

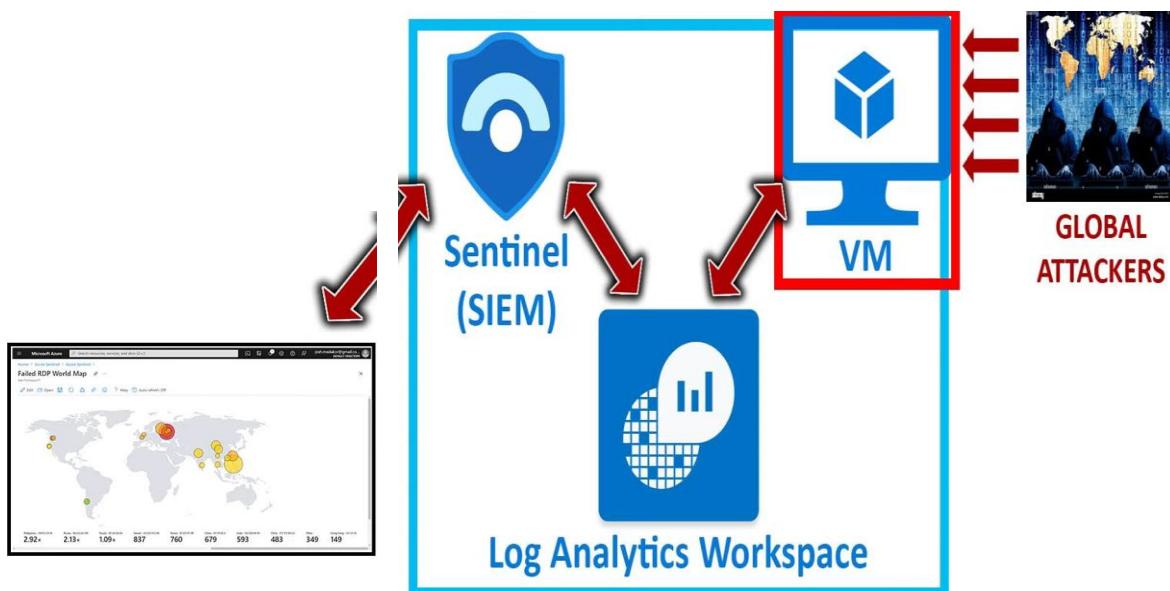
Azure Sentinel (Microsoft's Cloud SIEM)

Developed Content for, as well as performing the following tasks for Azure Sentinel (SIEM):

- Used custom PowerShell Script to extract metadata from Windows Event Viewer to be forwarded to third-party API to derive geolocation data
- Configured "Log Analytics Workspace" in Azure to ingest custom logs containing geographic information (latitude, longitude, state/province, and country)
- Configured custom fields in Log Analytics Workspace with the intent of mapping geo data in Azure Sentinel
- Configured Azure Sentinel (Microsoft's Cloud SIEM) workbook to display global attack data (RDP brute force) on the world map according to a physical location and magnitude of attacks.

You will see above all steps under stepwise everything with screenshots.

Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.



Brief: first, I will create virtual machine windows 10 through azure VM and turn off all firewalls, exposing it to the internet and making it vulnerable. Using log analytics workspace to ingest custom logs containing geographic information custom fields in Log Analytics Workspace with the intent of mapping geo data in Azure Sentinel.

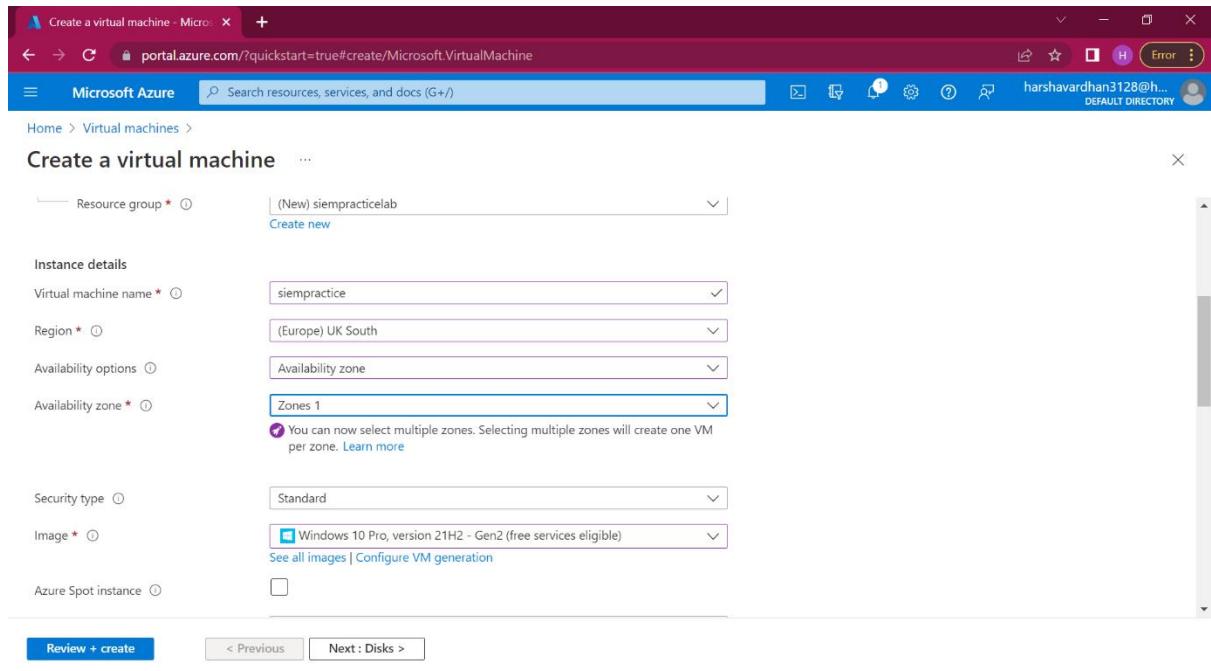


Fig1. Here I am creating a virtual Windows 10 through azure VMware.

