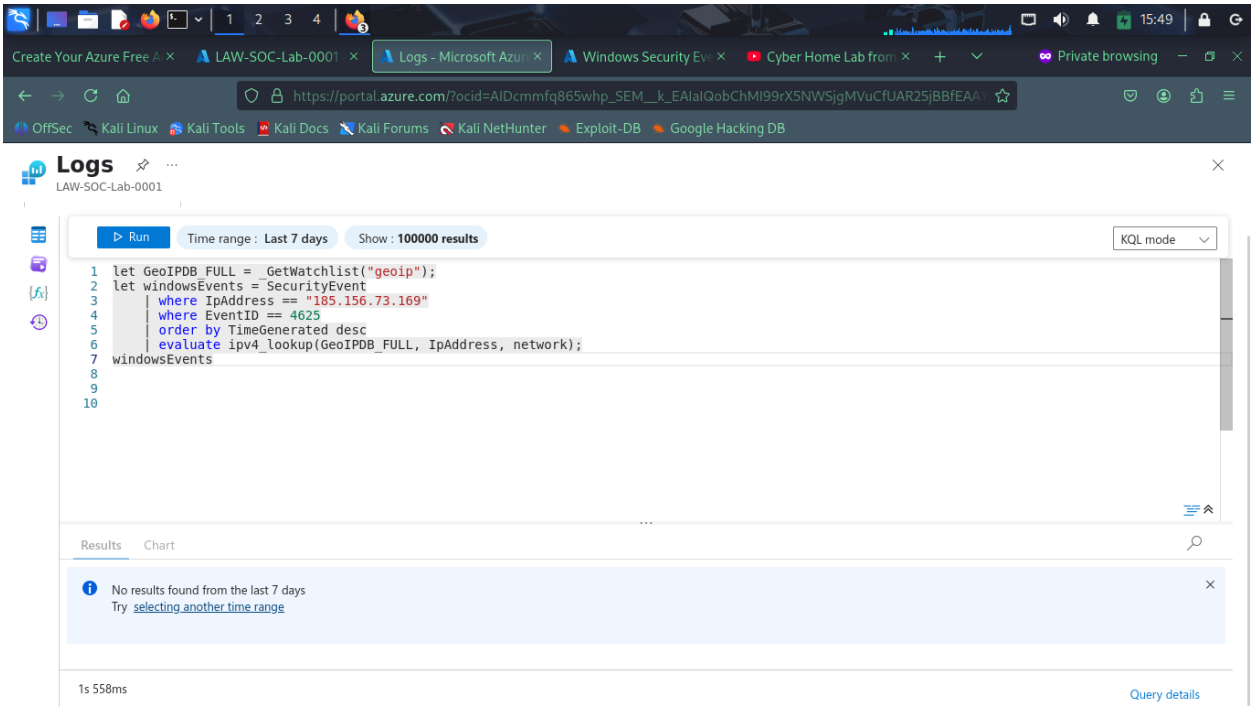


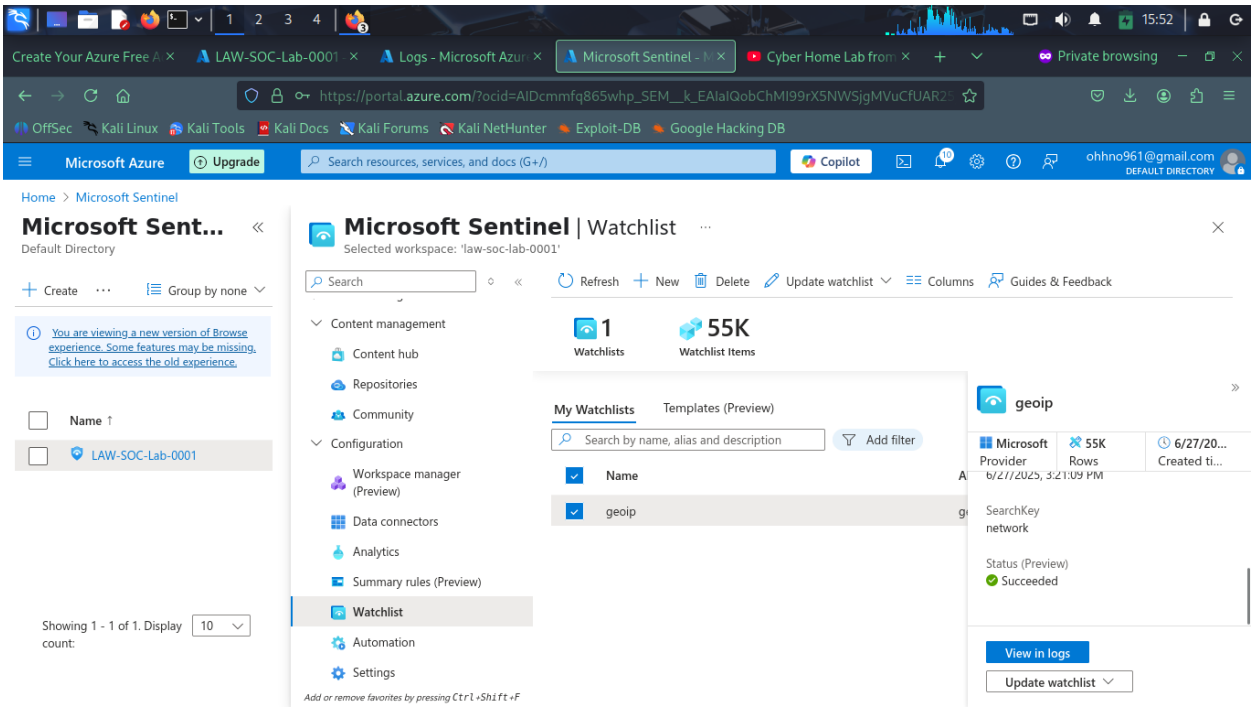
🔟 KQL Threat Hunting 🧠🔍

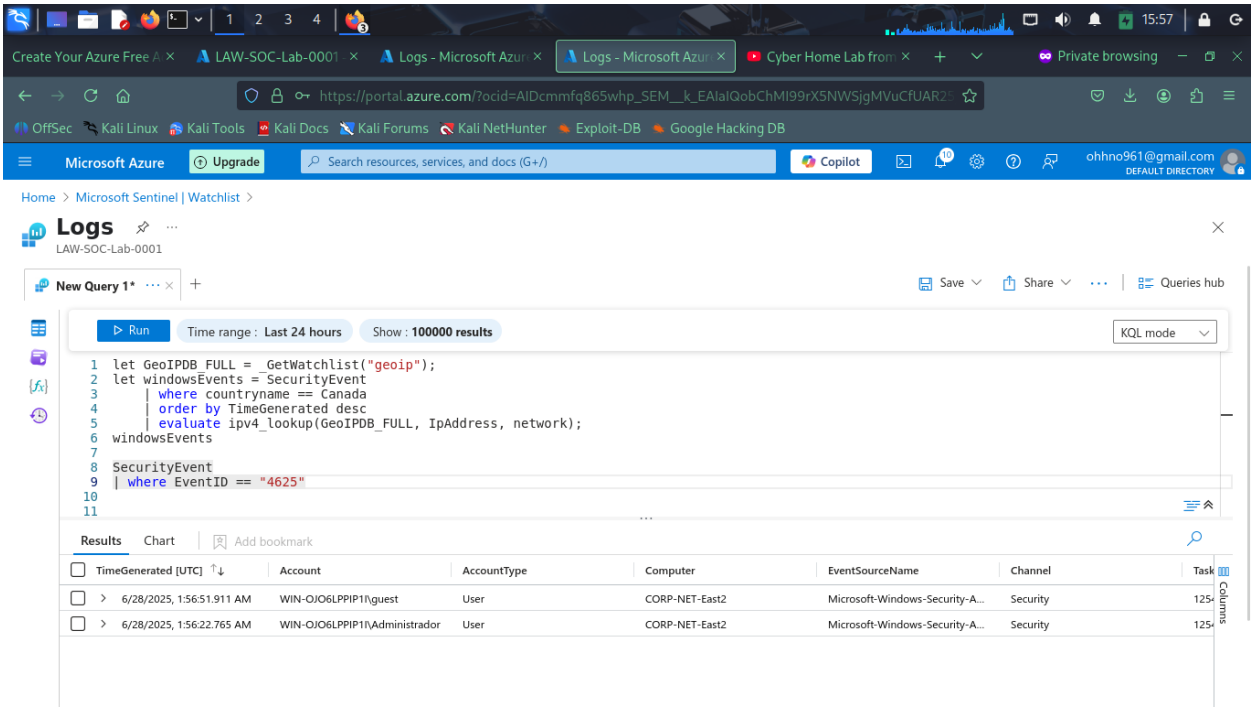
- In `Log Analytics` → **Logs**
- Run **failed login detection**:
- SecurityEvent
- | where EventID == 4625 // Failed logon
