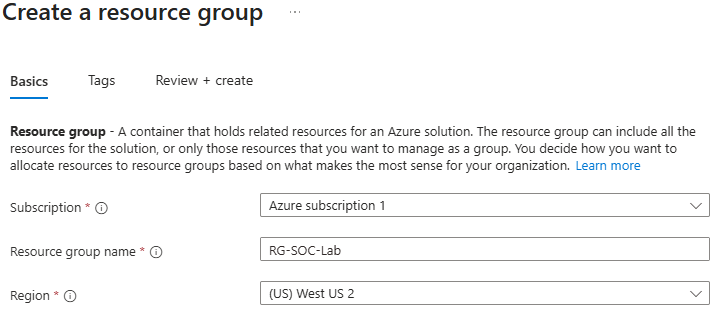
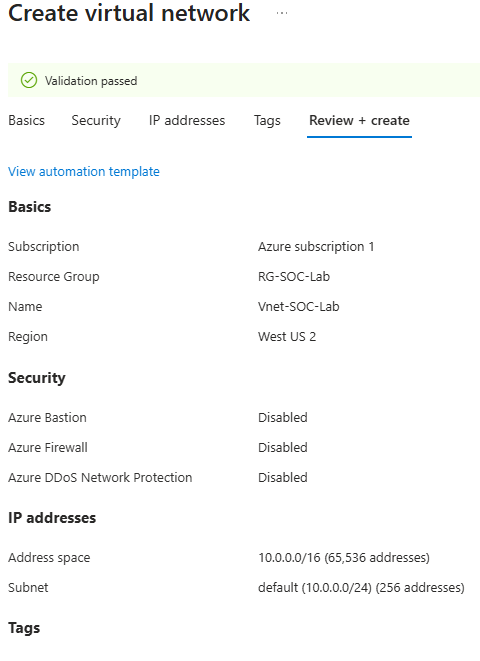
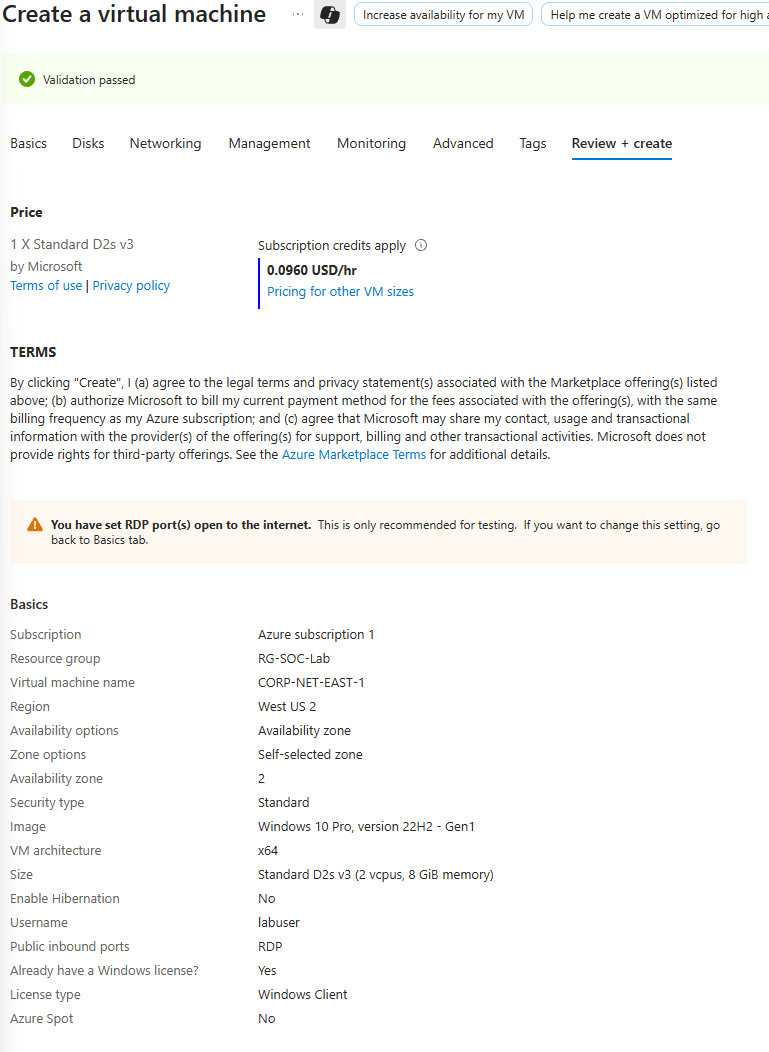