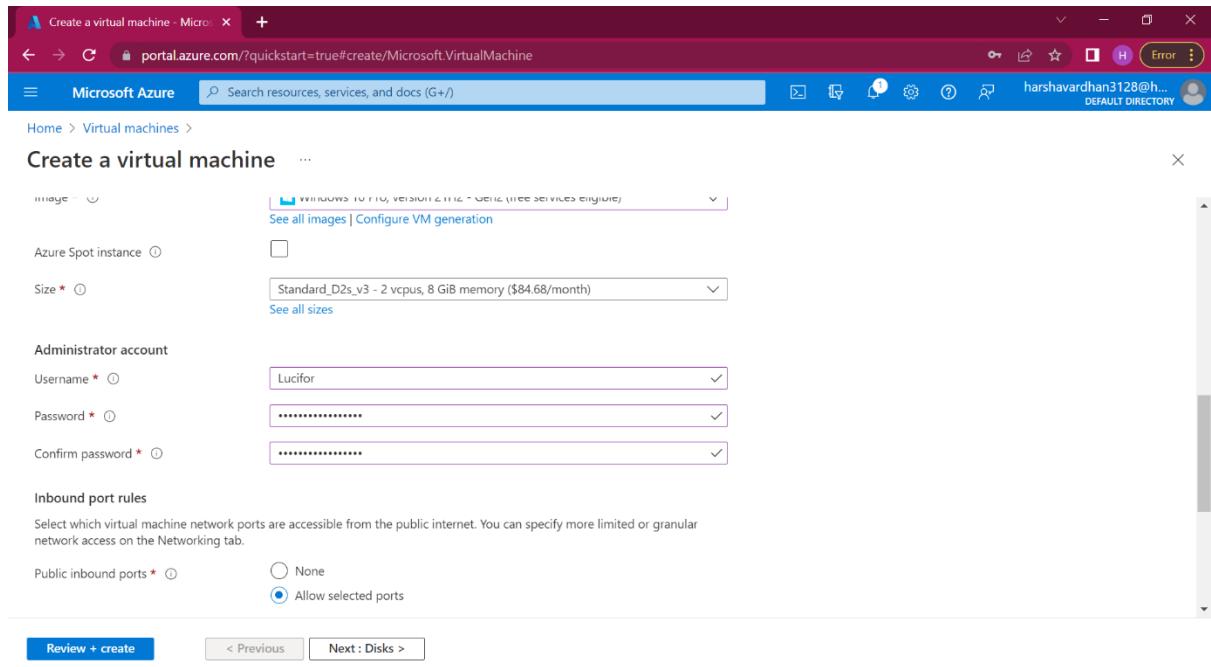


Fig2. Providing Windows credentials

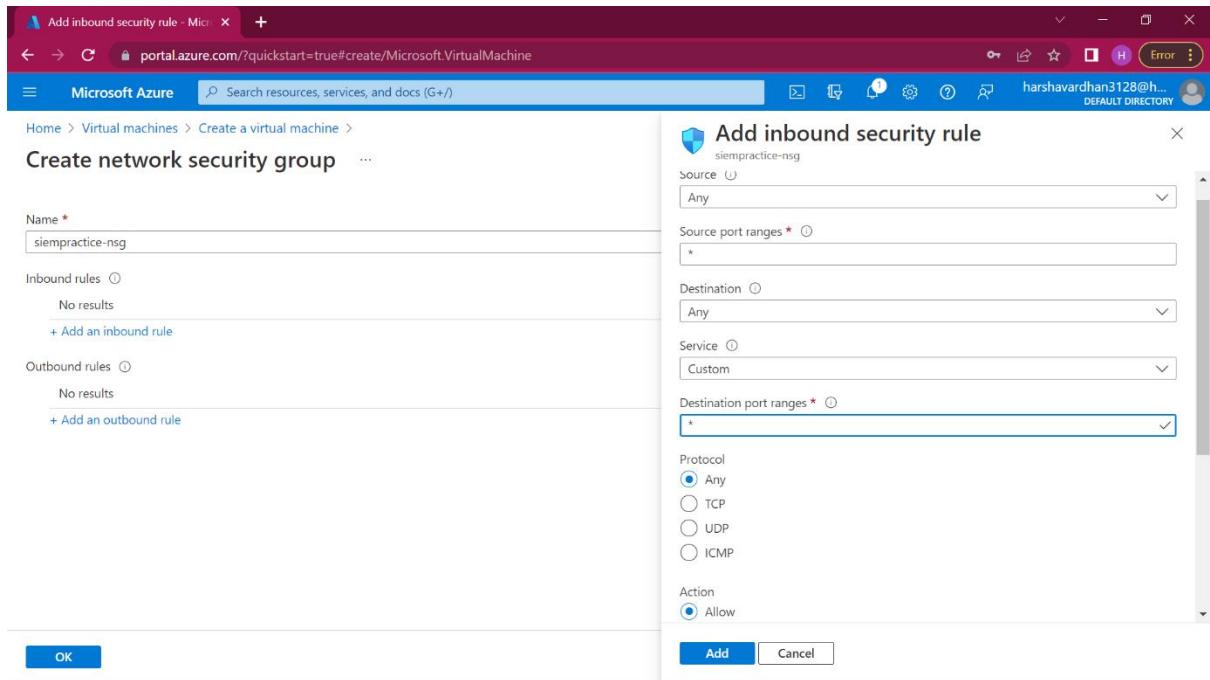


Fig3. Providing disk ranges and making port code ranges to all.

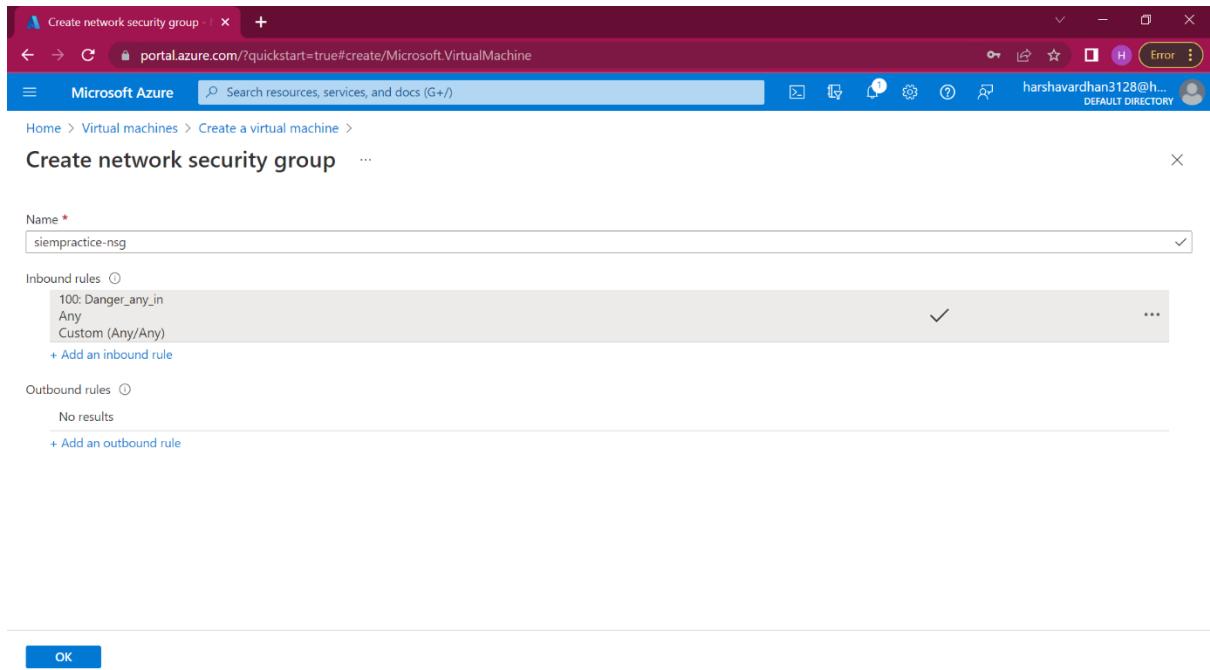


Fig4.Deleting the default security group and creating a new one

The screenshot shows the Azure portal interface for creating a virtual machine. The title bar says 'Create a virtual machine - Microsoft Azure'. The URL is 'portal.azure.com/?quickstart=true#create/Microsoft.VirtualMachine'. The top navigation bar includes 'Microsoft Azure', a search bar, and user information 'harshavardhan3128@h... DEFAULT DIRECTORY'. Below the navigation is a breadcrumb trail 'Home > Virtual machines > Create a virtual machine'. A green validation message 'Validation passed' is displayed. The main content area has tabs: Basics, Disks, Networking, Management, Advanced, Tags, and Review + create (which is selected). A note says 'Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.' Under 'PRODUCT DETAILS', it shows '1 X Standard D2s v3 by Microsoft' and a price of '0.1160 USD/hr'. There are links for 'Subscription credits apply', 'Terms of use | Privacy policy', and 'Pricing for other VM sizes'. The 'TERMS' section contains legal text about agreeing to terms and conditions. At the bottom are buttons for 'Create', '< Previous' (disabled), 'Next >', and 'Download a template for automation'.