- | join kind=inner (GetWatchlist('GeoIP')) on $left.IpAddress == $right.Network

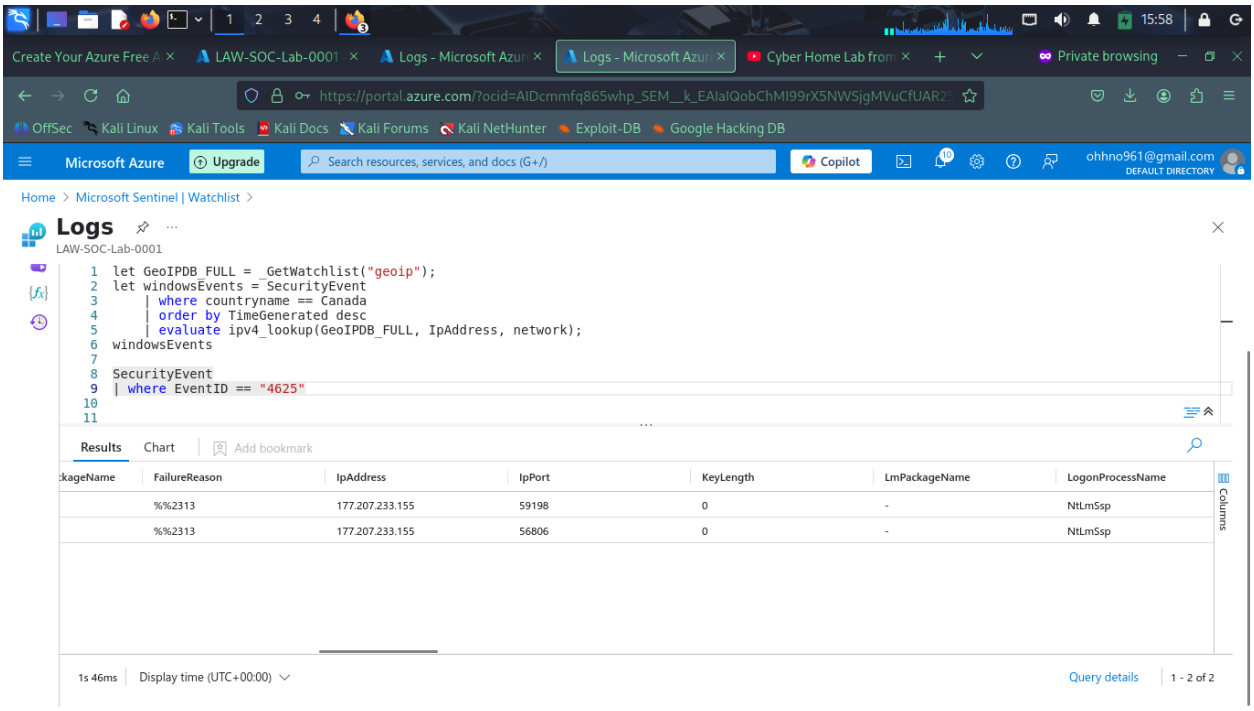
- | project TimeGenerated, Computer, AttackerIP=IpAddress,
- Country=CountryName, City=CityName, Latitude, Longitude
- | summarize Attempts=count() by AttackerIP, Country, City, Latitude, Longitude