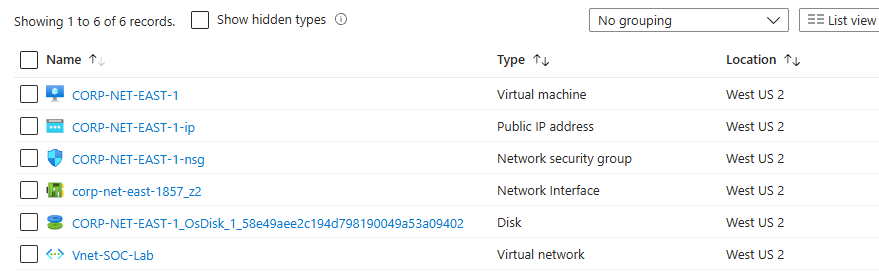
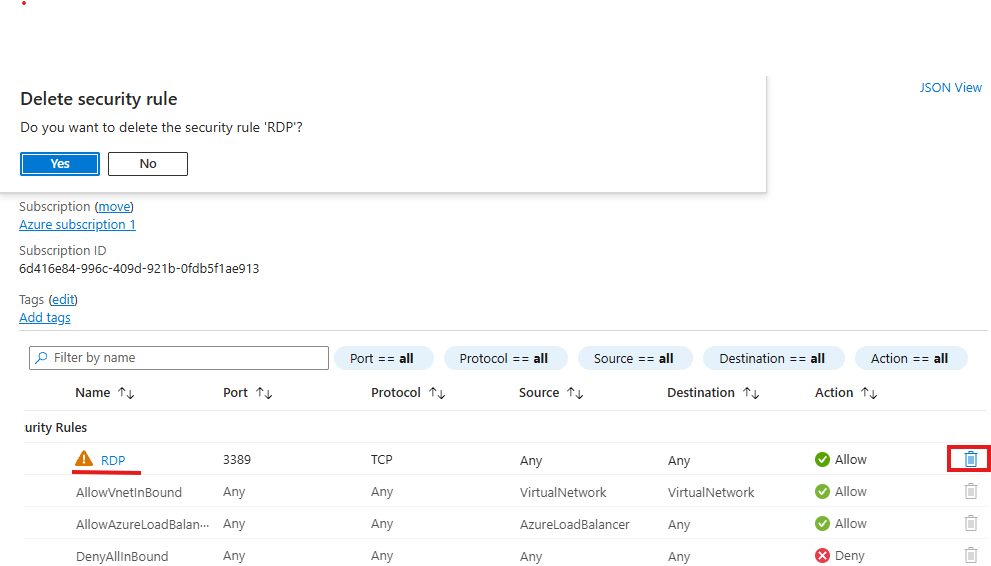
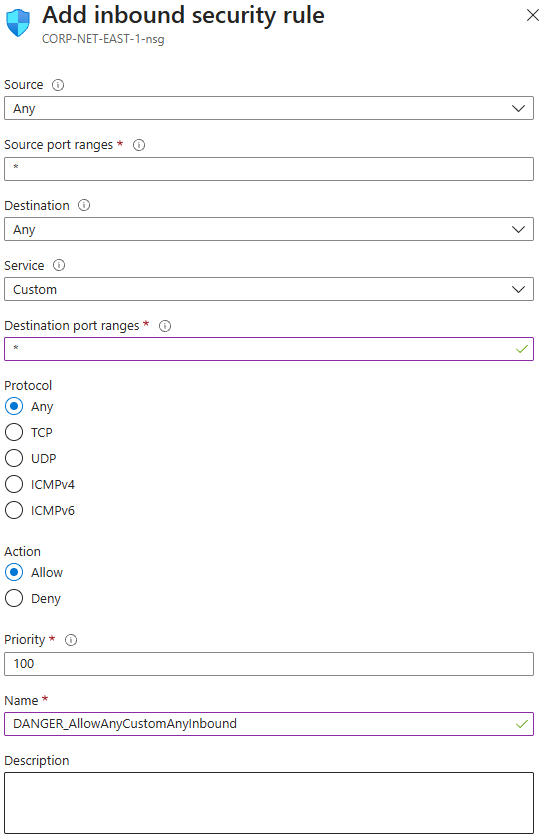
