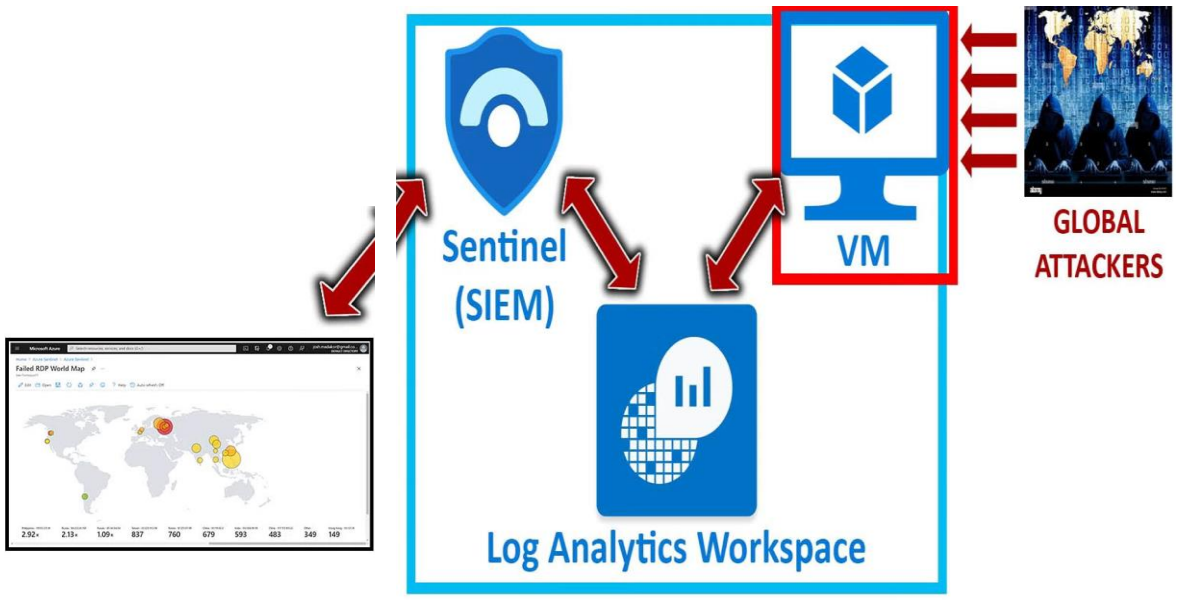
Azure Sentinel (Microsoft's Cloud SIEM)

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.

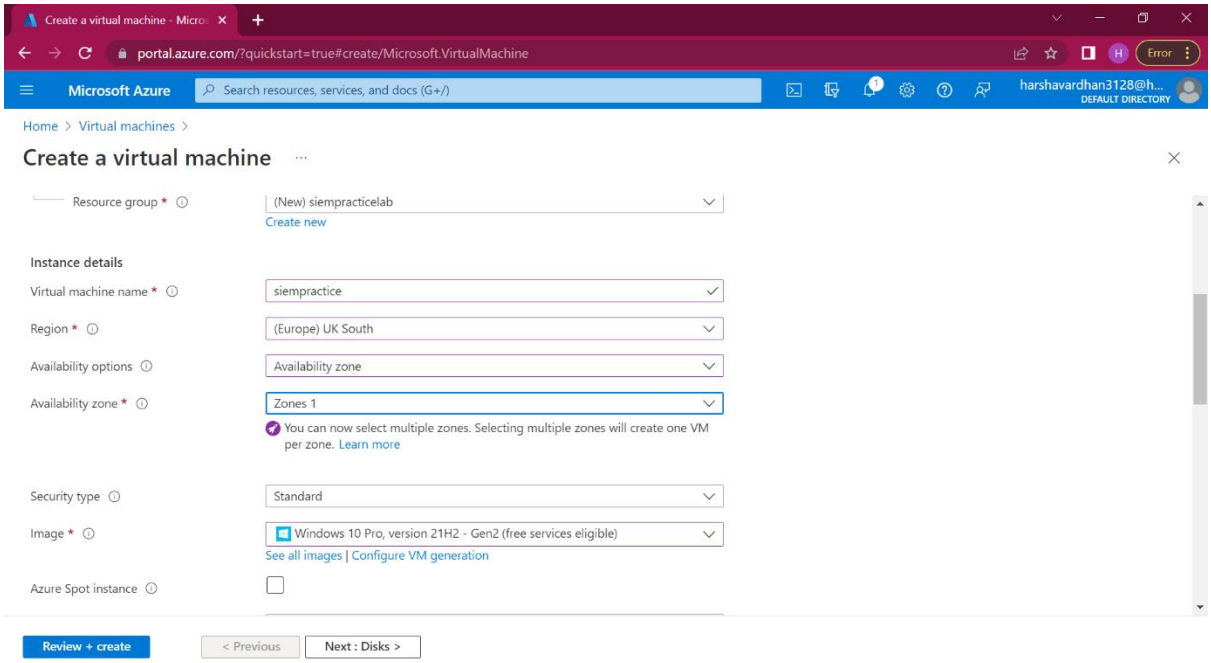


Fig1. Here I am creating a virtual Windows 10 through azure VMware.

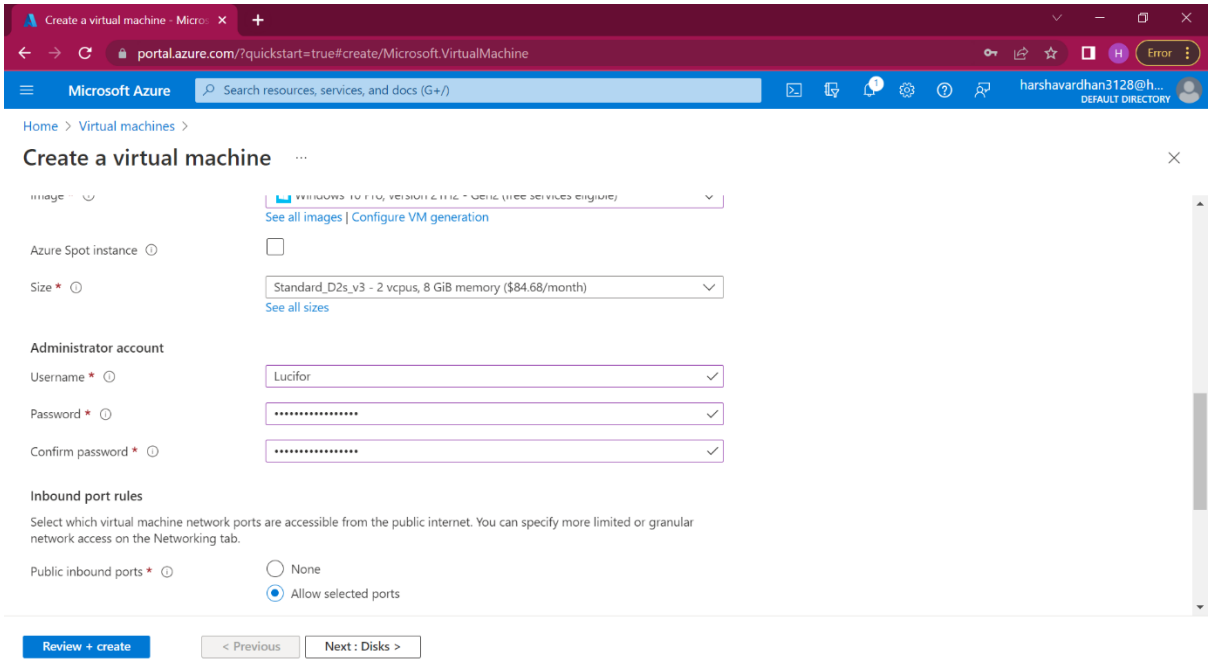


Fig2. Providing Windows credentials

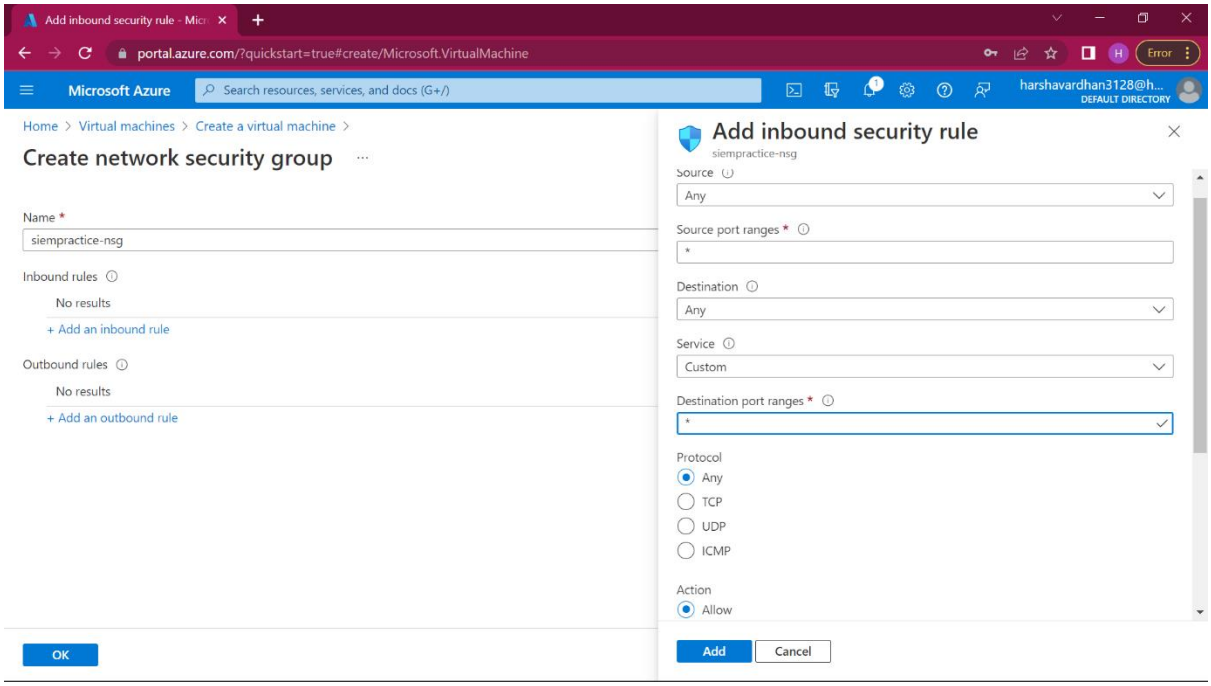


Fig3. Providing disk ranges and making port code ranges to all.