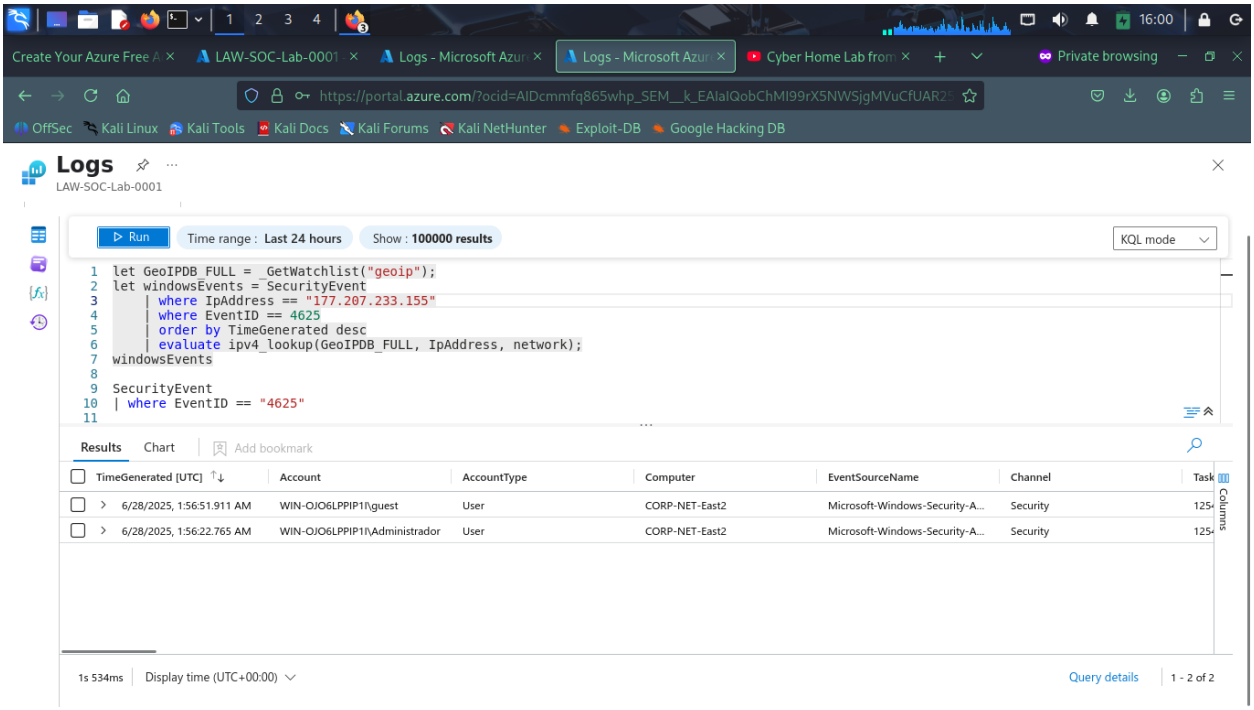


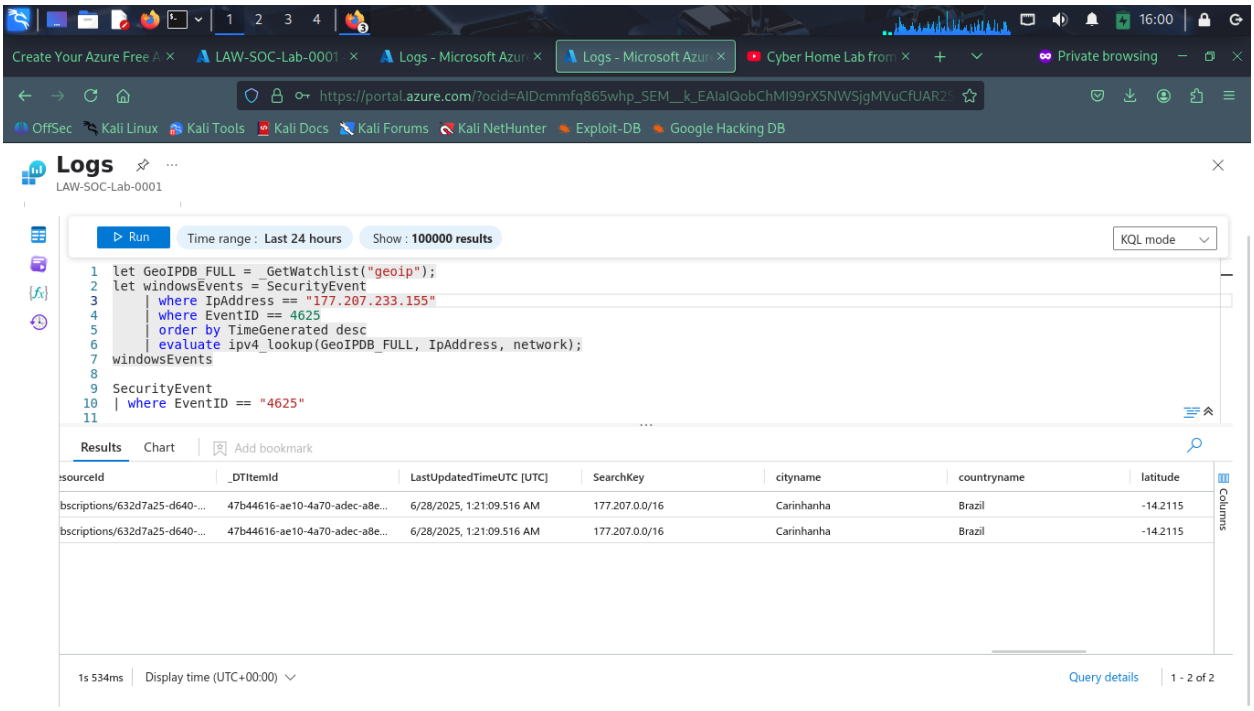


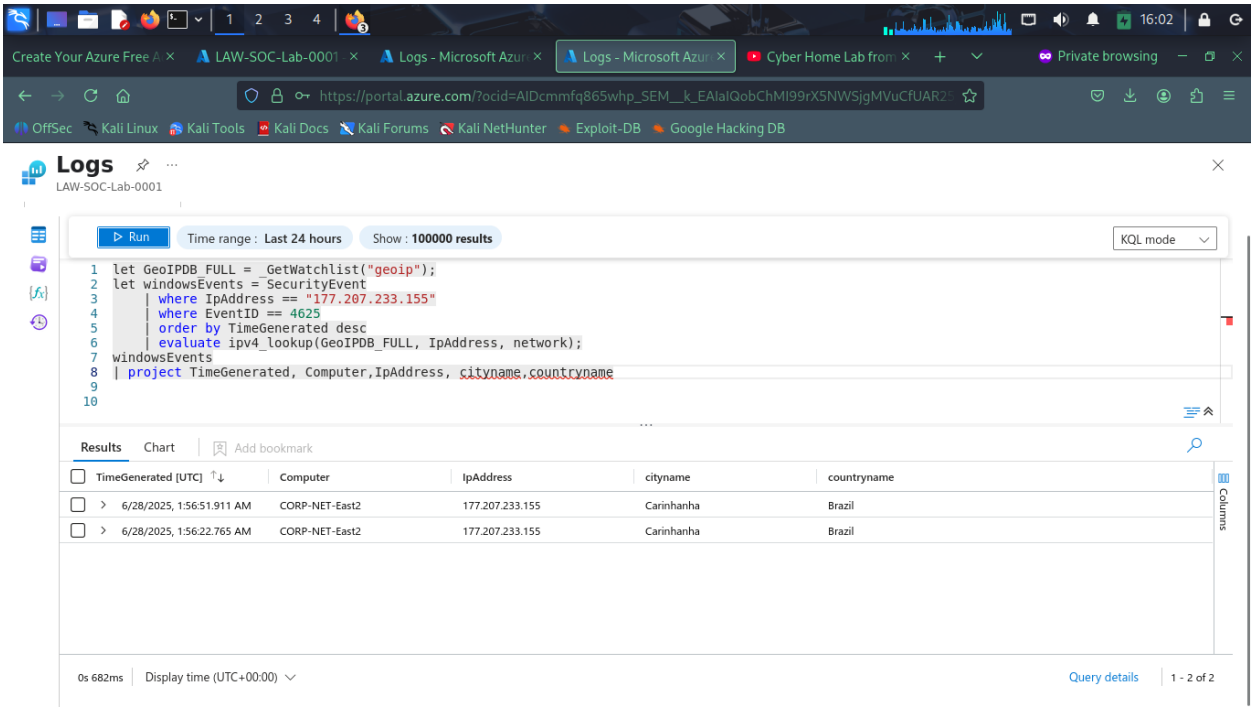

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel
Microsoft Sent...
Default Directory
Create
Group by none
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
LAW-SOC-Lab-0001
Showing 1 - 1 of 1. Display count: 10
Microsoft Sentinel | Watchlist
Selected workspace: 'law-soc-lab-0001'
Search
Refresh
New
Delete
Update watchlist
Columns
Guides & Feedback
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Automation
Settings
Add or remove favorites by pressing Ctrl+Shift+F
1
Watchlists
55K
Watchlist Items
My Watchlists
Templates (Preview)
Search by name, alias and description
Add filter
Name
geoip
geoip
Microsoft
Provider
55K
Rows
6/27/20...
Created ti...
SearchKey
network
Status (Preview)
Succeeded
View in logs
Update watchlist

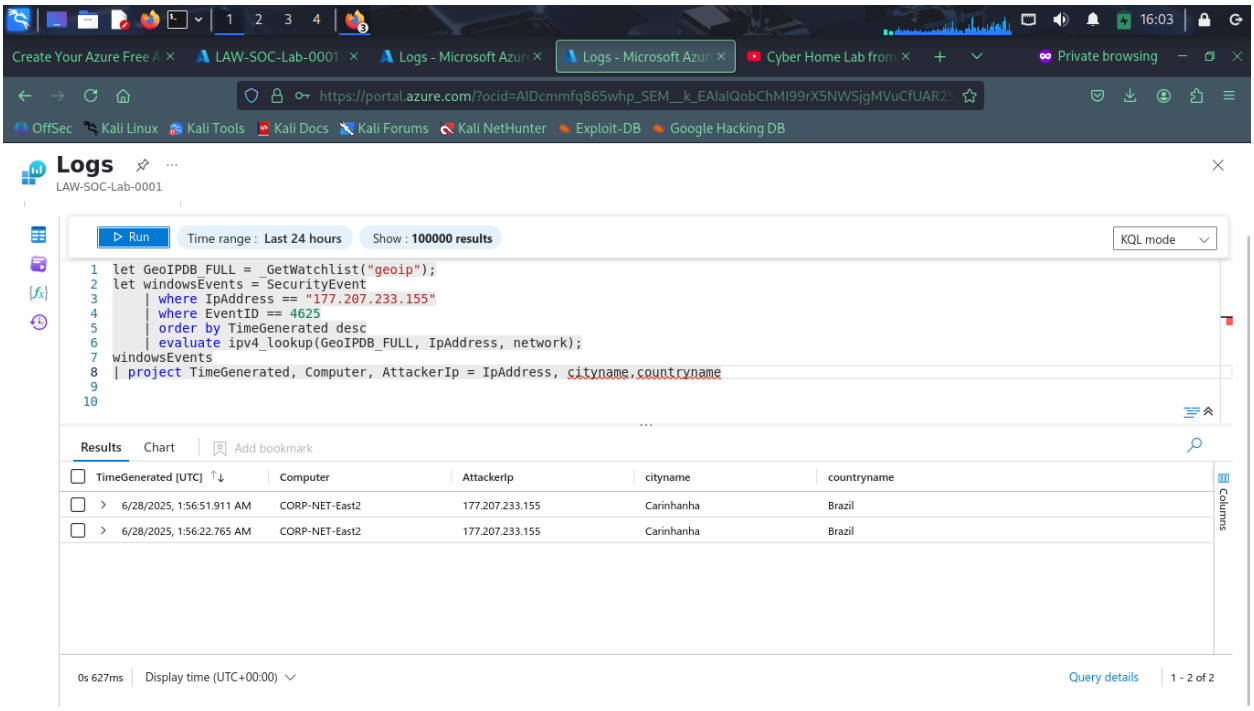

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel | Watchlist
Logs
LAW-SOC-Lab-0001
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 24 hours
Show : 100000 results
KQL mode
let GeoIPDB_FULL = _GetWatchlist("geoip");
let windowsEvents = SecurityEvent
| where countryname == Canada
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
windowsEvents
SecurityEvent
| where EventID == "4625"
Results
Chart
Add bookmark
TimeGenerated [UTC]
Account
AccountType
Computer
EventSourceName
Channel
Task
6/28/2025, 1:56:51.911 AM
WIN-OJO6LPPIP1I\guest
User
CORP-NET-East2
Microsoft-Windows-Security-A...
Security
125
6/28/2025, 1:56:22.765 AM
WIN-OJO6LPPIP1I\Administrador
User
CORP-NET-East2
Microsoft-Windows-Security-A...
Security
125