Fig 5. reviewing it and creating a virtual machine.

The screenshot shows the Azure portal interface for a deployment named 'CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20220613095452'. The title bar says 'CreateVm - MicrosoftWindowsDesktop.Windows-10-win10-20220613095452 | Overview'. The URL is 'portal.azure.com/?quickstart=true#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F1fb0dfea-3a6a-4c13-82...'. The top navigation bar includes 'Microsoft Azure', a search bar, and user information 'harshavardhan3128@h... DEFAULT DIRECTORY'. A modal window titled 'Deployment in progress...' shows the message 'Deployment to resource group 'siempрактиклаб' is in progress.' On the left, there's a sidebar with 'Overview', 'Inputs', 'Outputs', and 'Template' options. The main content area shows deployment details: 'Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows...', 'Subscription: Azure subscription 1', 'Resource group: siempрактиклаб', 'Start time: 6/13/2022, 10:06:26 AM', and 'Correlation ID: fc312fd8-3aa5-46d2-876a-107eaa8113f8'. Below this, a table titled 'Deployment details' is shown with columns: Resource, Type, Status, and Operation details. The table body says 'No results.'

Fig 6. While deployment is in progress, I am creating a log analytical workspace.

The screenshot shows the 'Create Log Analytics workspace' page in the Microsoft Azure portal. At the top, there's a green validation message: 'Validation passed'. Below it, the 'Log Analytics workspace' card by Microsoft is displayed. The 'Basics' section shows the following details:

Subscription	Azure subscription 1
Resource group	siempрактиклаб
Name	siempрактиче
Region	UK South

The 'Pricing' section indicates a 'Pay-as-you-go (Per GB 2018)' tier. A note states: '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.' Below this, there's a 'Tags' section and a navigation bar with 'Create', '< Previous', and 'Download a template for automation' buttons.

Fig7.creating it.

The screenshot shows the 'All services' page in the Microsoft Azure portal. The search bar at the top has 'security center' typed into it. The results list includes:

- Microsoft Defender for Cloud (Keywords: security center)
- Backup center
- Security Baselines
- VMware vCenters (Keywords: vCenter)
- Application security groups (Keywords: Network security Resource type: Microsoft.Network/applicationSe...)
- Extended Security Updates (Keywords: security)
- Network security groups (Keywords: security Keywords: Security Resource type: Microsoft.Network/Net...)
- Azure Edge Hardware Center

On the right side, there's a detailed view of the 'Microsoft Defender for Cloud' service, showing a star icon, a 'View' button, and a 'PREVIEW' button. It also includes sections for 'Free training from Microsoft', 'Top 5 security items to consider before pushin...', and 'Identity Security'. Below this, there's a 'Useful links' section with links to 'Overview', 'Get started', 'Documentation', and 'Pricing'.

Fig8.going security centre.

The screenshot shows the Microsoft Defender for Cloud Environment settings page. The left sidebar includes links for Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems, Cloud Security (Security posture, Regulatory compliance, Workload protections, Firewall Manager), and Management (Environment settings, Security solutions, Workflow automation). The main area displays a multi-cloud account management interface with sections for Azure subscriptions (1), AWS accounts (0), and GCP projects (0). A welcome message states: "Welcome to the new multi-cloud account management page (preview). To switch back to the classic cloud connectors experience, click here." Below this are search and filter options (Search by name, Environments = All, Standards = All, Coverage = All) and a table header for Name, Total resources, Defender coverage, and Standards. The table lists one Azure subscription.

Fig9.under environment settings

The screenshot shows the Microsoft Defender plans settings page. The left sidebar has links for Settings (Defender plans, Data collection) and Save. The main area displays a summary: "Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace". It includes a section titled "Select Defender plan by resource type" with an "Enable all" button. Below is a table showing three resource types: Security posture management (Free, On/Off), Servers (\$15/Server/Month, On/Off), and SQL servers on machines (\$15/Server/Month \$0.015/Core/Hour, On/Off).

Microsoft Defender for	Resource quantity	Pricing	Plan
Security posture management		Free	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Servers	0 servers	\$15/Server/Month	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
SQL servers on machines	0 servers	\$15/Server/Month \$0.015/Core/Hour	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off

Fig10.under defender plans, turn on the security posture management and servers.

The screenshot shows the Microsoft Azure portal interface for 'Settings | Defender plans'. At the top, it says 'Microsoft Defender plans will apply to: 0 Azure and 0 non-Azure resources reporting to this workspace'. Below this, there's a table titled 'Select Defender plan by resource type' with three rows:

Microsoft Defender for	Resource quantity	Pricing	Plan
Security posture management	0 servers	Free	<input checked="" type="button"/> On <input type="button"/> Off
Servers	0 servers	\$15/Server/Month	<input checked="" type="button"/> On <input type="button"/> Off
SQL servers on machines	0 servers	\$15/Server/Month \$0.015/Core/Hour	<input type="button"/> On <input checked="" type="button"/> Off

Fig11.turned on.

The screenshot shows the Microsoft Azure portal interface for 'Settings | Data collection'. It displays the 'Store additional raw data - Windows security events' section. A note states: 'To help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.' Below this, it says 'Select the level of data to store for this workspace. Charges will apply for all settings other than "None".' There are four radio button options:

- All Events: 'All Windows security and AppLocker events.'
- Common: 'A standard set of events for auditing purposes.'
- Minimal: 'A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.'
- None: 'No security or AppLocker events.'

Fig 12. under data collection, select all events. Here we want to collect all the data.

Microsoft Sentinel

No Microsoft Sentinel to display

Create Microsoft Sentinel

Learn more ↗

Give feedback ↗

Fig 13. Now going to Microsoft sentinel

Add Microsoft Sentinel to a workspace

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
siempactice	uksouth	siempactice	Azure subscription 1	Default Directory

Add Cancel

Fig14.created a Microsoft sentinel with the name of SiemPractice.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar for 'Virtual machines' with a search bar and a list of resources. In the center, a detailed view of a virtual machine named 'siempракти' is displayed. The 'Essentials' section includes fields for Resource group, Status, Location, Subscription, Subscription ID, Availability zone, and Tags. A 'Public IP address' field shows '20.77.34.82'. On the right, there are tabs for Properties, Monitoring, Capabilities (7), Recommendations, and Tutorials. At the bottom, there's a feedback link.

Fig 15. now coming back to my virtual machine and copying the ipv4 address.

The screenshot shows the Microsoft Azure portal with a 'Remote Desktop Connection' dialog box overlaid. The dialog box has 'Computer' set to '20.77.34.82'. Below it, there are fields for 'User name' and 'Password', and a checkbox for 'Remember me'. At the bottom are 'OK' and 'Cancel' buttons. To the right of the dialog, the virtual machine's properties are shown again, including the public IP address '20.77.34.82'.