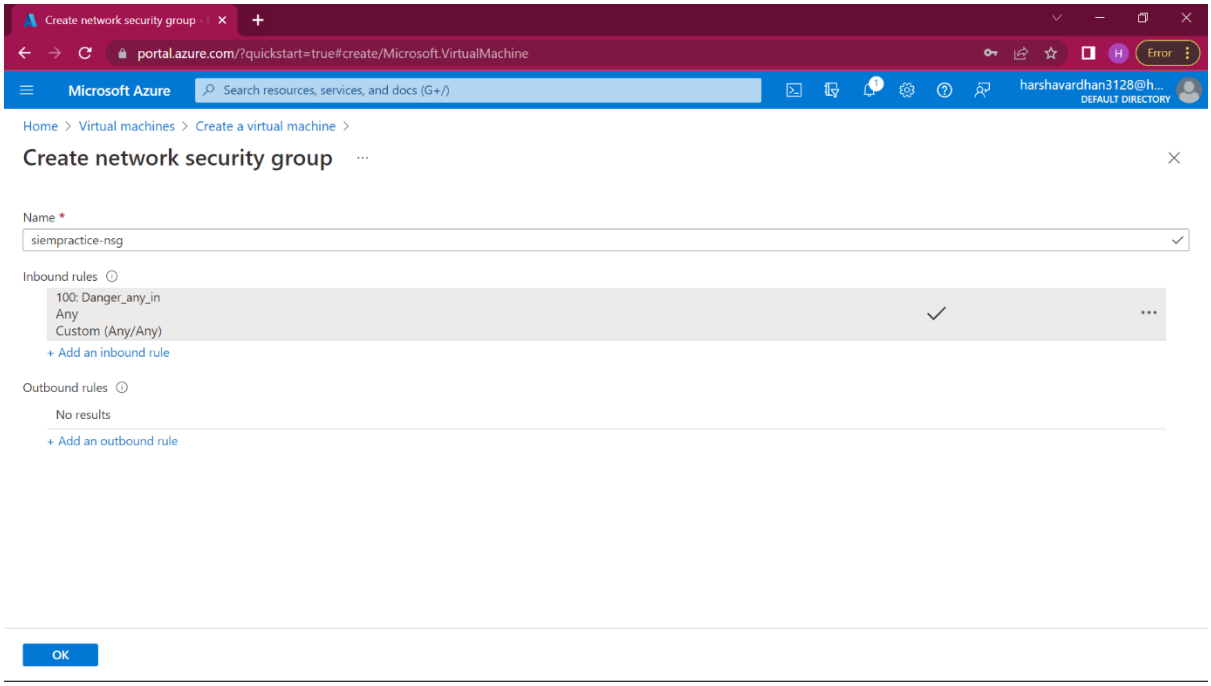


Fig4.Deleting the default security group and creating a new one

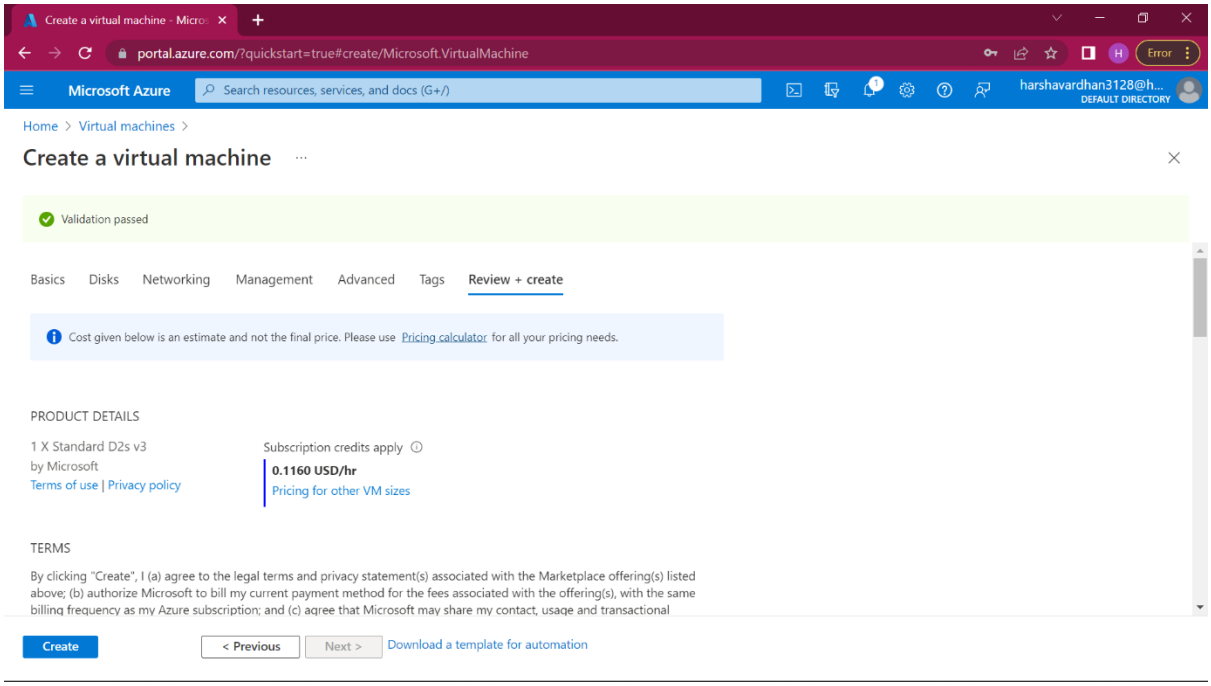


Fig 5. reviewing it and creating a virtual machine.

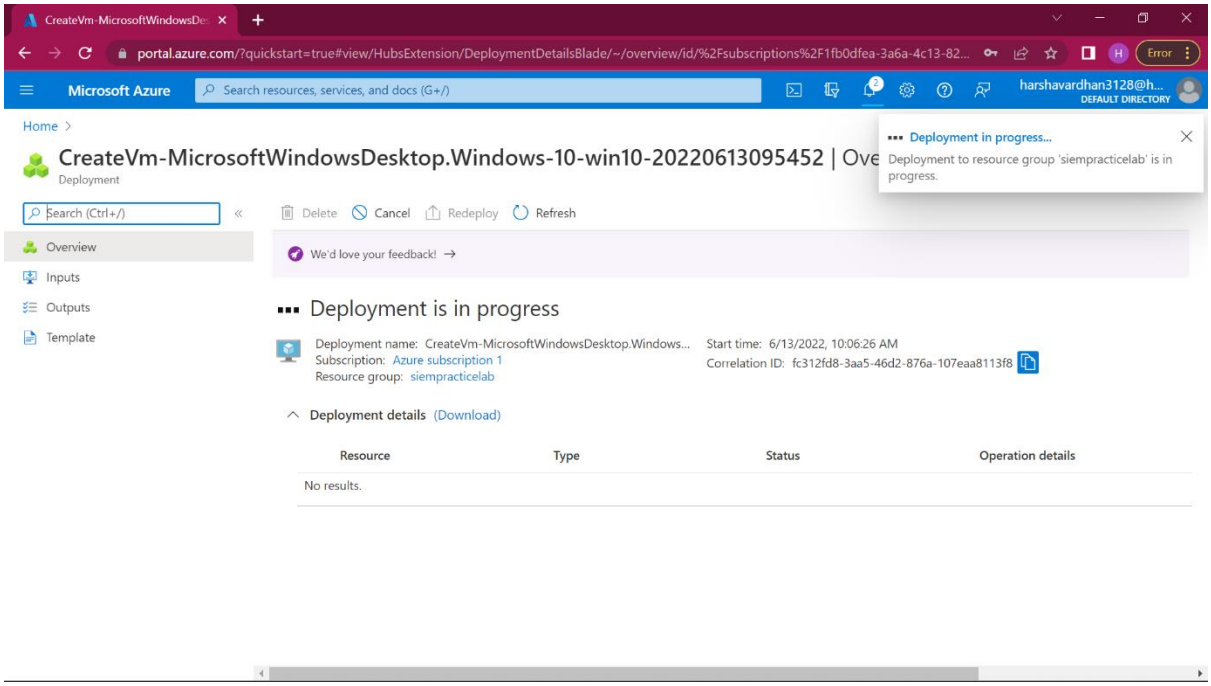


Fig 6. While deployment is in progress, I am creating a log analytical workspace.

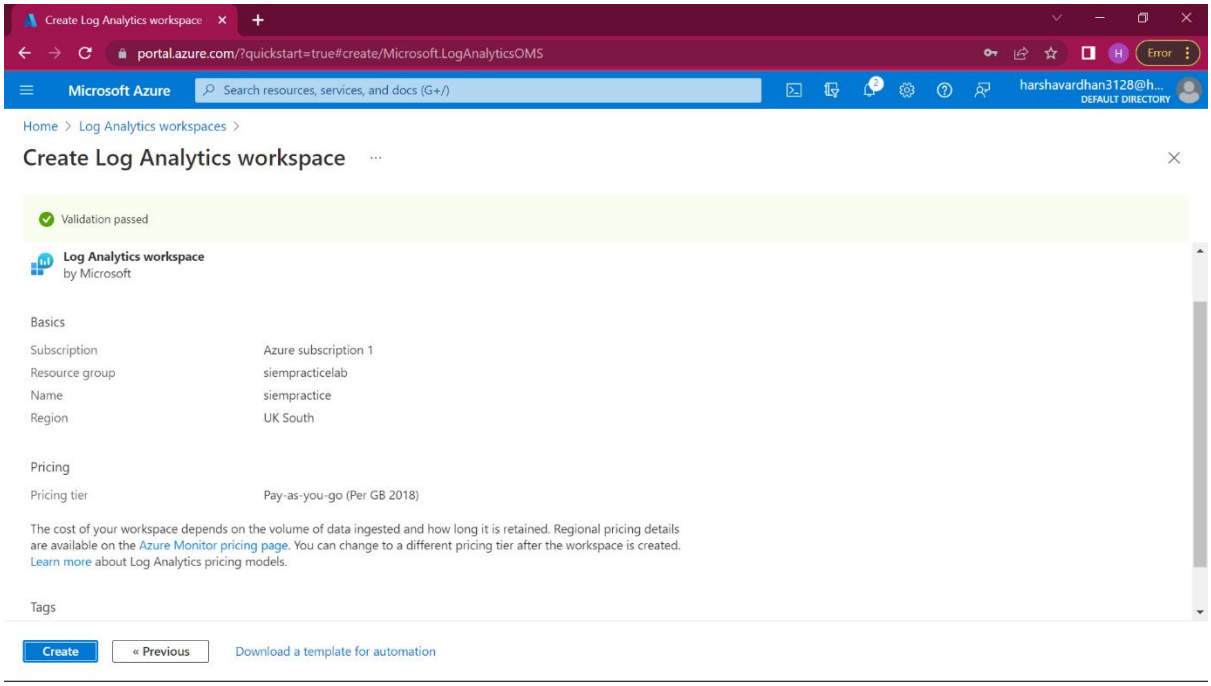


Fig7.creating it.

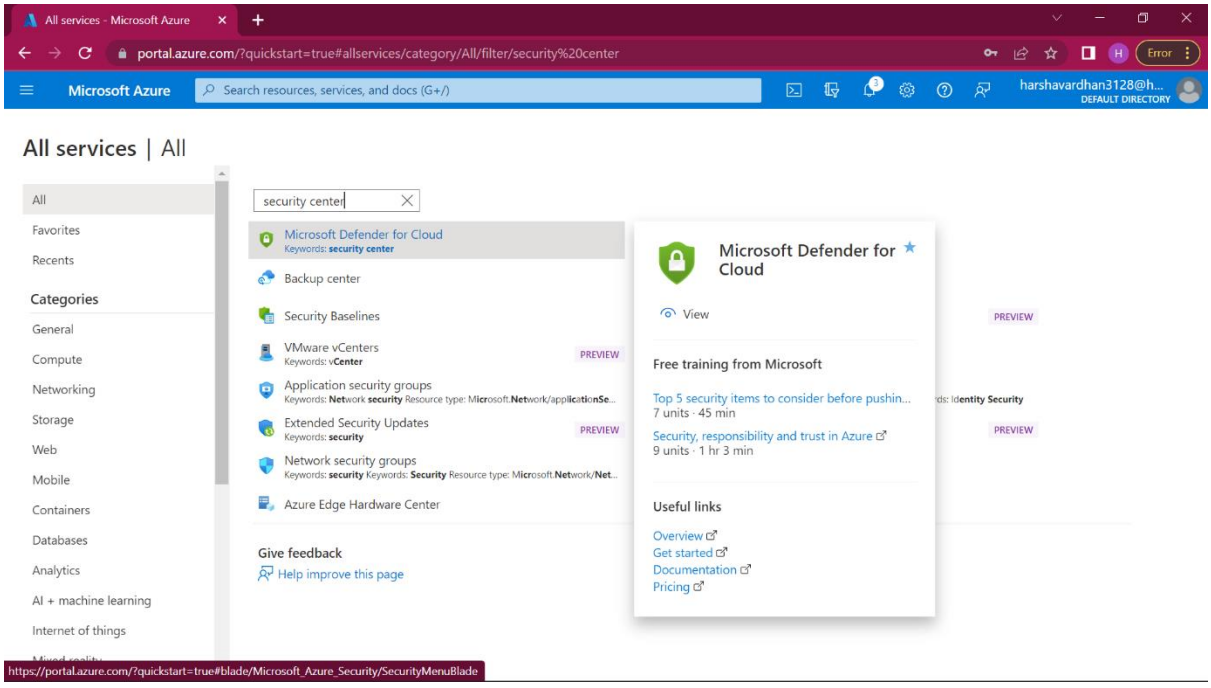


Fig8.going security centre.