Columns


Create Your Azure Free A
LAW-SOC-Lab-0001
Logs - Microsoft Azur
Logs - Microsoft Azur
Cyber Home Lab from
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25
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+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel | Watchlist >
Logs
LAW-SOC-Lab-0001
let GeoIPDB_FULL = _GetWatchlist("geoip");
let windowsEvents = SecurityEvent
| where countryname == Canada
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
windowsEvents
SecurityEvent
| where EventID == "4625"
Results
Chart
Add bookmark
FailureReason
IpAddress
IpPort
KeyLength
LmPackageName
LogonProcessName
%%2313
177.207.233.155
59198
0
-
NtLmSsp
%%2313
177.207.233.155
56806
0
-
NtLmSsp
Columns
1s 46ms
Display time (UTC+00:00)
Query details
1 - 2 of 2


Create Your Azure Free A
LAW-SOC-Lab-0001
Logs - Microsoft Azur
Logs - Microsoft Azur
Cyber Home Lab from
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Logs
LAW-SOC-Lab-0001
Run
Time range : Last 24 hours
Show : 100000 results
KQL mode
let GeoIPDB_FULL = _GetWatchlist("geoip");
let windowsEvents = SecurityEvent
| where IpAddress == "177.207.233.155"
| where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
windowsEvents
SecurityEvent
| where EventID == "4625"
Results
Chart
Add bookmark
TimeGenerated [UTC]
Account
AccountType
Computer
EventSourceName
Channel
6/28/2025, 1:56:51.911 AM
WIN-OJO6LPPIP1I\guest
User
CORP-NET-East2
Microsoft-Windows-Security-A...
Security
6/28/2025, 1:56:22.765 AM
WIN-OJO6LPPIP1I\Administrador
User
CORP-NET-East2
Microsoft-Windows-Security-A...
Security
Columns
1s 534ms
Display time (UTC+00:00)
Query details
1 - 2 of 2