Fig16.now accessing my virtual machine with ipv4 address through remote desktop connection and logging in with credentials.

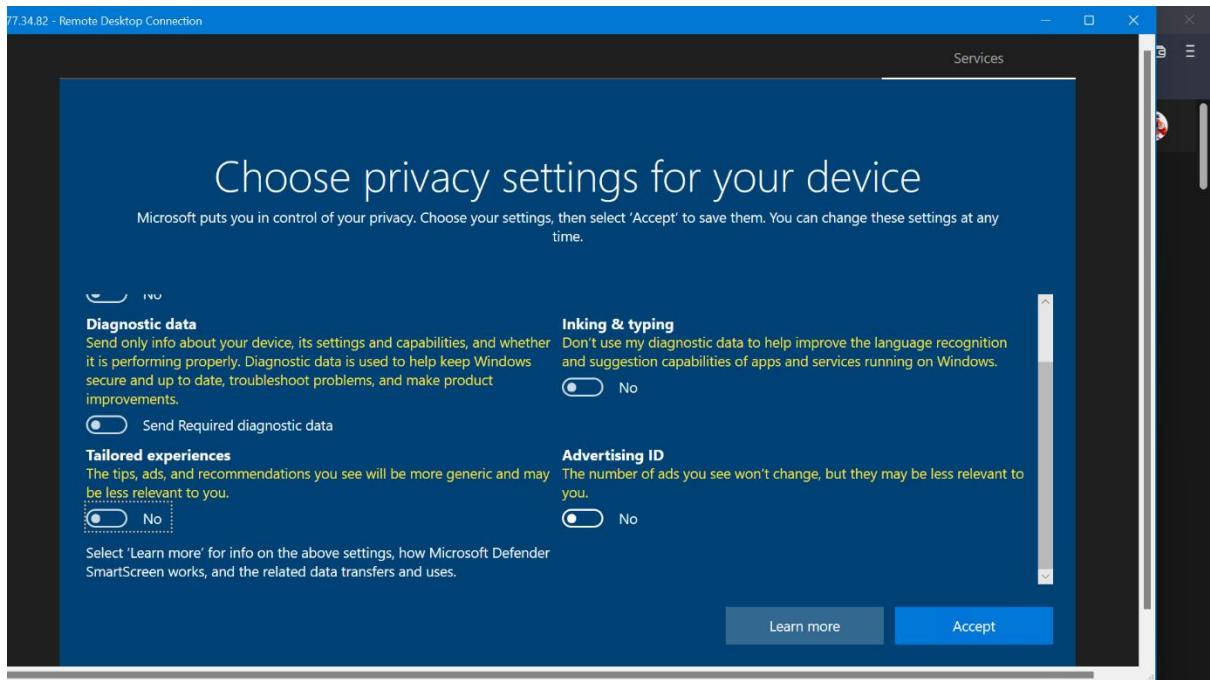


Fig 17. turning off all the settings.

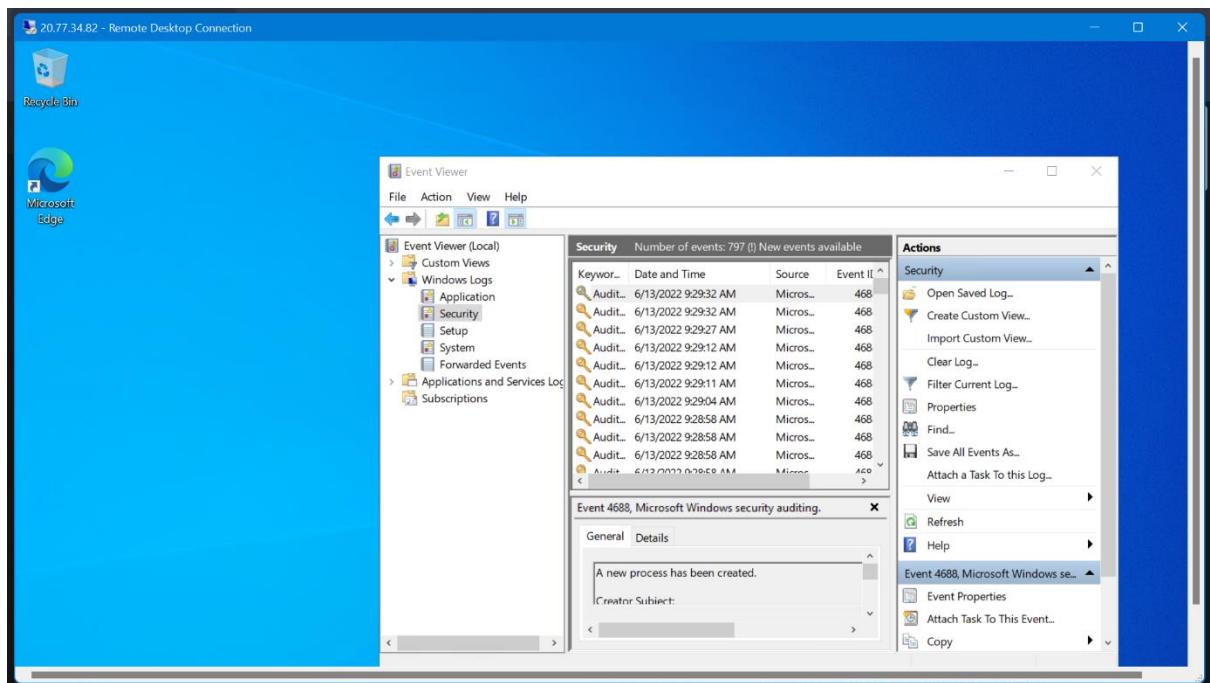


Fig 18. After accessing the virtual machine and opening the event viewer and under security, this will capture all the events when logging in and the geo-location through longitude and latitudes. I want to retrieve this data and send it to the log analytical workspace in azure.