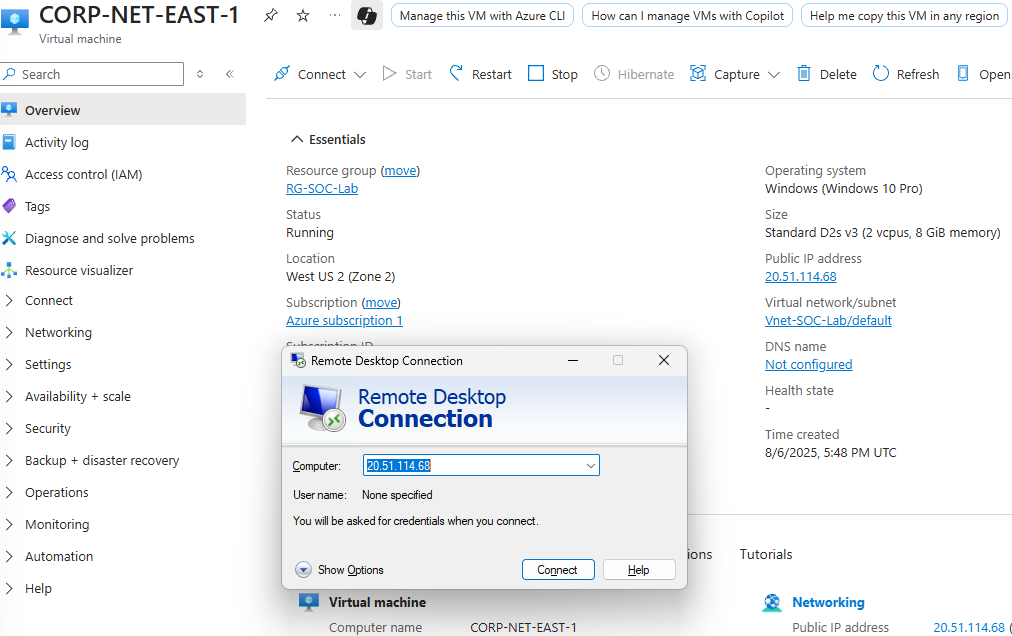
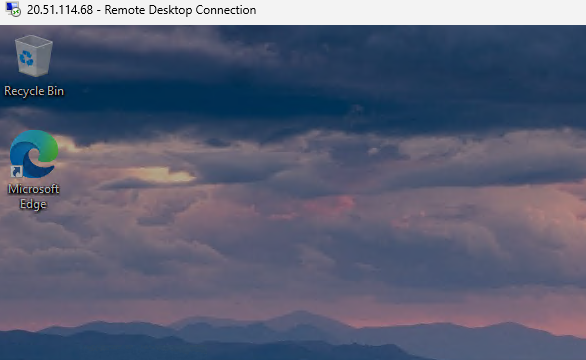
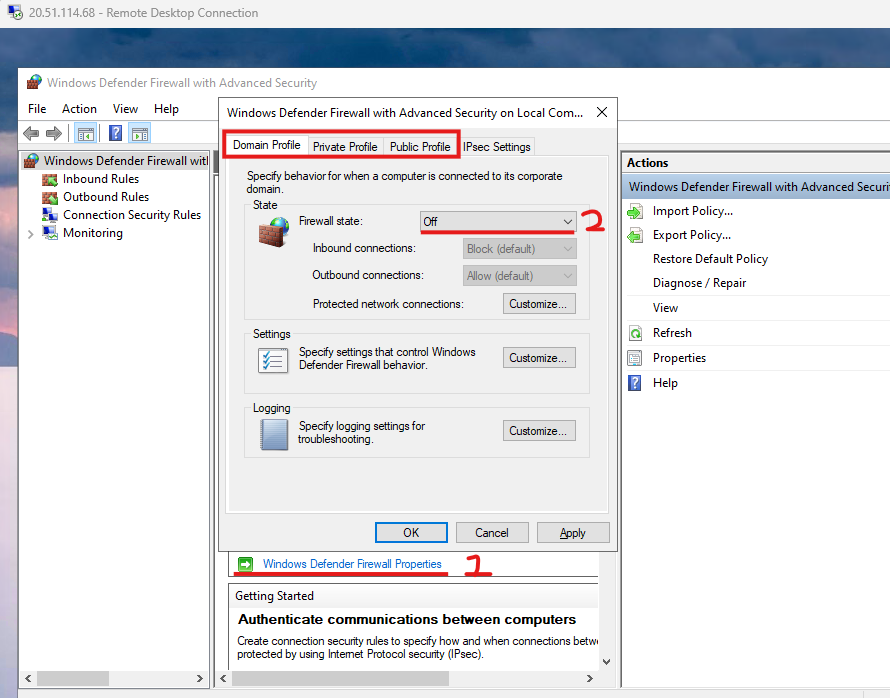
1. Create a resource group