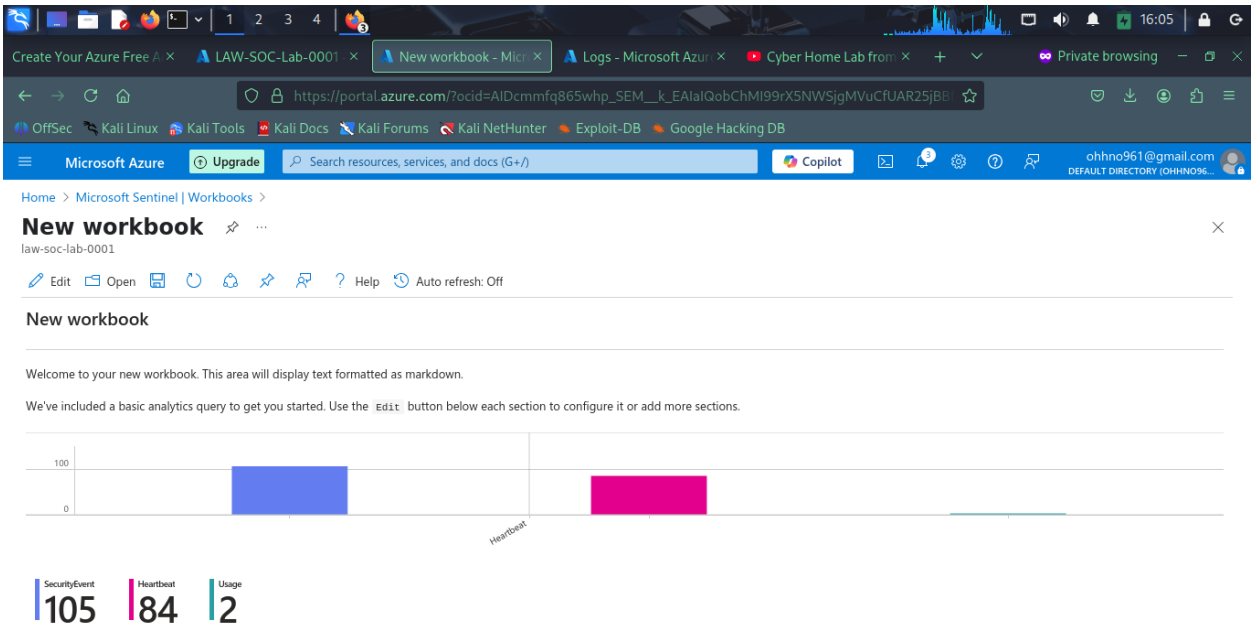

Logs
LAW-SOC-Lab-0001
Run
Time range : Last 24 hours
Show : 100000 results
KQL mode
let GeoIPDB_FULL = _GetWatchlist("geoip");
let windowsEvents = SecurityEvent
| where IpAddress == "177.207.233.155"
| where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
windowsEvents
SecurityEvent
| where EventID == "4625"
Results
Chart
Add bookmark
_DTItemId
LastUpdatedTimeUTC [UTC]
SearchKey
cityname
countryname
latitude
47b44616-ae10-4a70-adec-a8e...
6/28/2025, 1:21:09.516 AM
177.207.0.0/16
Carinhanha
Brazil
-14.2115
Columns
1s 534ms
Display time (UTC+00:00)
Query details
1 - 2 of 2

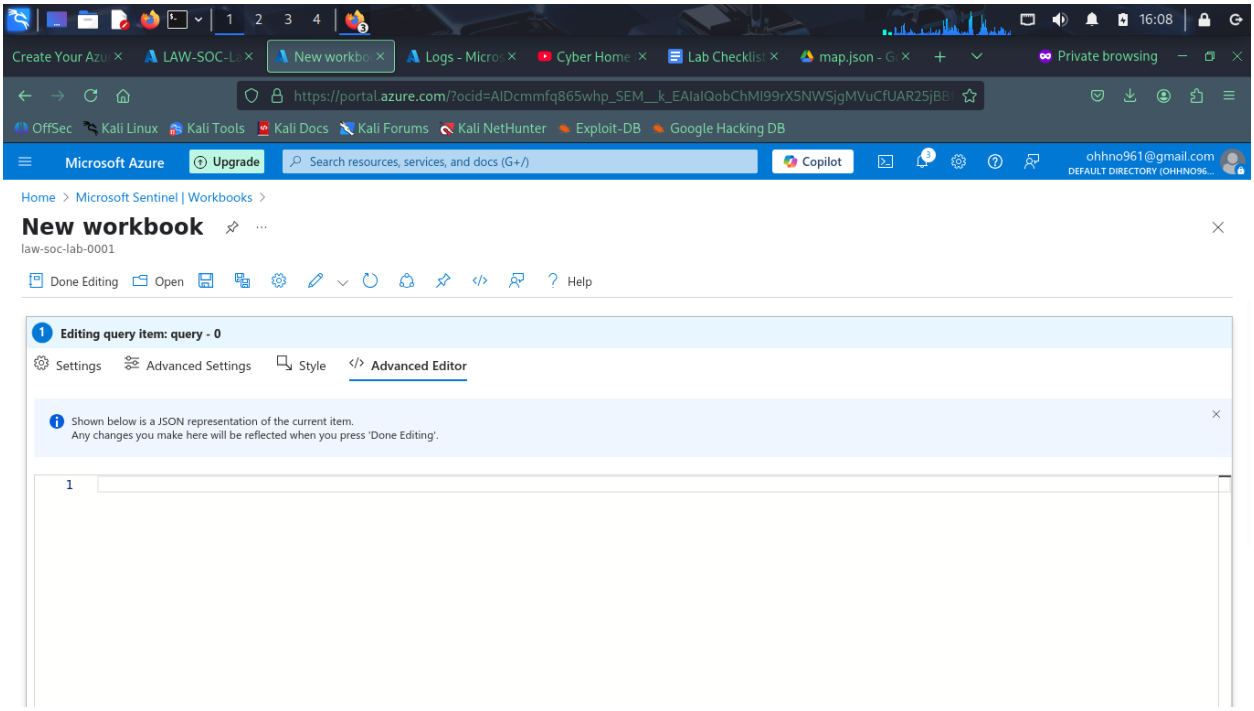

Logs
LAW-SOC-Lab-0001
Run
Time range : Last 24 hours
Show : 100000 results
KQL mode
let GeoIPDB_FULL = _GetWatchlist("geoip");
let windowsEvents = SecurityEvent
| where IpAddress == "177.207.233.155"
| where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
windowsEvents
| project TimeGenerated, Computer,IpAddress, cityname,countryname
Results
Chart
Add bookmark
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
Columns
0s 682ms
Display time (UTC+00:00)
Query details
1 - 2 of 2