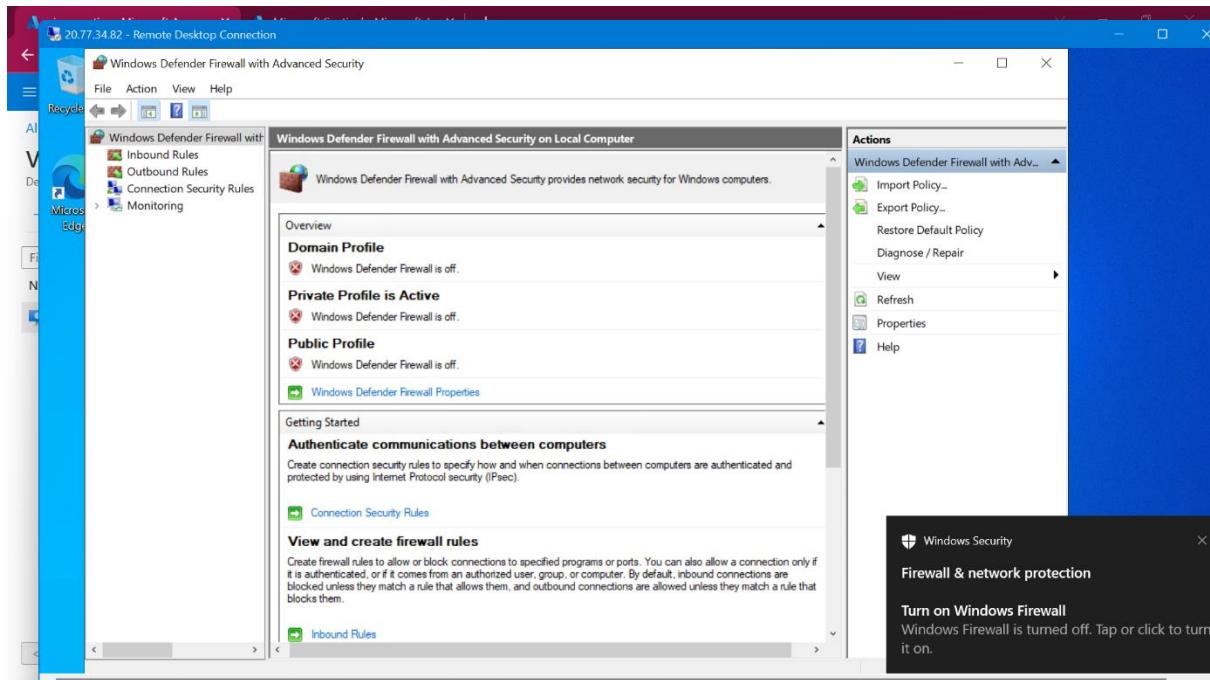


Fig19.turning off all windows firewalls to make it vulnerable and exposing this to attackers.

A screenshot of the ipgeolocation.io API dashboard. The left sidebar has links for Dashboard, Billing, Documentation, Profile, and Logout. The main dashboard shows 'Developer | API Subscription' and 'API Keys' with a button to 'Add'. On the right, there's an 'API Usage' section with a table showing consumption statistics. A message at the bottom left says 'API key has been copied to the clipboard.' and an 'OK' button. A 'Notification Preference' button is in the bottom right corner.

Fig 20. here I am using the IP geolocation website for the API key.

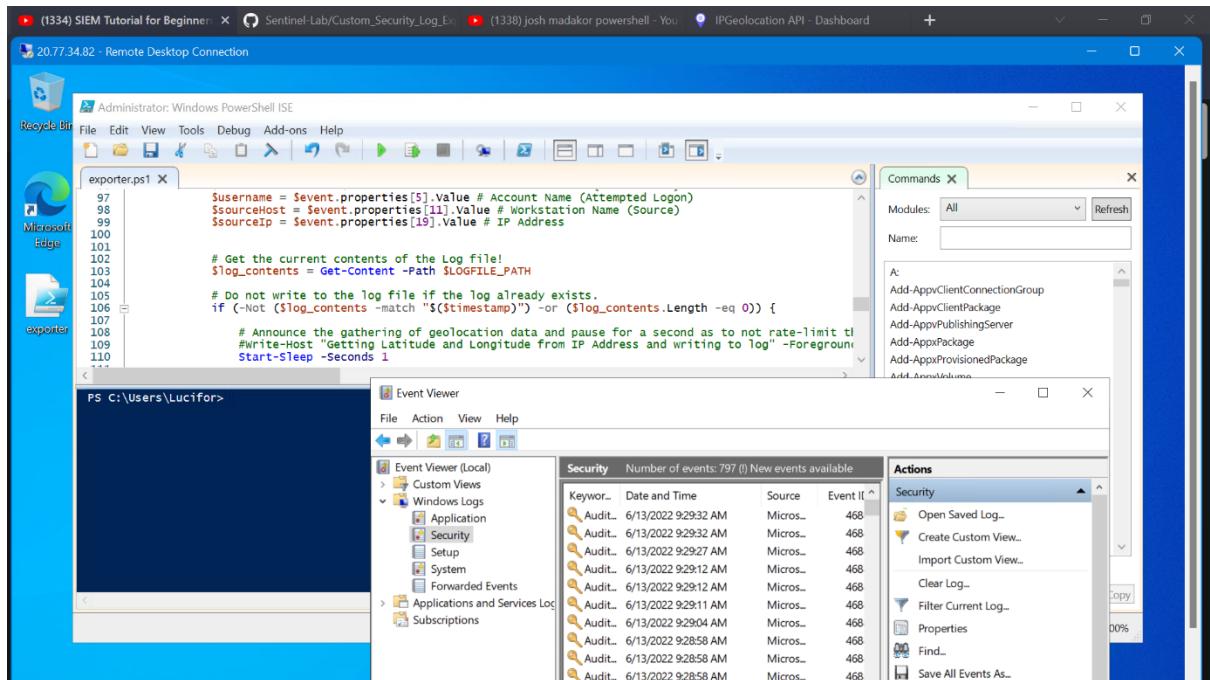


Fig 21. here I am using a custom PowerShell Script to extract metadata from Windows Event Viewer to be forwarded to a third-party API (IP geolocation website) to derive geolocation data.

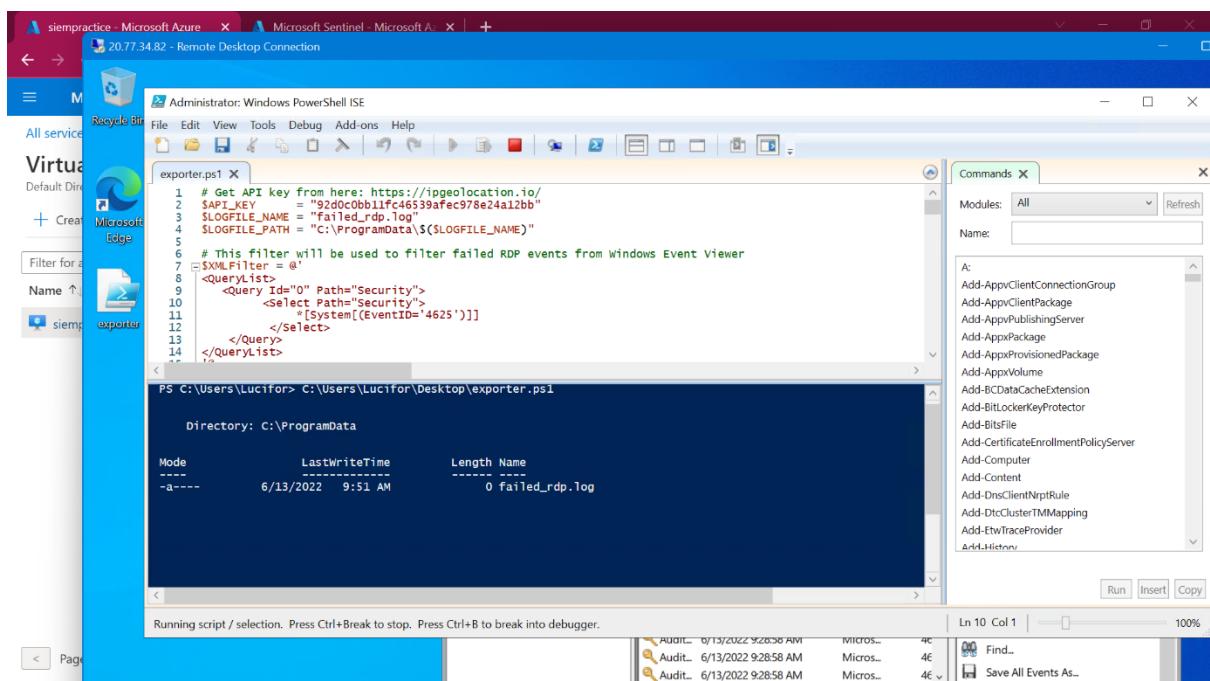


Fig 22. Running that PowerShell script.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar has two tabs: 'siempactice - Microsoft Azure' and 'Microsoft Sentinel - Microsoft Azure'. The main address bar shows the URL 'portal.azure.com/?quickstart=true#@harshvardhan3128hotmail.onmicrosoft.com/resource/subscriptions/1fb0dfea-3a6a-4c13-8261-63c9802a2f44/resourceGroups/siempрактиclab/providers/Microsoft.OperationalInsights/workspaces/siempactice'. The user 'harshvardhan3128@...' is logged in.