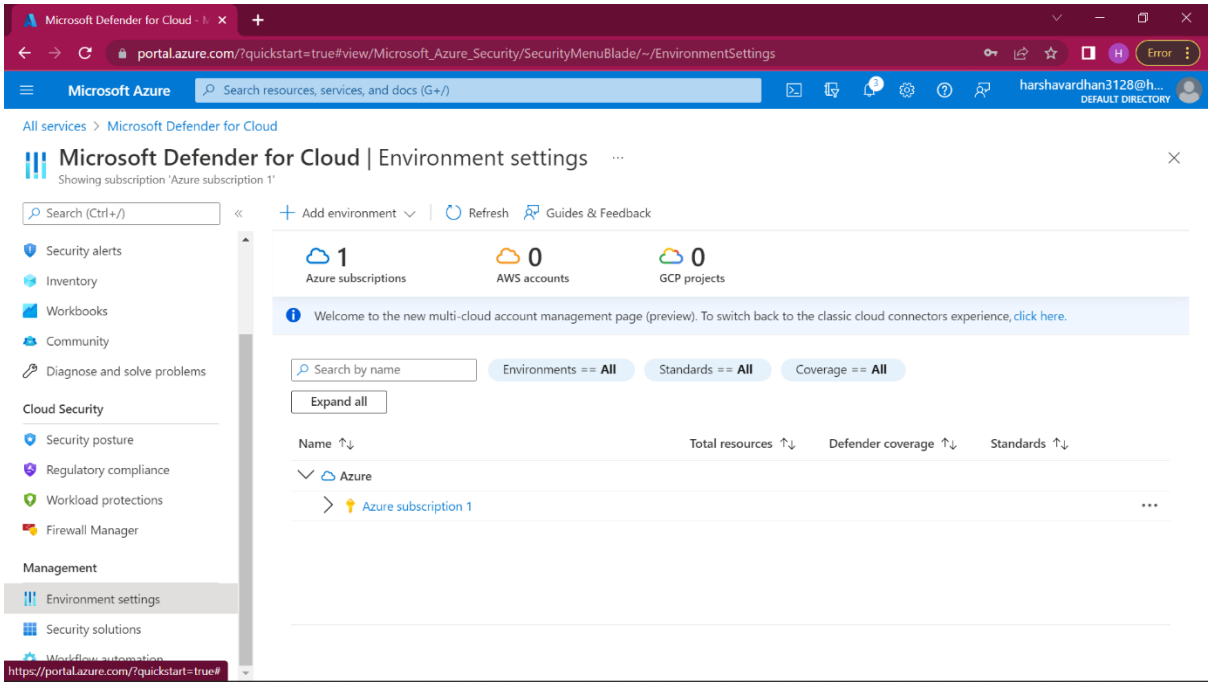


Fig9.under environment settings

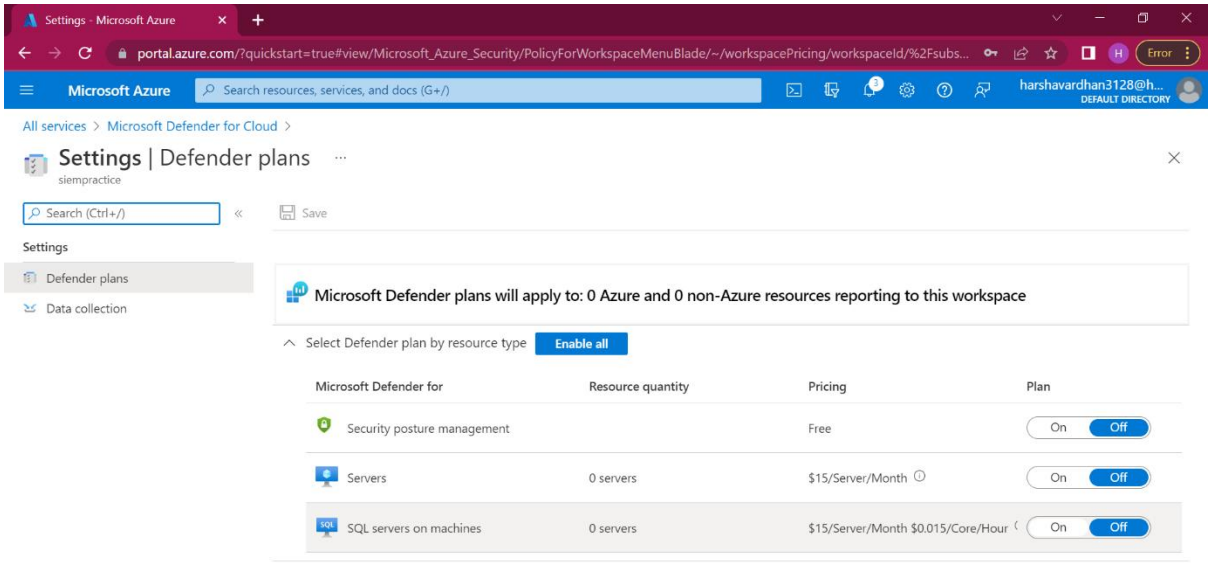


Fig10.under defender plans, turn on the security posture management and servers.

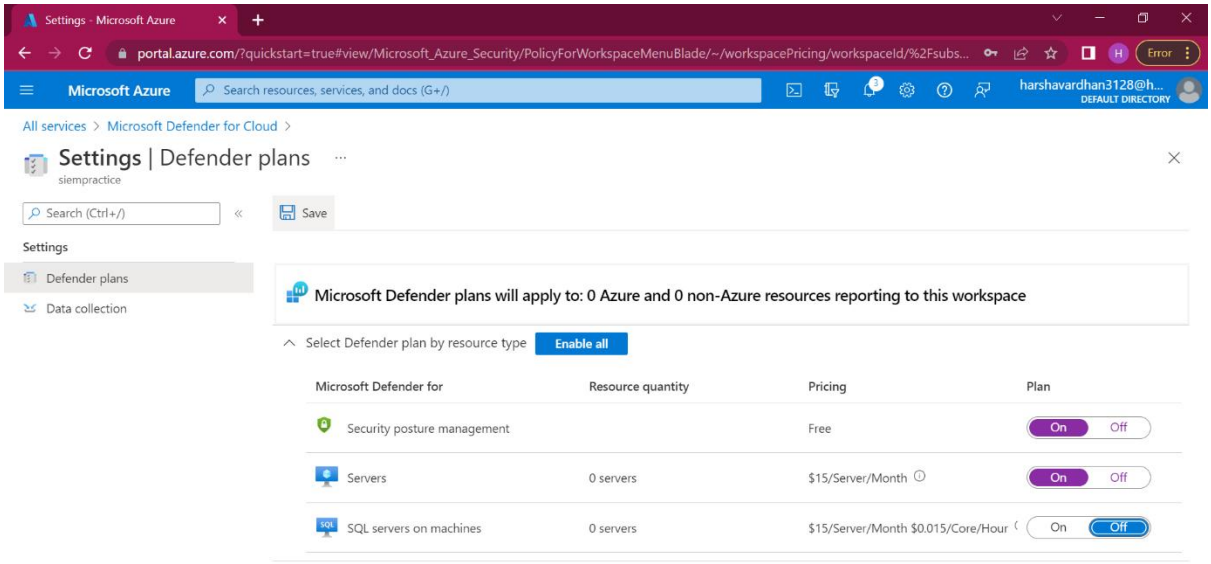


Fig11.turned on.

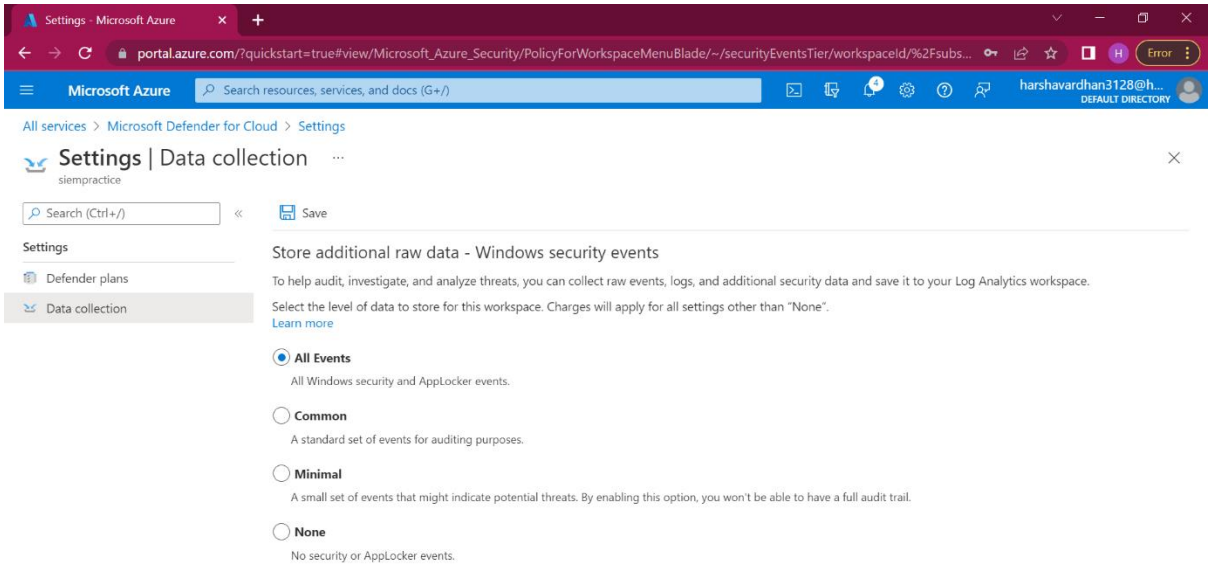


Fig 12. under data collection, select all events. Here we want to collect all the data.

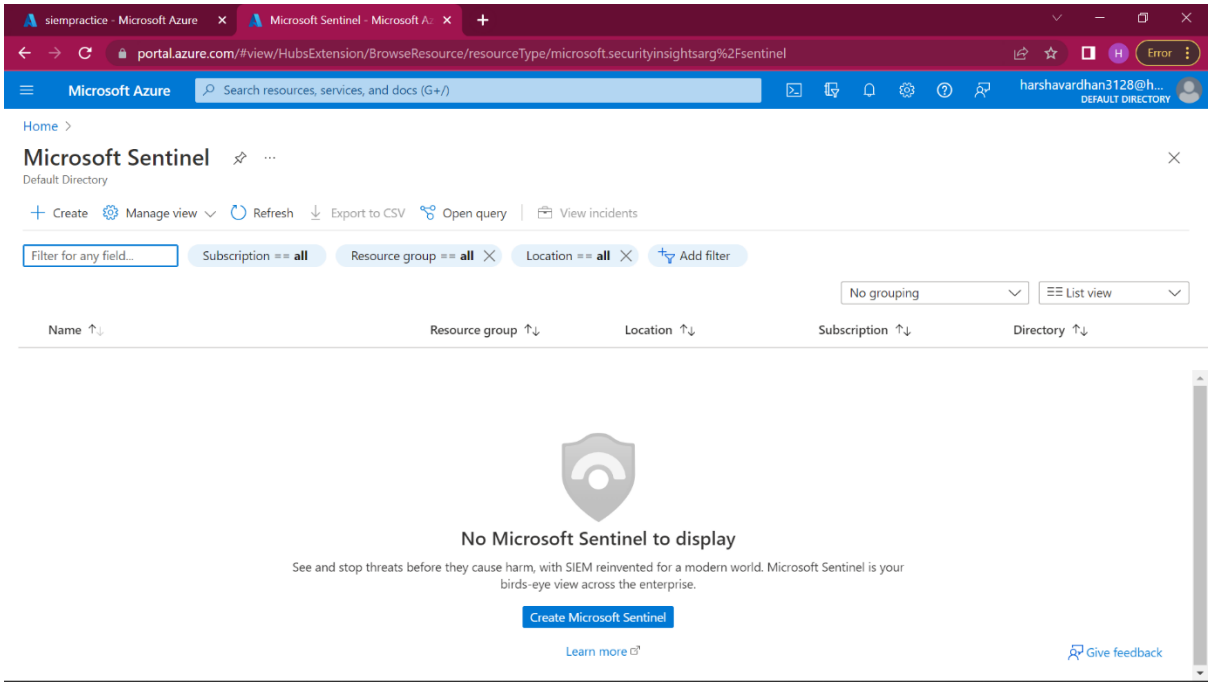


Fig 13. Now going to Microsoft sentinel

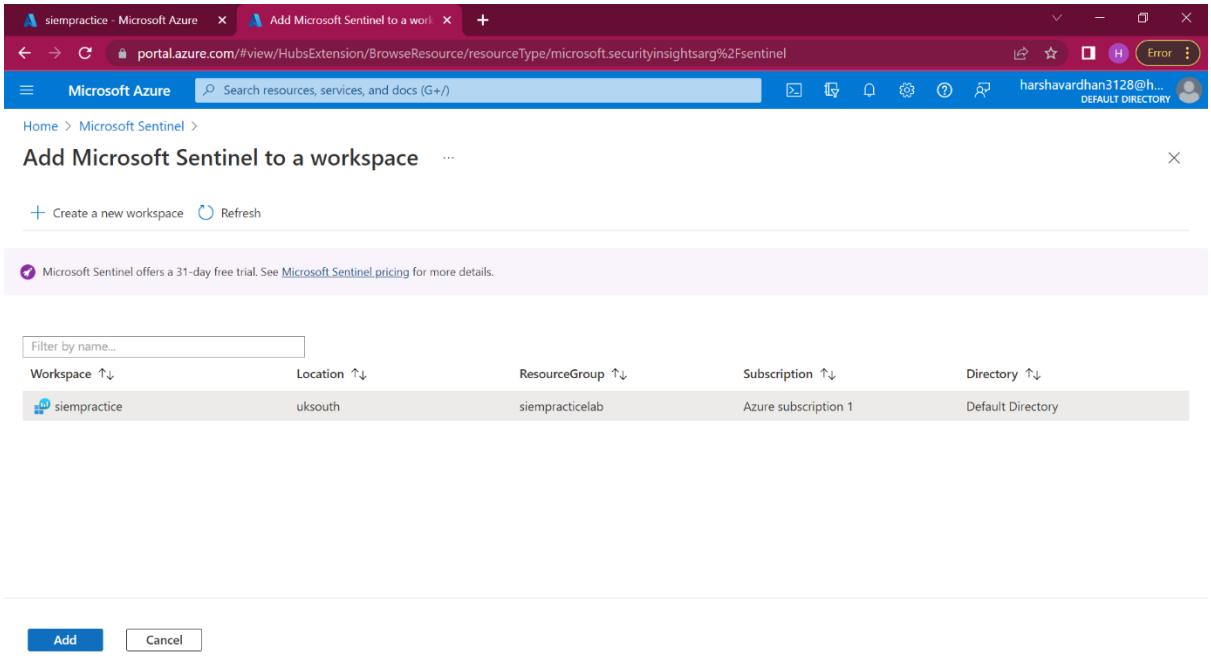


Fig14.created a Microsoft sentinel with the name of SiemPractice.