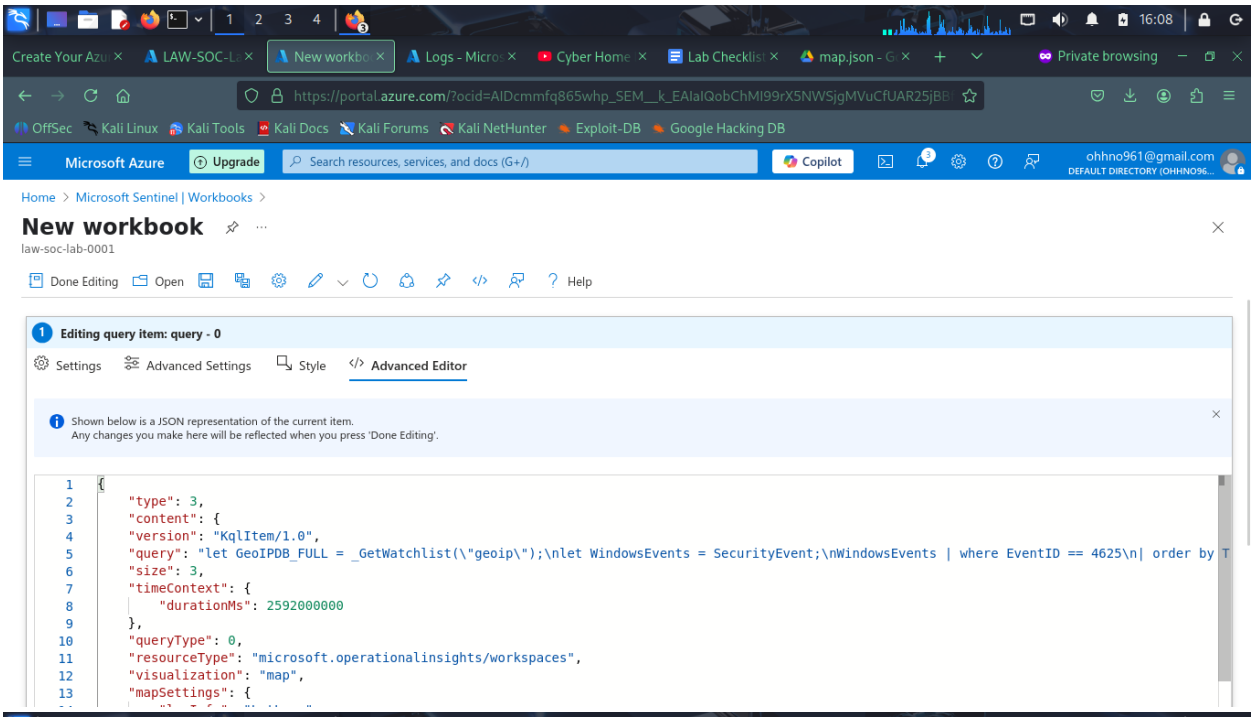


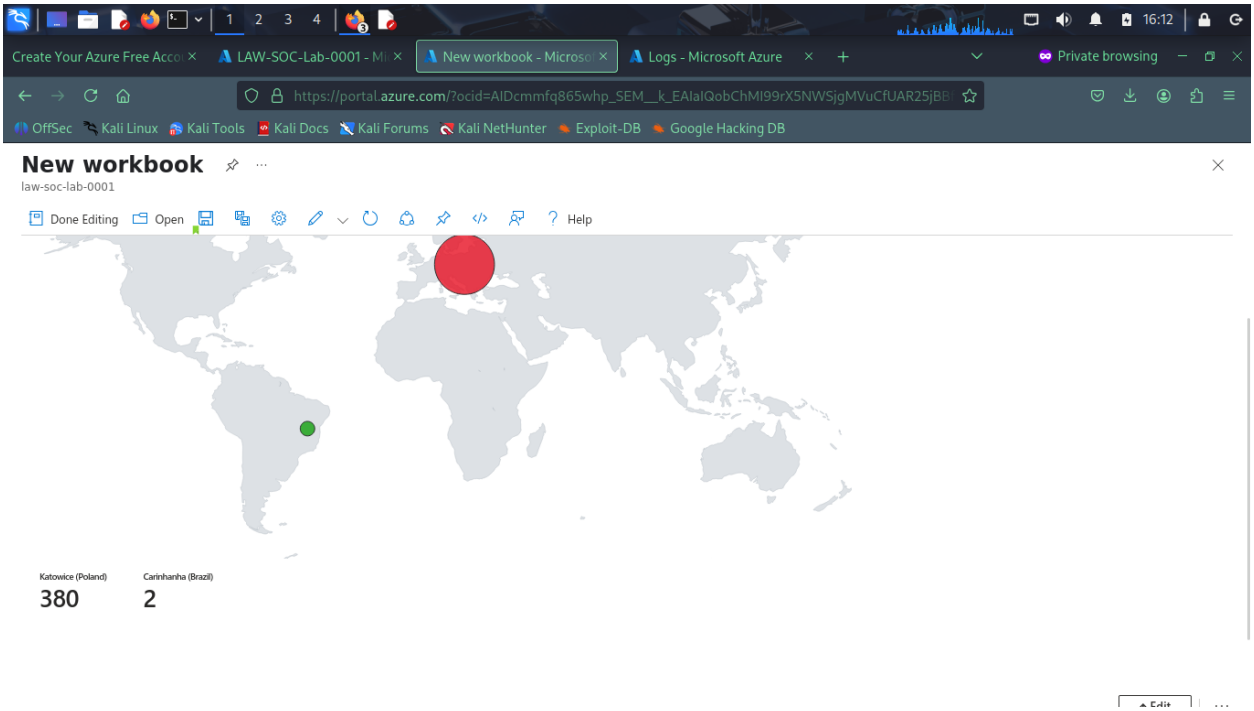
11.Attack Map Visualization 🗺️📈

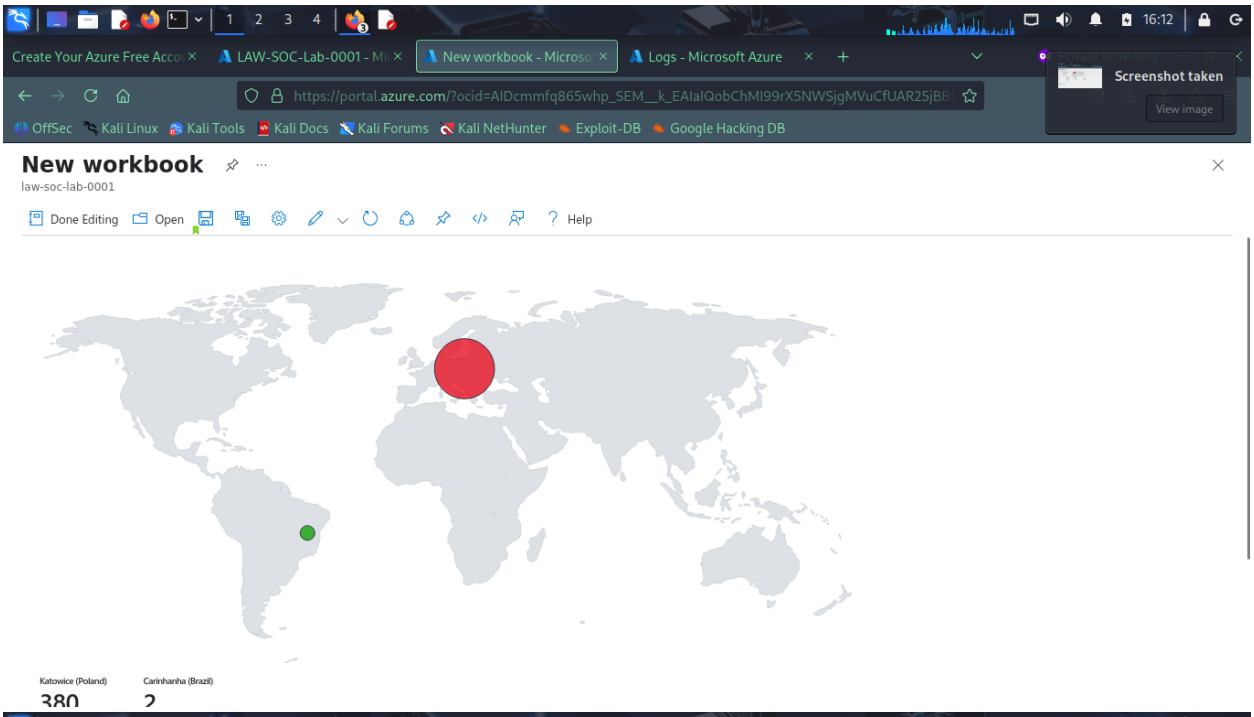
- In Sentinel → `Workbooks` → **Add workbook**
- Edit → **Advanced Editor** → Paste JSON template:

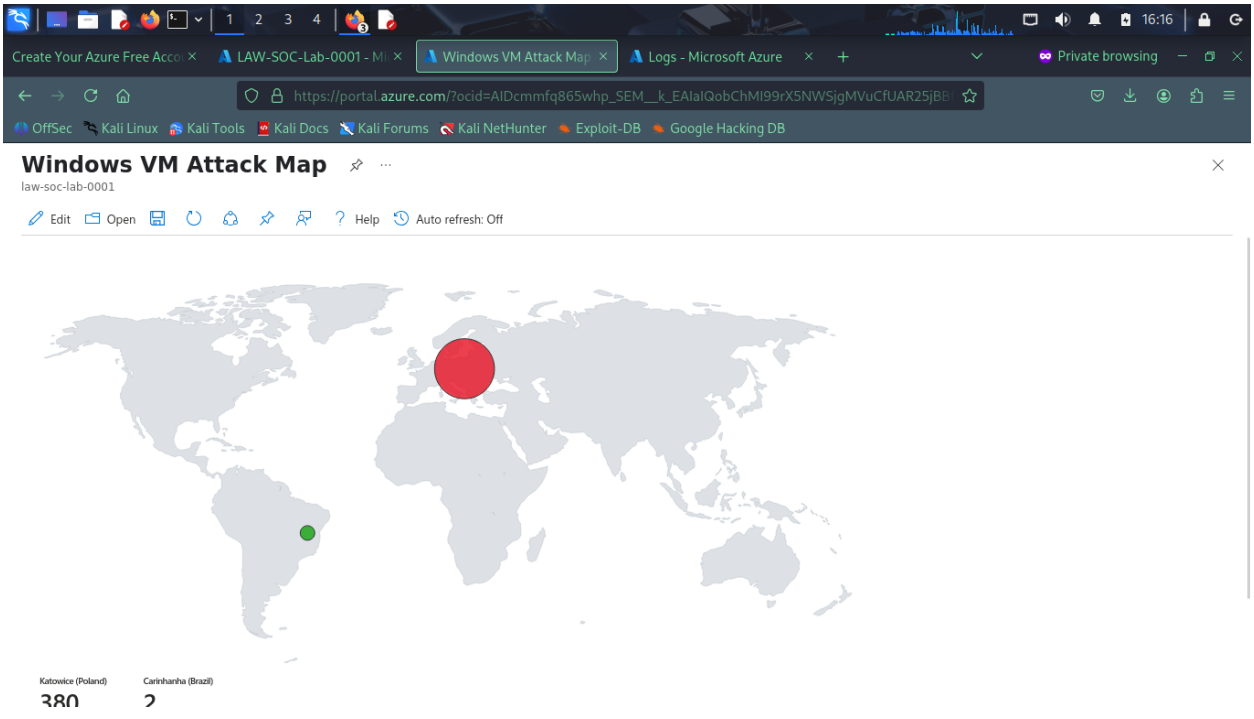

Create Your Azure Free A
LAW-SOC-Lab-0001
New workbook - Micr
Logs - Microsoft Azur
Cyber Home Lab from
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBB
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home
Microsoft Sentinel | Workbooks
New workbook
law-soc-lab-0001
Edit
Open
Help
Auto refresh: Off
New workbook
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
105
Heartbeat
84
Usage
2