The left sidebar shows 'All services > Log Analytics workspaces > siempactice'. The main content area is titled 'Log Analytics workspace' and displays the 'Overview' section for the 'siempactice' workspace. The 'Essentials' panel on the right lists the following details:

Workspace Name	siempactice
Workspace ID	37339db5-4056-4a80-ba6a-e06b3186425f
Pricing tier	Pay-as-you-go
Access control mode	Use resource or workspace permissions
Operational issues	✓ OK

Below the essentials panel, there's a 'Get started with Log Analytics' section and two buttons: 'Connect a data source' and 'Configure monitoring solutions'.

Fig 23. Open log analytics workspace activity log under custom logs.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar has two tabs: 'Create a custom log - Microsoft' and 'Microsoft Sentinel - Microsoft Azure'. The main address bar shows the URL 'portal.azure.com/?quickstart=true#/view/Microsoft_OperationsManagementSuite_Workspace/CreateCustomLogBlade/workspaceId/%2bsubscr...'. The user 'harshvardhan3128@...' is logged in.

The left sidebar shows 'All services > Log Analytics workspaces > siempactice'. The main content area is titled 'Create a custom log' and is on the first step of a wizard: 'Sample'. The steps are numbered 1 through 5: 1. Sample, 2. Record delimiter, 3. Collection paths, 4. Details, 5. Review + Create.

The 'Sample' step instructions say 'Upload a sample of the custom log. The wizard will parse and display the entries in this file.' There is a 'Learn more' link. A 'Select a sample log' input field is present, with a note 'Select a sample log *' and a 'Select a file' button.

At the bottom, there are 'Previous' and 'Next' buttons.

Fig 24. create a custom file. Enter a sample log.

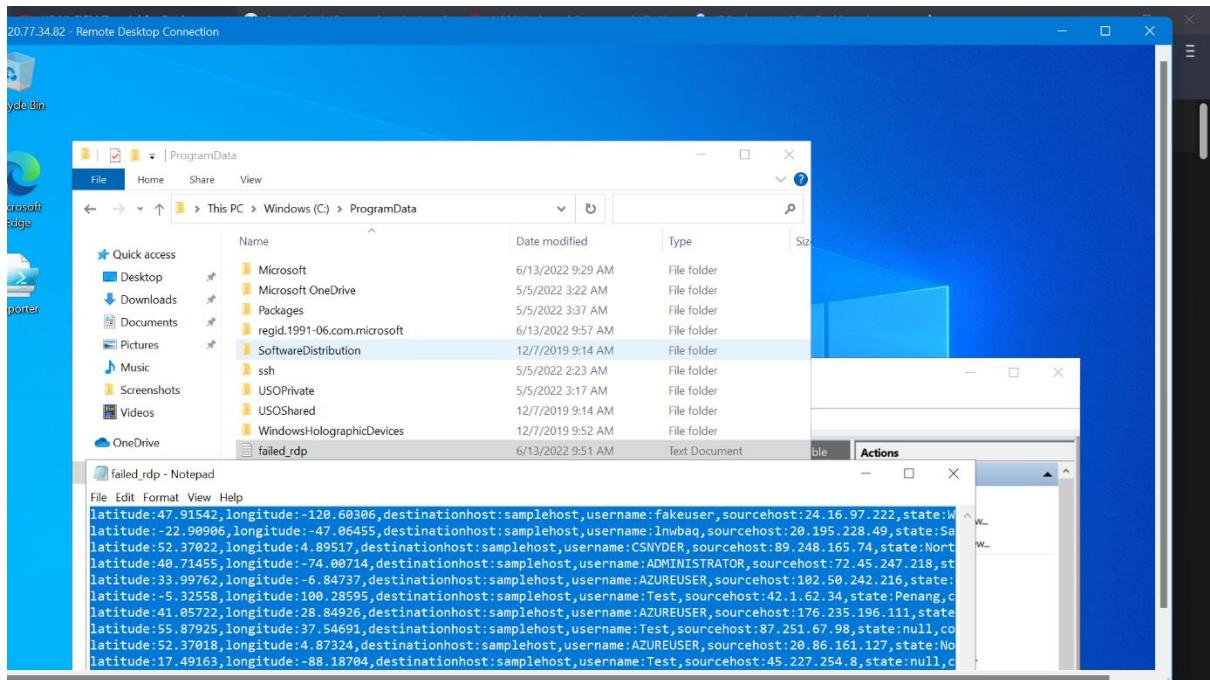


Fig 25. sample file you can find in the failed_rdp file in a virtual machine.

Collection paths

Type	Path
Windows	C:\ProgramData\failed_rdp.log
Select type	

[« Previous](#) [Next »](#)

Fig 26. enter path.

Create a custom log

Review + Create

Sample
Sample log failed_rdp.log

Record delimiter
Record delimiter New line

Collection paths
Windows C:\ProgramData\failed_rdp.log

Details
Custom log name failedrpg_CL
Description

« Previous Create

Fig 27. review and create.

siempactice | Logs

Results

TimeGenerated [UTC]	Computer	RawData	Type	Resource
6/13/2022, 10:22:56.000 AM	siempactice	latitude:33.99762,longitude:-6.8...	failedrpg_CL	/sub
6/13/2022, 10:22:56.000 AM	siempactice	latitude:-5.32558,longitude:10...	failedrpg_CL	/sub

Extract fields from 'failedrpg_CL'

Fig 28. under logs failedrpg_CL open Extract fields from 'failedrpg_CL'

Custom Fields - Microsoft Azure x Microsoft Sentinel - Microsoft A... + v – !

portal.azure.com/?quickstart=true#@harshavardhan3128hotmail.onmicrosoft.com/resource/subscriptions/1fb0dfa-3a6a-4c13-8261-63c9802... o l ☆ D H Error ...