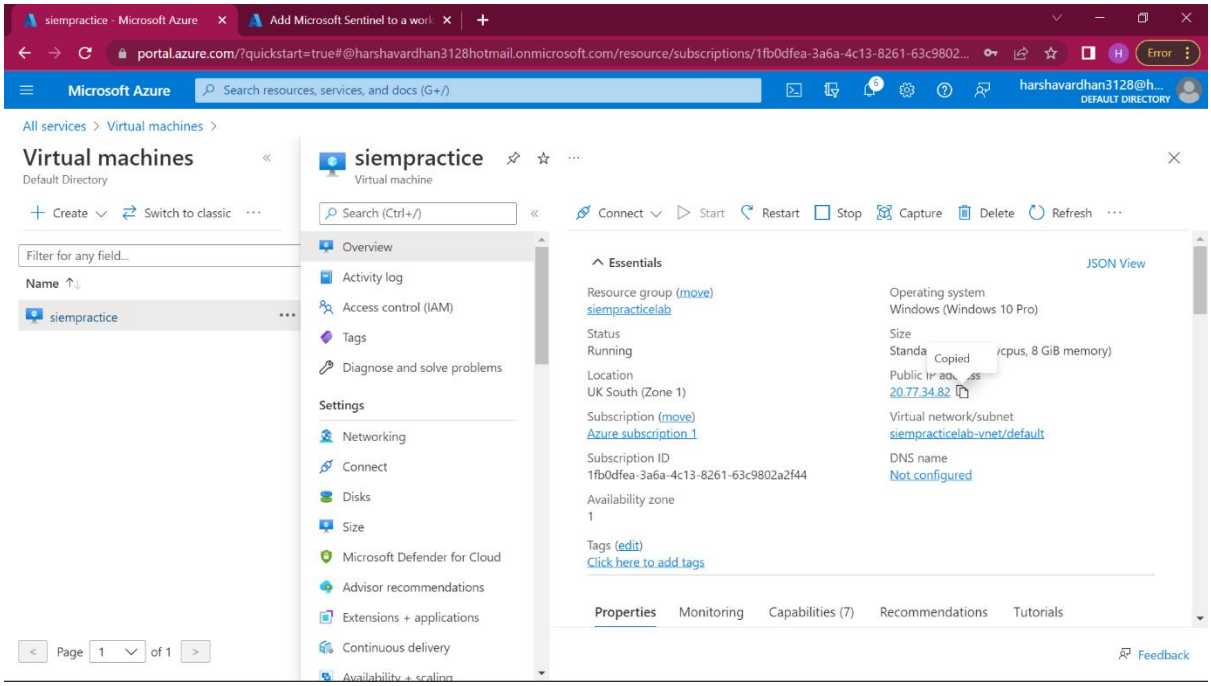


Fig 15. now coming back to my virtual machine and copying the ipv4 address.

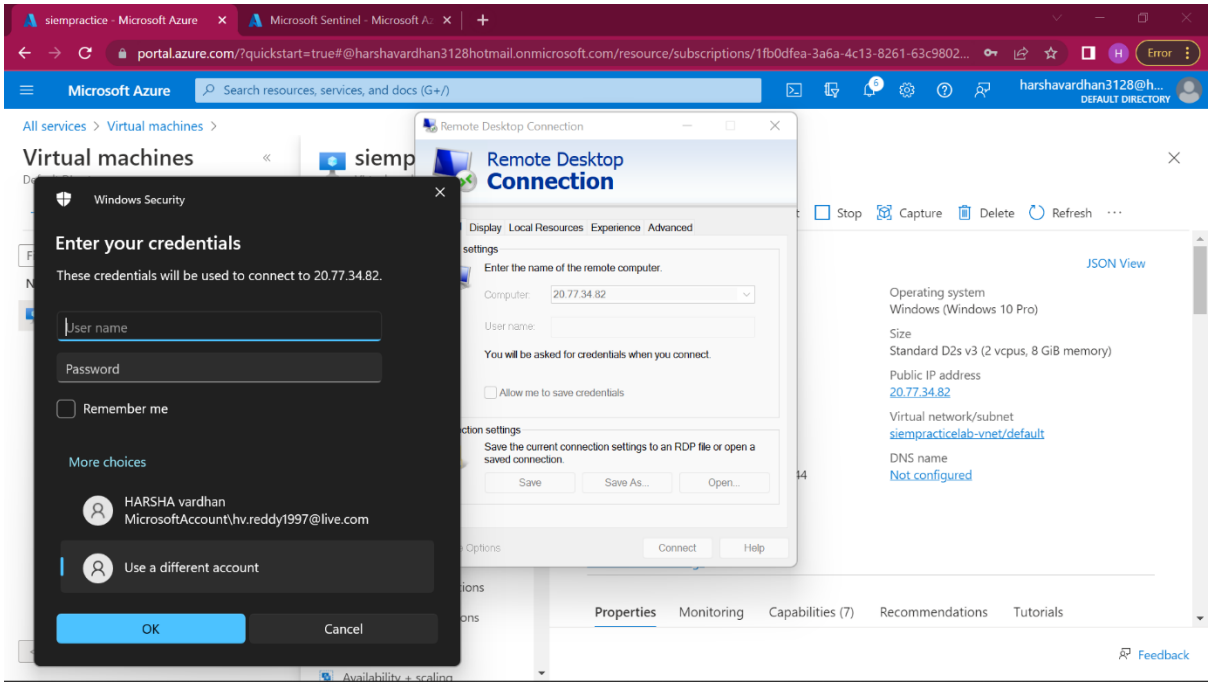


Fig16.now accessing my virtual machine with ipv4 address through remote desktop connection and logging in with credentials.

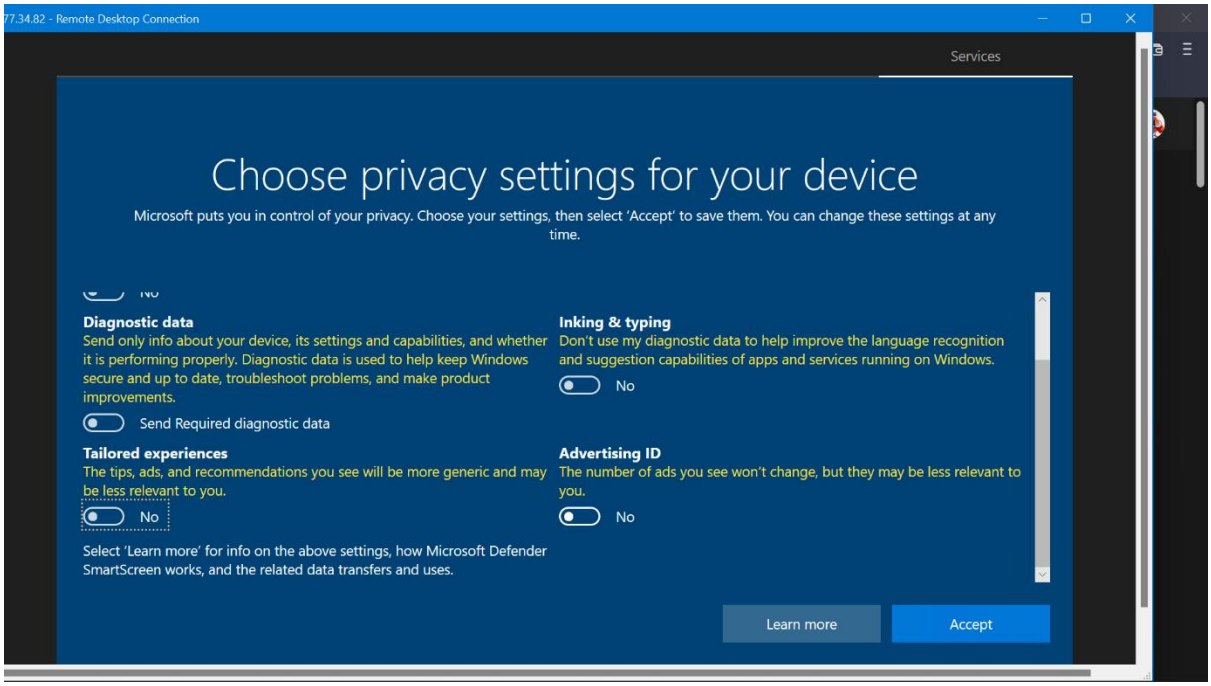


Fig 17. turning off all the settings.

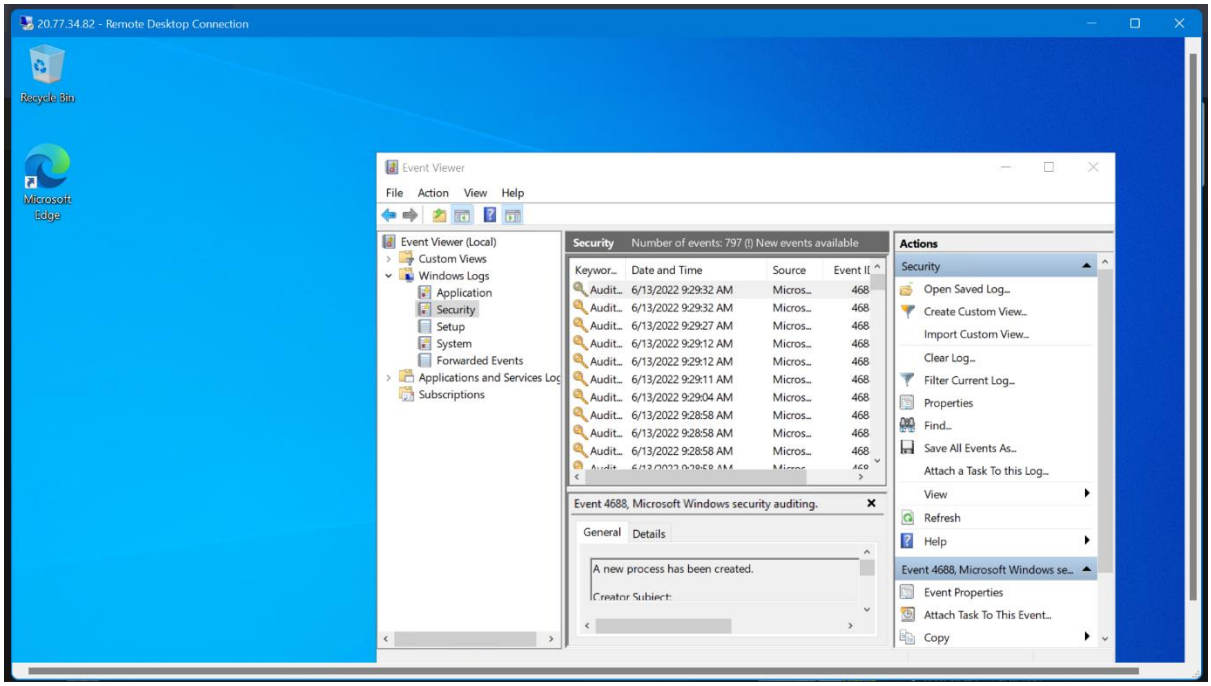


Fig 18. After accessing the virtual machine and opening the event viewer and under security, this will capture all the events when logging in and the geo-location through longitude and latitudes. I want to retrieve this data and send it to the log analytical workspace in azure.