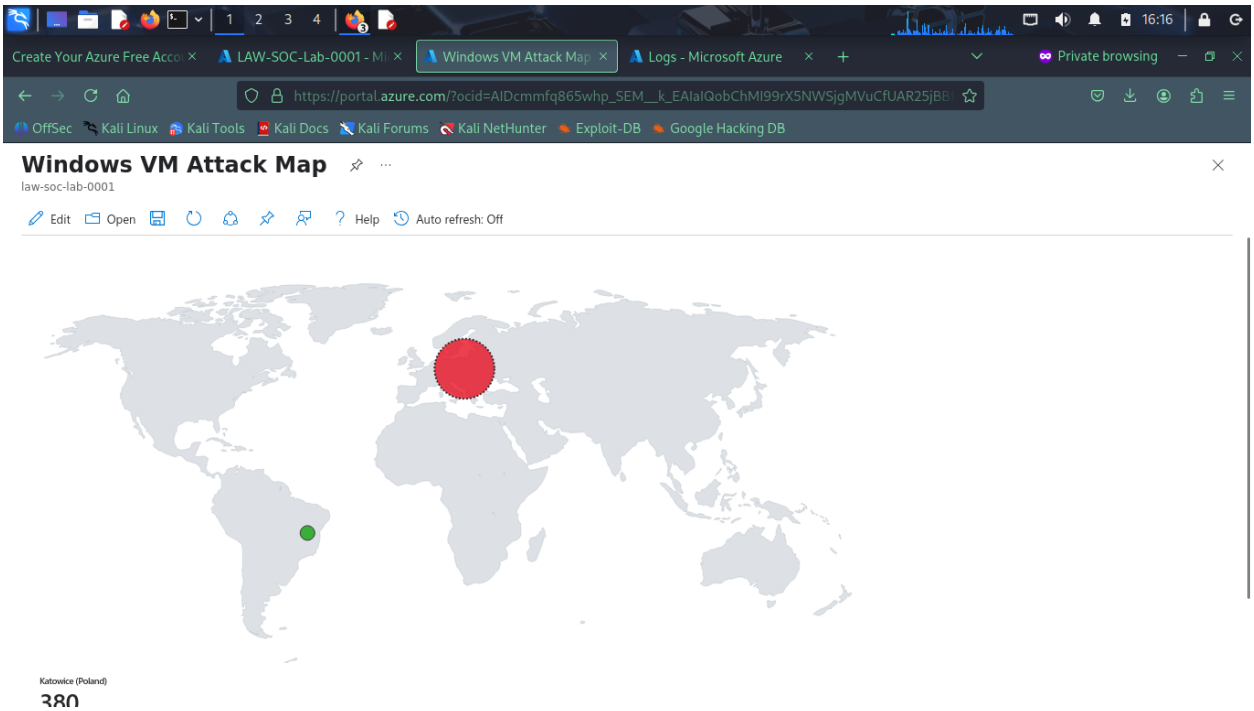

Create Your Azu
LAW-SOC-La
New workbo
Logs - Micro
Cyber Home
Lab Checklist
map.json - G
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBB
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home
Microsoft Sentinel | Workbooks
New workbook
law-soc-lab-0001
Done Editing
Open
Help
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

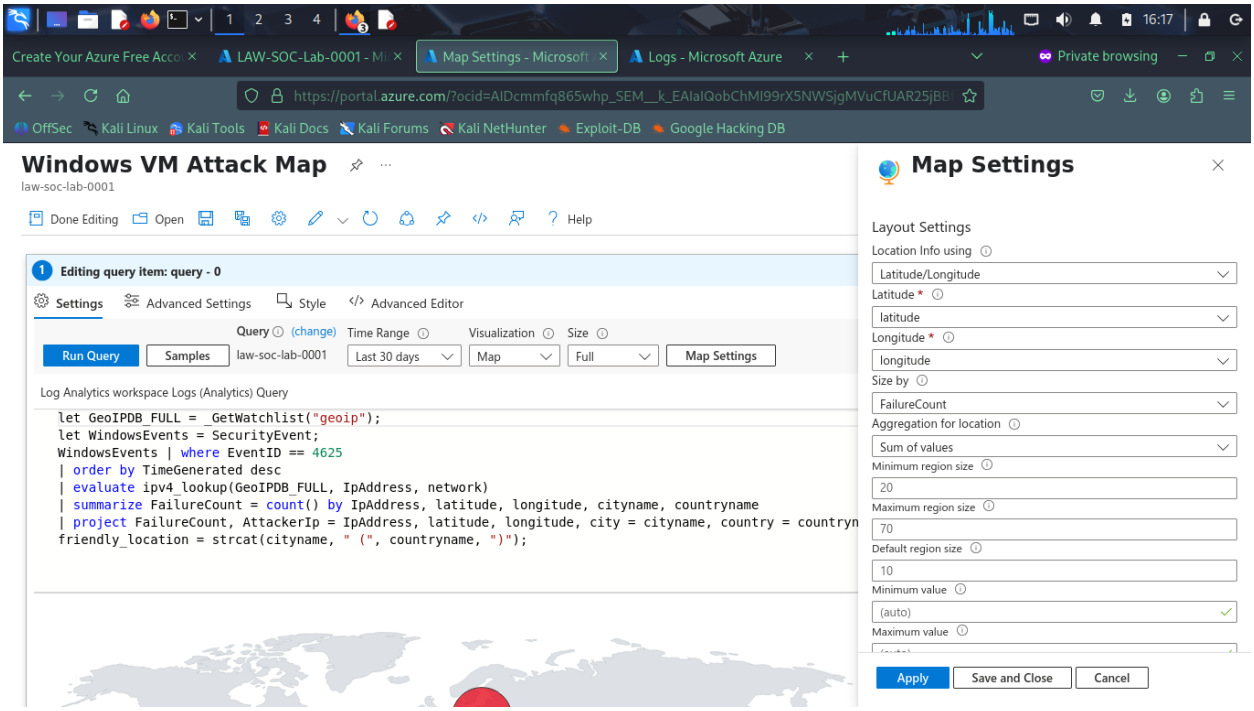

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
Home > Microsoft Sentinel | Workbooks >
New workbook
law-soc-lab-0001
Done Editing
Open
Help
Editing query item: query - 0
Settings
Advanced Settings
Style
Advanced Editor
Shown below is a JSON representation of the current item.
Any changes you make here will be reflected when you press 'Done Editing'.
{
"type": 3,
"content": {
"version": "KqlItem/1.0",
"query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n| order by T
"size": 3,
"timeContext": {
"durationMs": 2592000000
},
"queryType": 0,
"resourceType": "microsoft.operationalinsights/workspaces",
"visualization": "map",
"mapSettings": {


New workbook - Microsoft Azure
Logs - Microsoft Azure
Private browsing
New workbook
law-soc-lab-0001
Done Editing
Open
Help
Katowice (Poland)
380
Carinhanha (Brazil)
2


Create Your Azure Free Acco
LAW-SOC-Lab-0001 - Mi
New workbook - Microso
Logs - Microsoft Azure
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBB
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Screenshot taken
View image
New workbook
law-soc-lab-0001
Done Editing
Open
Help
Katowice (Poland)
380
Carinhanha (Brazil)
2


Create Your Azure Free Acco
LAW-SOC-Lab-0001 - Mi
Windows VM Attack Map
Logs - Microsoft Azure
Private browsing
https://portal.azure.com/?ocid=AIDcmmfq865whp_SEM__k_EAIaIQobChMI99rX5NWSjgMVuCfUAR25jBB
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Windows VM Attack Map
law-soc-lab-0001
Edit
Open
Help
Auto refresh: Off
Katowice (Poland)
380
Carinhanha (Brazil)
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.