Microsoft Azure Search resources, services, and docs (G+) harshavardhan3128@...
DEFAULT DIRECTORY

All services > Log Analytics workspaces > siempractice >

Custom Fields

siempractice

Refresh Logs

MAIN EXAMPLE | SEARCH RESULTS | SUMMARY

failedrpg_CL

FILTER	FIELD NAME	VALUE
<input type="checkbox"/>	TenantId	: 37339db5-4056-4a80-ba6a-e06b3186425f
<input type="checkbox"/>	SourceSystem	: OpsManager
<input type="checkbox"/>	ManagementGroupName	: AOI-37339db5-4056-4a80-ba6a-e06b3186425f
<input type="checkbox"/>	TimeGenerated	: 2022-06-13T10:22:56Z
<input type="checkbox"/>	Computer	: siempractice
<input type="checkbox"/>	RawData	<p>latitude : <input type="text" value="5.32558"/> Field value : <input type="text" value="latitude_CF"/> username:Testa - 42.1.62.34.</p> <p>tsourcetimest... Field Title : <input type="text" value="latitude_CF"/> Field Type : <input type="button" value="Numeric"/> <input type="button" value="Extract"/></p>

Condition failedrpg_CL | limit 100

Save extraction

Fig 29. Here I am extracting everything by name. (custom fields/extract fields from raw custom log data)

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The top navigation bar includes 'Custom Fields - Microsoft Azure' and 'Microsoft Sentinel - Microsoft A...' tabs, along with a search bar and various icons. The main content area displays a 'Custom Fields' section with a 'MAIN EXAMPLE' table and a 'SEARCH RESULTS' table.

MAIN EXAMPLE

SourceSystem	:	OpsManager
ManagementGroupName	:	AOI-37339db5-4056-4a80-ba6a-e06b3186425f
TimeGenerated	:	2022-06-13T10:22:56Z
Computer	:	siempракти
RawData	:	latitude: -5.32558,longitude:100.28595,destinationhost:samplehost,username: Test,sourcehost:42.1.6.234,state:Penang,country:Malaysia,label:Malaysia - 42.1.6.234,timestamp:2021-10-26 11:04:45

SEARCH RESULTS

120.60306	latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:amefakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24.16.97.222,timestamp:2021-10-26 03:28:29
82.80906	latitude: 82.80906,longitude: -47.06455,destinationhost:samplehost,username:ameInwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:20
89.248.165.74	latitude:52.3.7022,longitude:4.89517,destinationhost:samplehost,username:cNSYD,sourcehost:89.248.165.74.state:North Holland,country:Netherlands,label:Netherlands - 89.248.165.74,timestamp:2021-10-26 06:12:56
74.00714	latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,timestamp:2021-10-26 10:47
6.84737	latitude:6.84737,longitude:-75.00000,destinationhost:samplehost,username:harshavardhan3128@hotmail.onmicrosoft.com,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,timestamp:2021-10-26 10:47

SUMMARY

Condition: faileddrp_CL | limit 100

latitude_CF (12 values)

120.60306 (1 matched)
82.80906 (1 matched)
89.248.165.74 (1 matched)
74.00714 (1 matched)
6.84737 (1 matched)
1.32994 (1 matched)
76.235.196.111 (1 matched)
72.45.247.218 (1 matched)
20.195.228.49 (1 matched)
89.248.165.74 (1 matched)
53.86602 (1 matched)
6.16247 (1 matched)

New - Highlight text to mark a custom field. Click on existing highlights to remove.

Latitude: 47.91542
State: 2.5444444444444445

Field value:
Field Title:
Field Type:
Numeric

Close Extract

Save extraction Cancel

Fig 30. Checking and correcting the data and extracting

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The URL in the browser is <https://portal.azure.com/?quickstart=true#/harshavardhan3128hotmail.onmicrosoft.com/resource/subscriptions/1fb0dfea-3a6a-4c13-8261-63c9802...>. The page title is "siemppractice | Custom logs". A search bar at the top left contains "cus". Below it, a table lists 9 results under the heading "Showing 9 results". The columns are "Custom field name", "Table name", and "Field type". The data includes fields like "country_CF", "destinationhost_CF", "label_CF", etc., all mapped to the "failedrpg_CL" table and various field types (Text, Numeric, DateTime).

Fig 31. Like this, extracting everything by names.

The screenshot shows the Microsoft Azure New workbook interface. The URL in the browser is <https://portal.azure.com>. The page title is "New workbook". A query editor window is open with the following details:

- Editing query item: query - 0**
- Run Query** button is highlighted.
- Advanced Settings** and **Style** tabs are visible.
- Data source**: Logs
- Resource type**: Log Analytics
- Log Analytics workspace**: siemppractice
- Time Range**: Last 24 hours
- Visualization** dropdown is open, showing options: Bar chart, Bar chart (Categorical), Bar chart (Unstacked), Line chart, Pie chart, Scatter chart, Time chart, Tiles, Graph, Map (selected), Medium.
- Query text:**

```
failedrpg_CL | summarize event_count=count() by sourcehost_CF, latitude_CF, longitude_CF, country_CF
| where destinationhost_CF != "samplehost"
| where sourcehost_CF != ""
```
- Message at bottom:** "The query returned no results."

Fig 32. Hereafter that is coming back to azure sentinel and under the workbook and writing a query to Setup map in sentinel with Latitude and Longitude (or country)

```

# Get API key from here: https://ipgeolocation.io/
$APIT_KEY = "92dc0bb1fc46539afec978e24a12bb"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$LOGFILE_NAME"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @"
<QueryList>
    <Query Id="0" Path="Security">
        <Select Path="Security">
            *[System[EventID='4625']]
        </Select>
    </Query>
</QueryList>

```

Mode	LastWriteTime	Length	Name
-a---	6/13/2022 9:51 AM	0	failed_rdp.log
			latitude:-6.18247,longitude:106.82681,destinationhost:siemplice,username:AZUREUSER,sourcehost:36.91.242.152,state:ABODETABEK,label:Indonesia - 36.91.242.152,timestamp:2022-06-13 10:13:46
			latitude:-37.81739,longitude:144.96751,destinationhost:siemplice,username:AZUREUSER,sourcehost:20.70.98.240,state:Victoria,label:Australia - 20.70.98.240,timestamp:2022-06-13 11:02:04
			latitude:-37.81739,longitude:144.96751,destinationhost:siemplice,username:STUDENT,sourcehost:20.70.98.240,state:Victoria,label:Australia - 20.70.98.240,timestamp:2022-06-13 11:15:56

Fig 33. here you can see on my virtual machine someone from Australia who tried to log in with details shown on the map through azure sentinel. You can see this in the following figure.