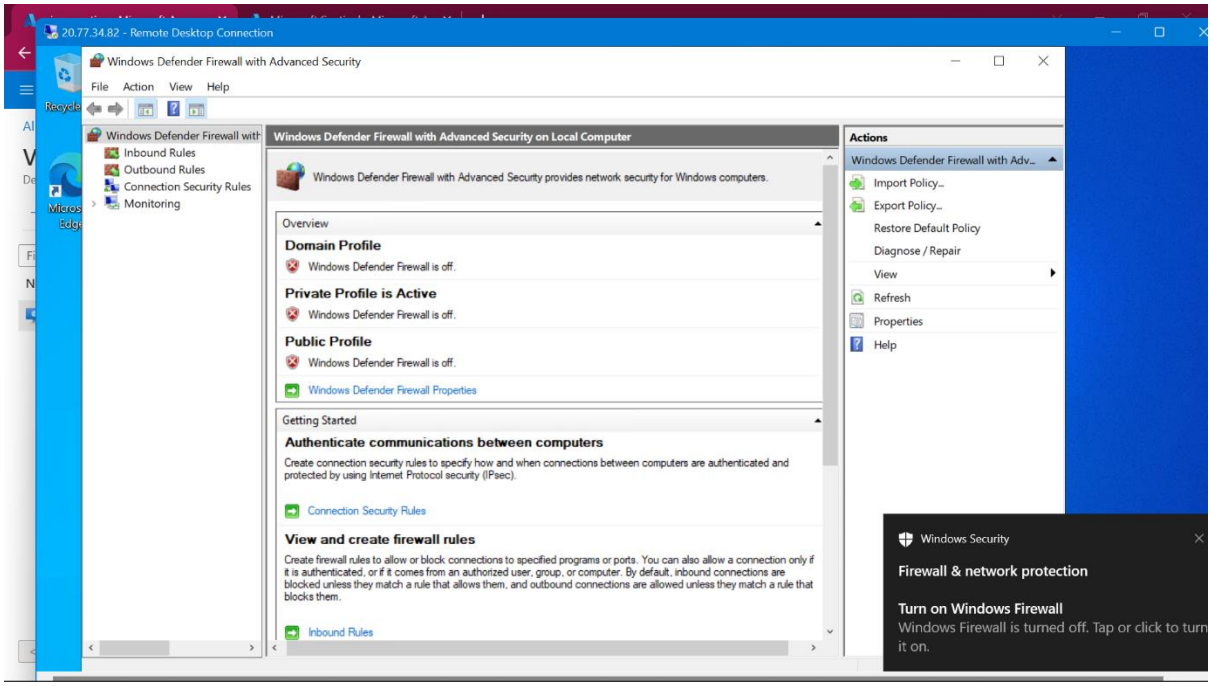


Fig19.turning off all windows firewalls to make it vulnerable and exposing this to attackers.

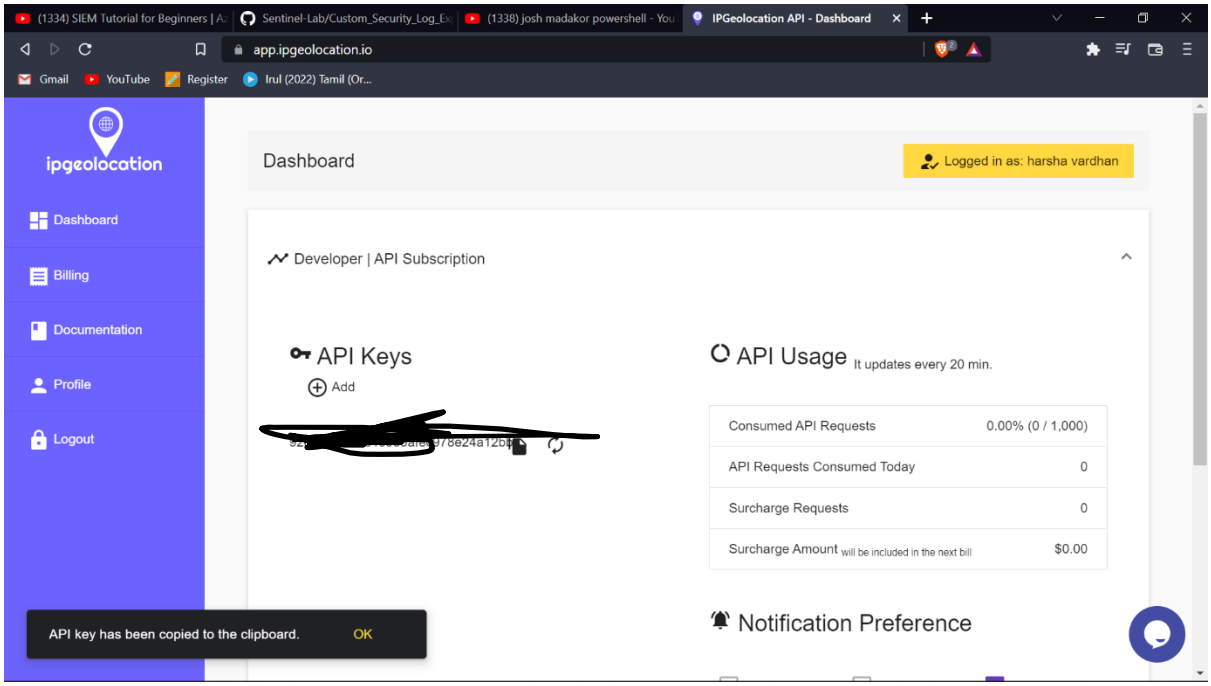


Fig 20. here I am using the IP geolocation website for the API key.

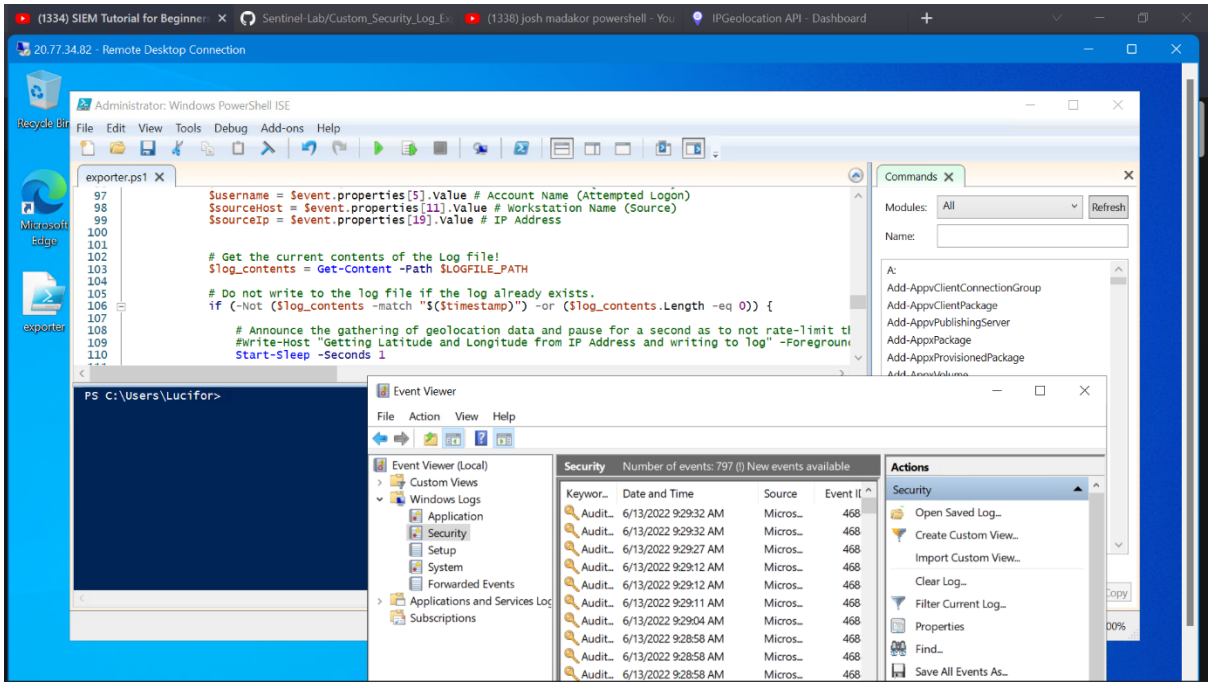


Fig 21. here I am using a custom PowerShell Script to extract metadata from Windows Event Viewer to be forwarded to a third-party API (IP geolocation website) to derive geolocation data.

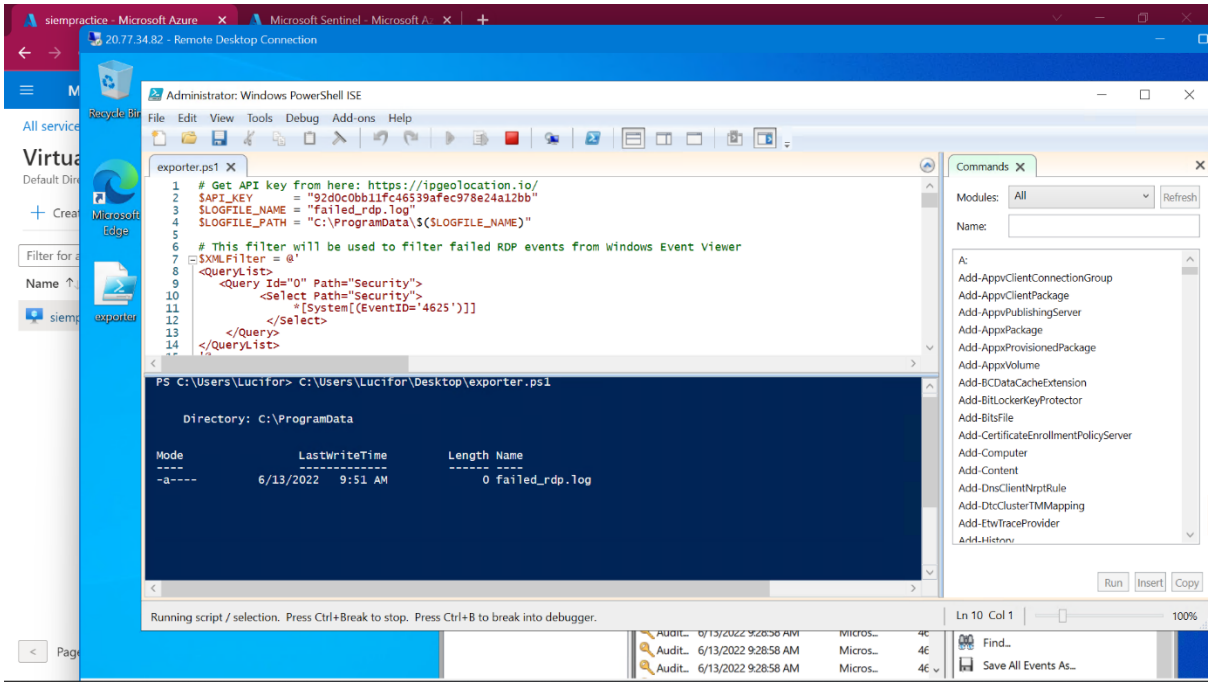


Fig 22. Running that PowerShell script.

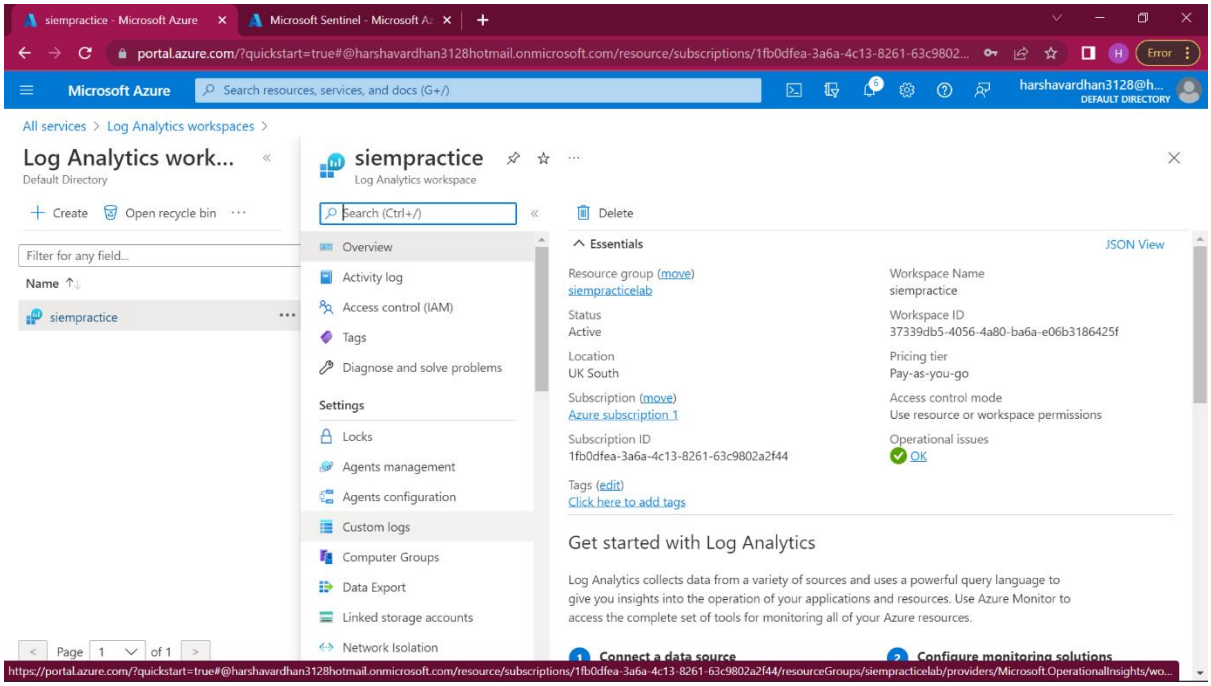


Fig 23. Open log analytics workspace activity log under custom logs.

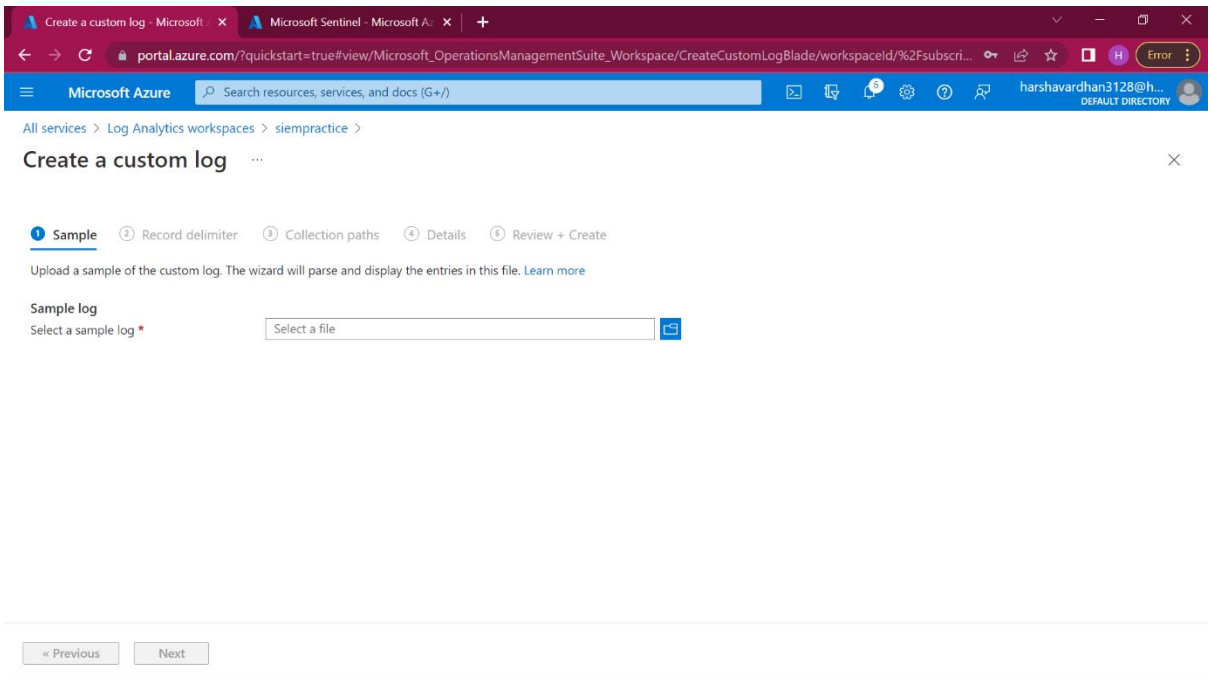


Fig 24. create a custom file. Enter a sample log.

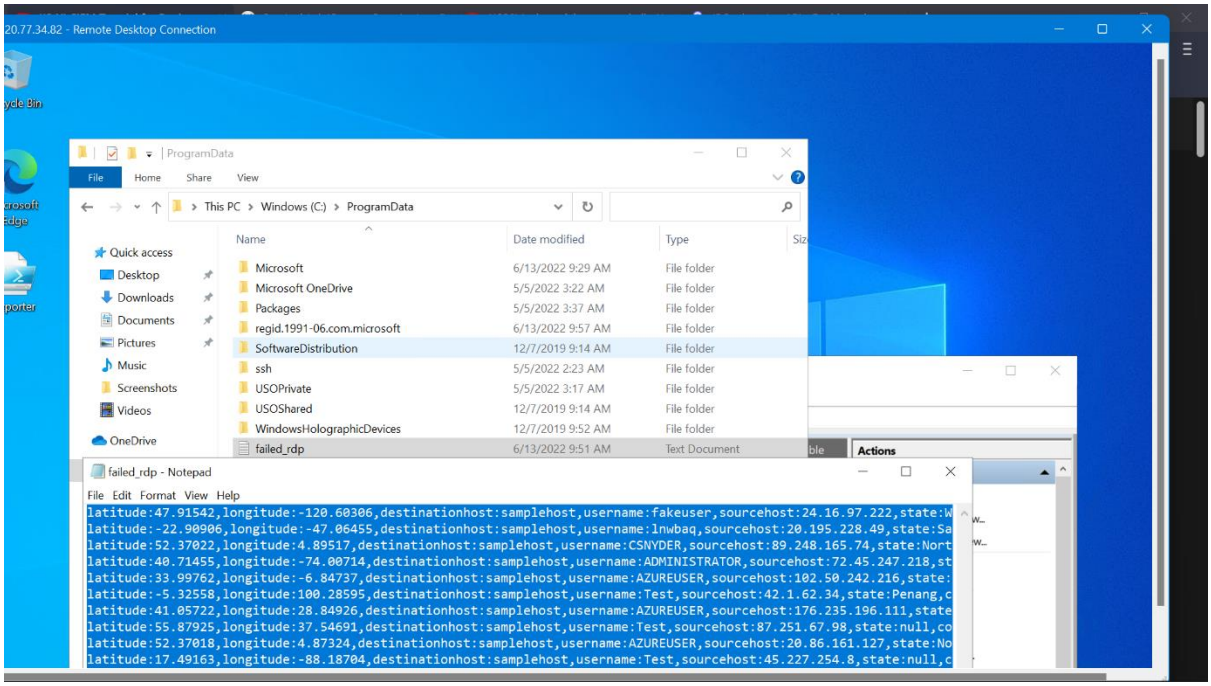


Fig 25. sample file you can find in the failed_rdp file in a virtual machine.

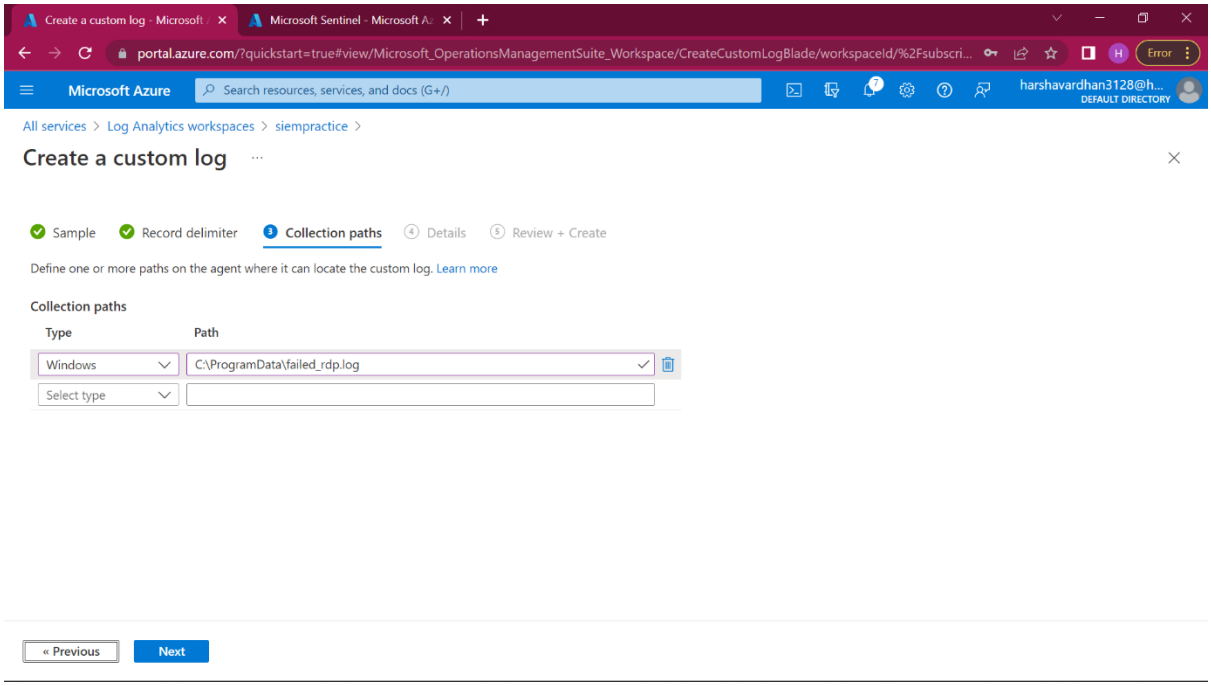


Fig 26. enter path.

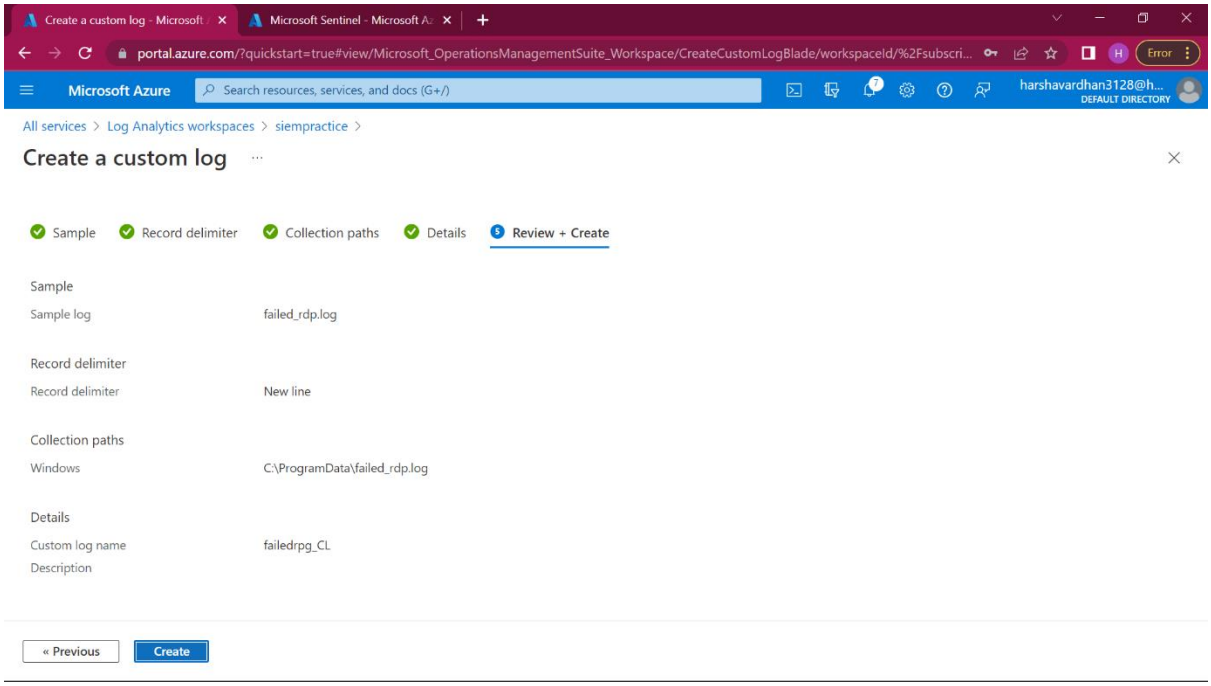


Fig 27. review and create.