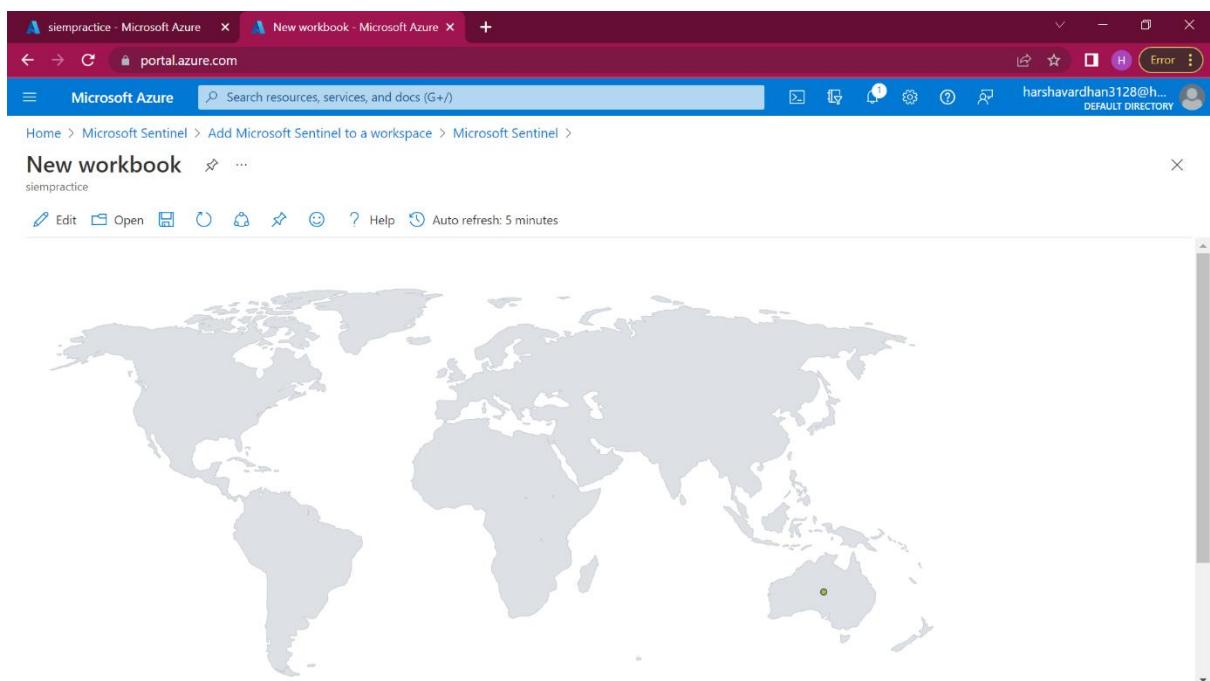


Fig 34. you can see here a green dot from Australia.

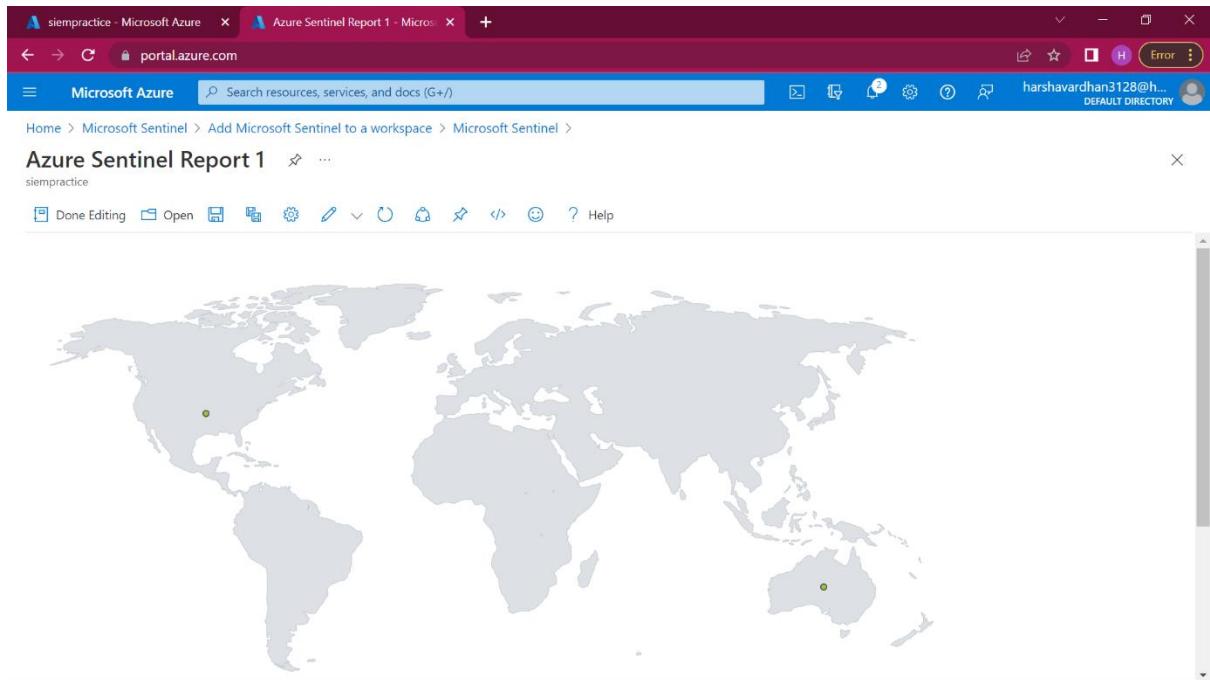


Fig 35. After that, I waited a few hours. One was recorded someone tried to log in with the USA.

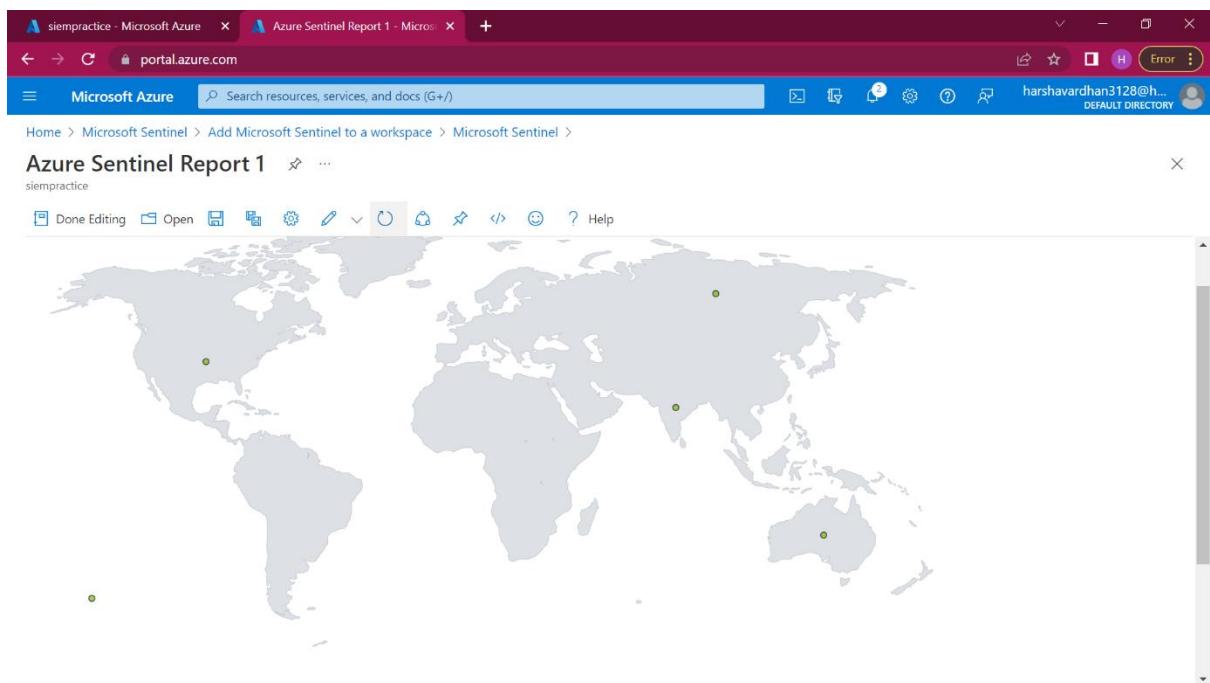


Fig 36. after a few hours, someone from India and Russia tried to log in with my virtual windows.