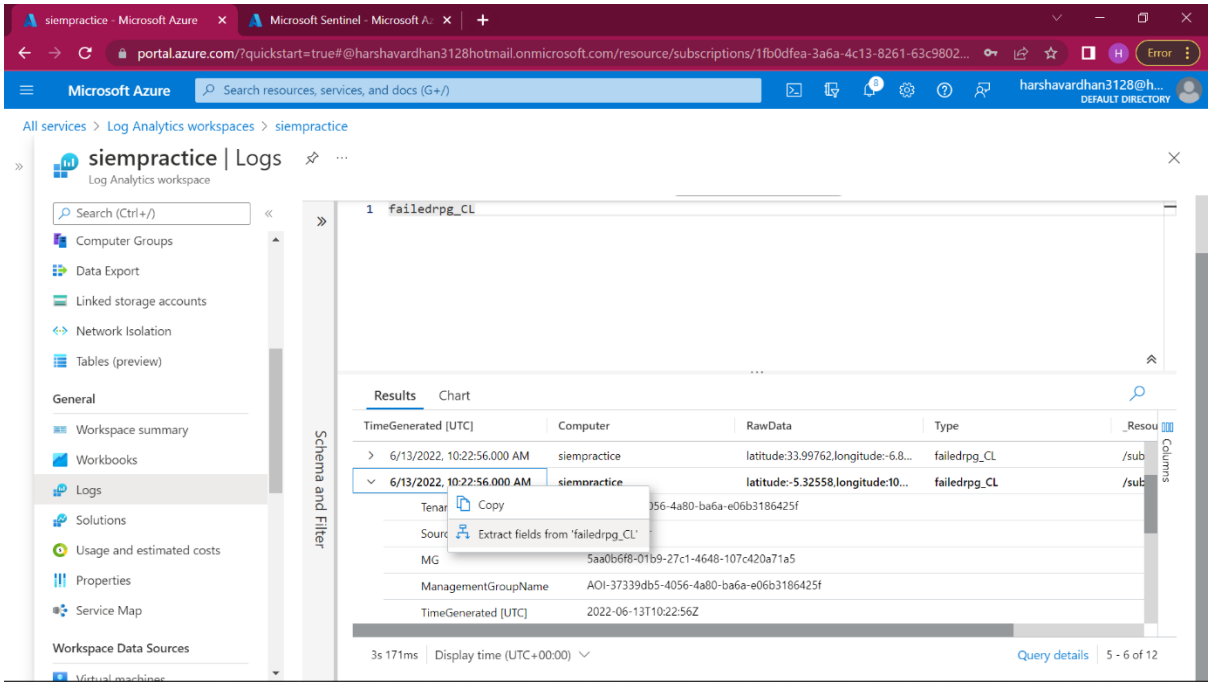


Fig 28. under logs failedrpg_CL open Extract fields from ‘failedrpg_CL’

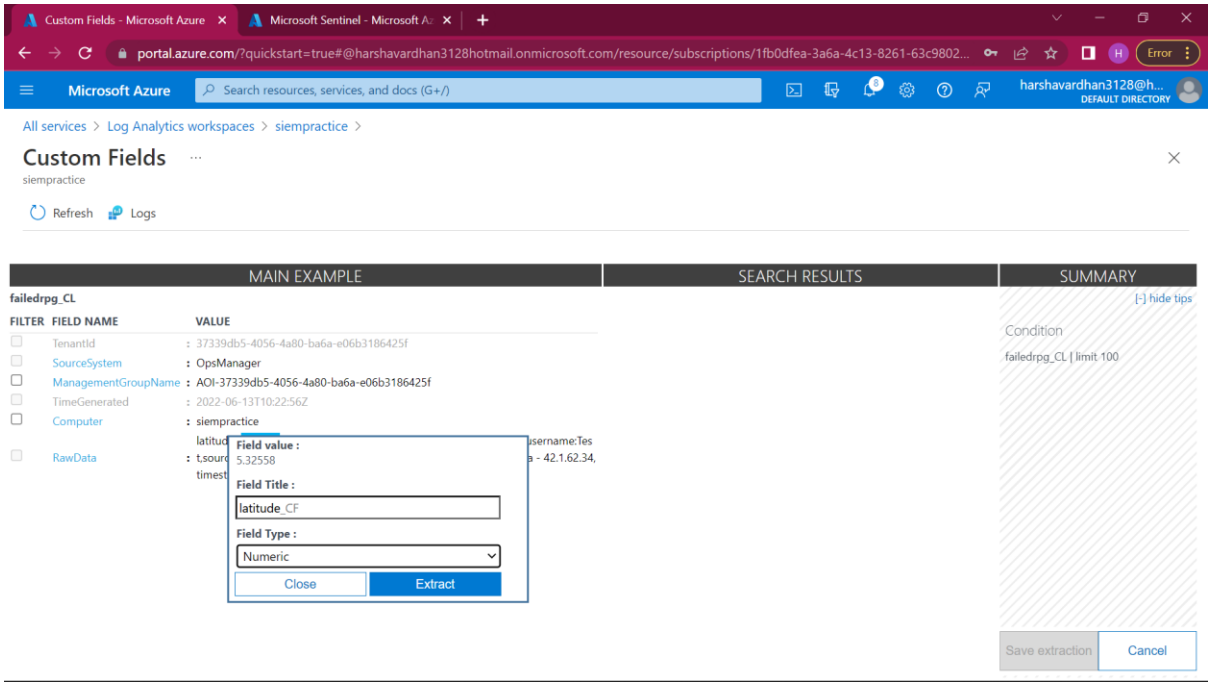


Fig 29. Here I am extracting everything by name. (custom fields/extract fields from raw custom log data)

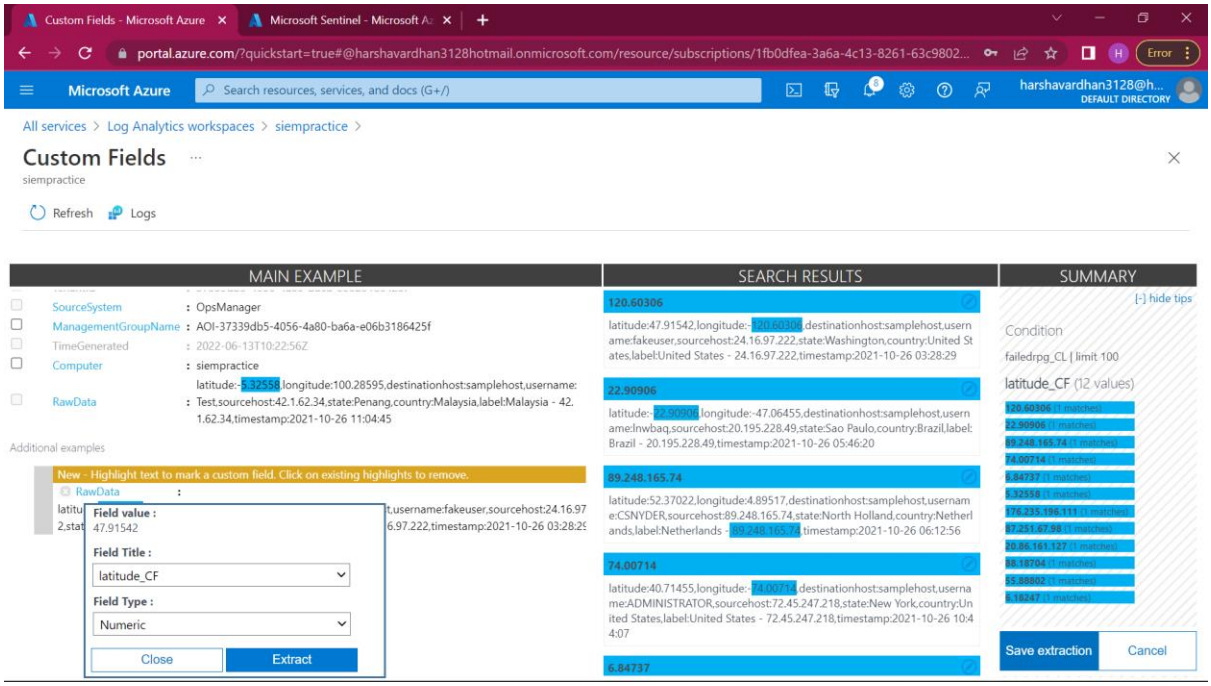


Fig 30. Checking and correcting the data and extracting

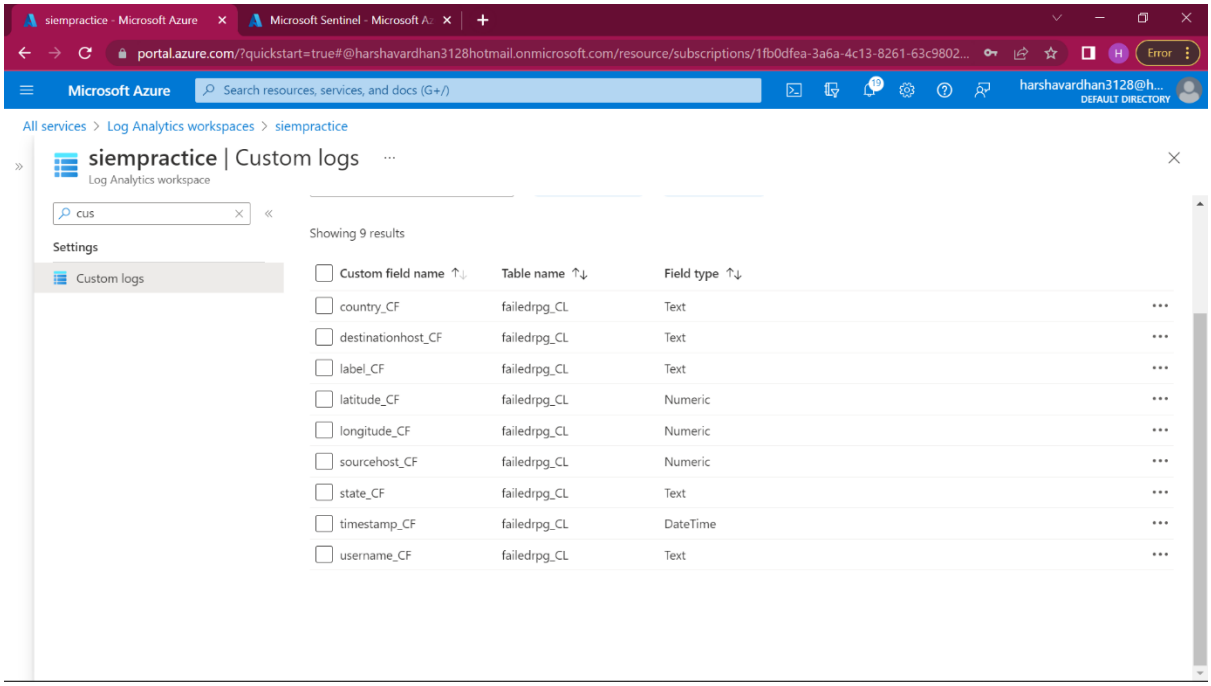


Fig 31. Like this, extracting everything by names.

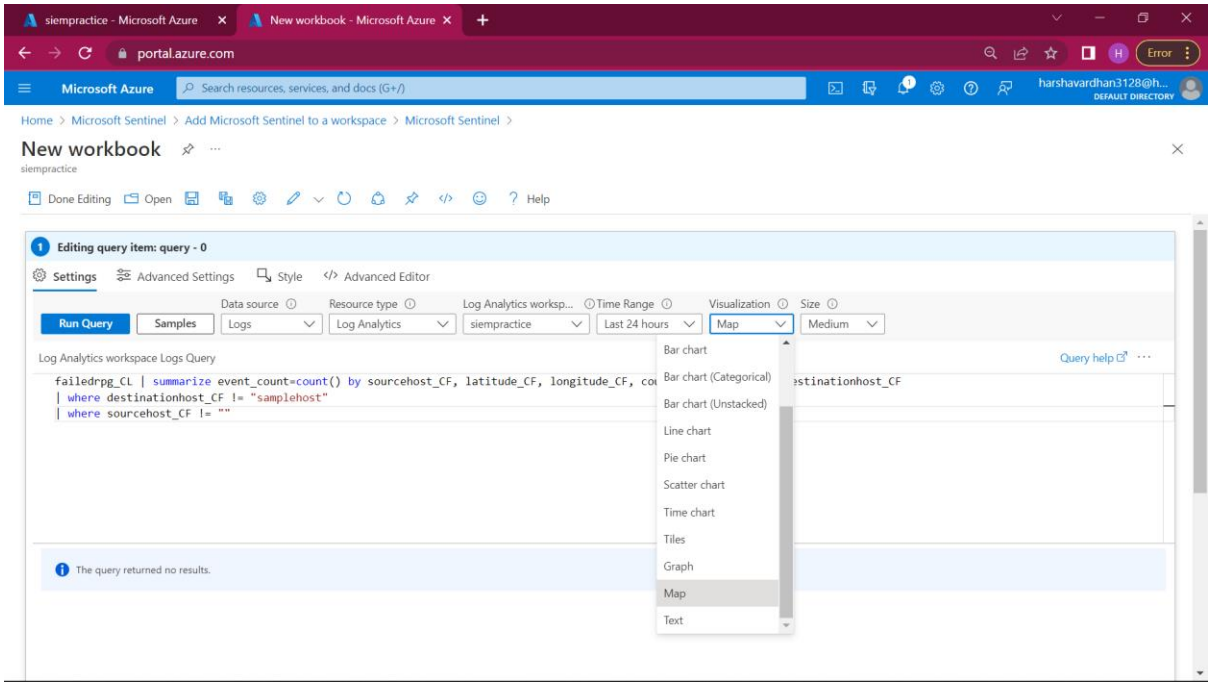


Fig 32. Hereafter that is coming back to azure sentinel and under the workbook and writing a query to Setup map in sentinel with Latitude and Longitude (or country)

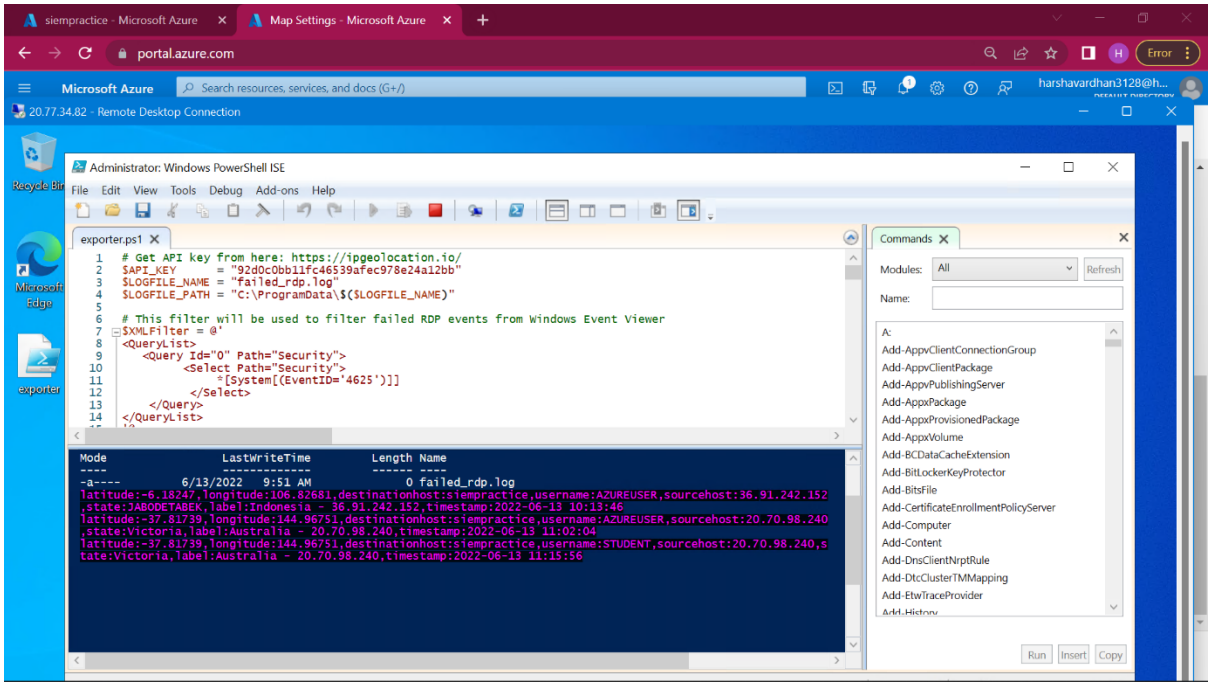


Fig 33. here you can see on my virtual machine someone from Australia who tried to log in with details shown on the map through azure sentinel. You can see this in the following figure.

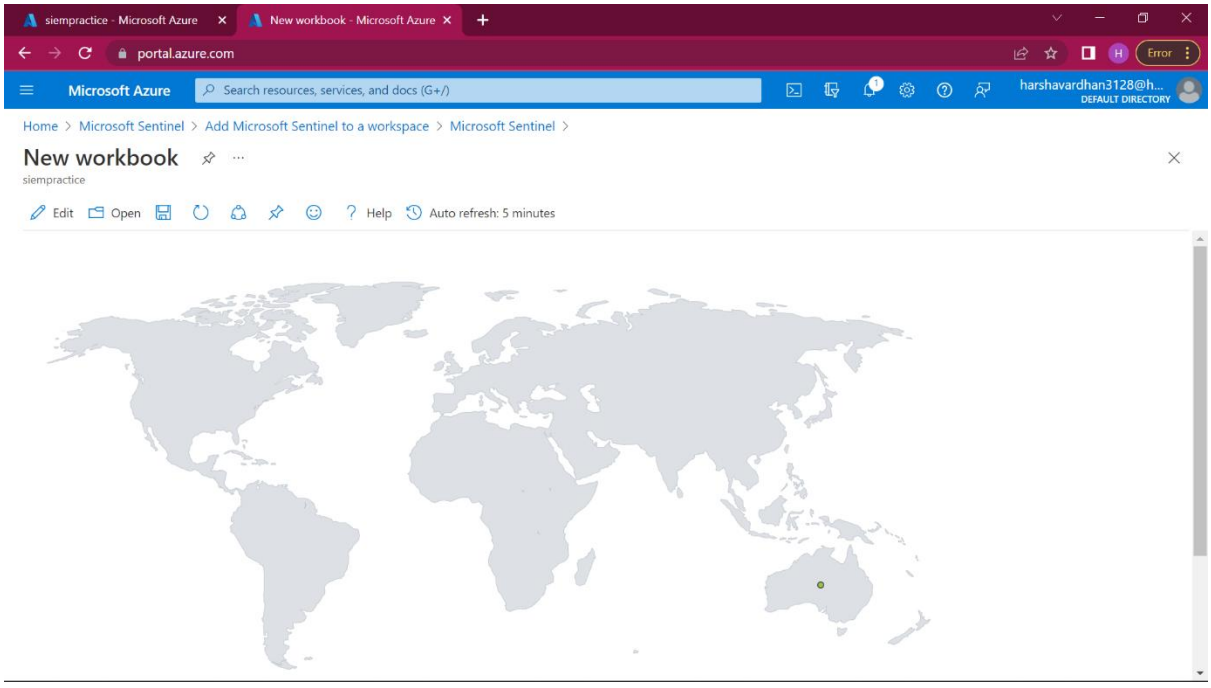


Fig 34. you can see here a green dot from Australia.

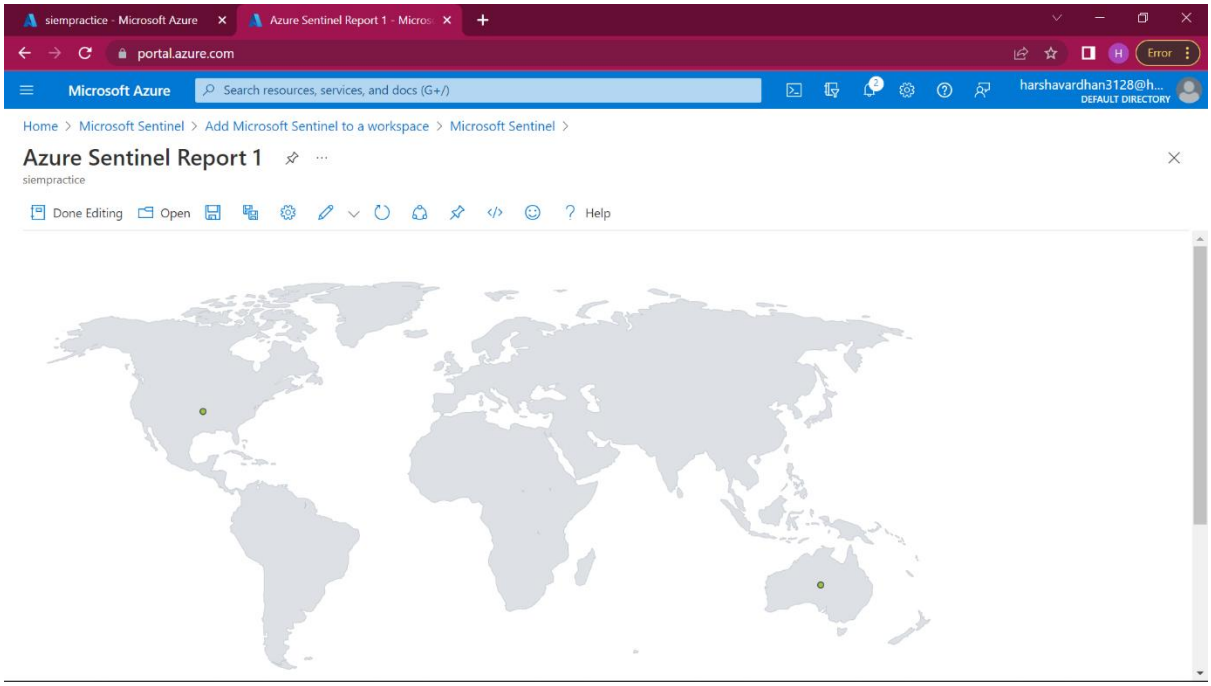


Fig 35. After that, I waited a few hours. One was recorded someone tried to log in with the USA.

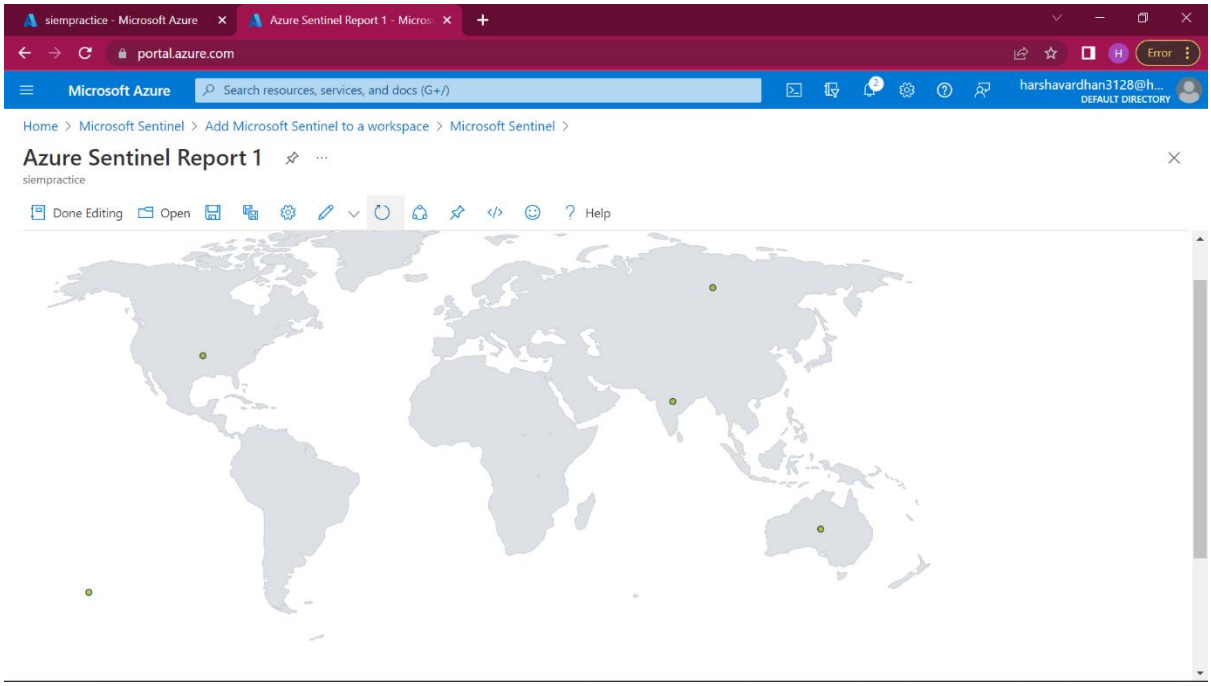


Fig 36. after a few hours, someone from India and Russia tried to log in with my virtual windows.