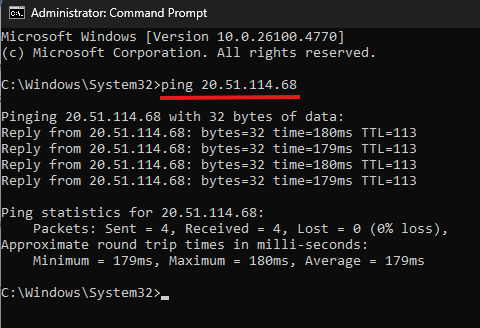
1. Create a virtual network
2. Create a virtual machine (Honeypot) -Password- Cyberlab123!  
   
3. This is the resource groups after done of created look.  
   
4. Go to network security group to open the firewall for the attack vector access . Delete the default RDP.  
   
5. Add new inbound security rule .  
   
6. Go the Azure virtual machines copy the Public IP address. Use your own computer Remote Desktop Connection paste the Public IP content. After that , enter the VM username and password to access the Azure VM.  
   
7. Access successfully.



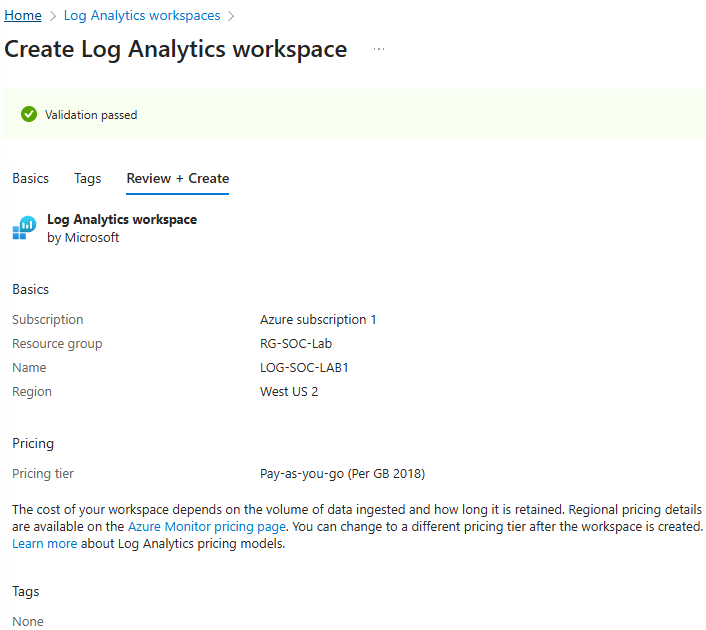
1. Run -” wf.msc “. Go to Windows Defender Firewall Properties. Turn off domain, private and public profile firewall state.



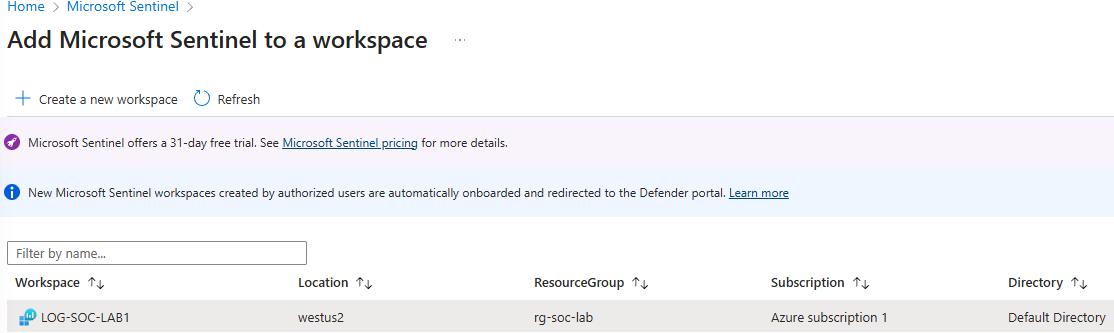
1. Go to your own cmd try to ping the VM Public IP. Check can access for the VM or not.



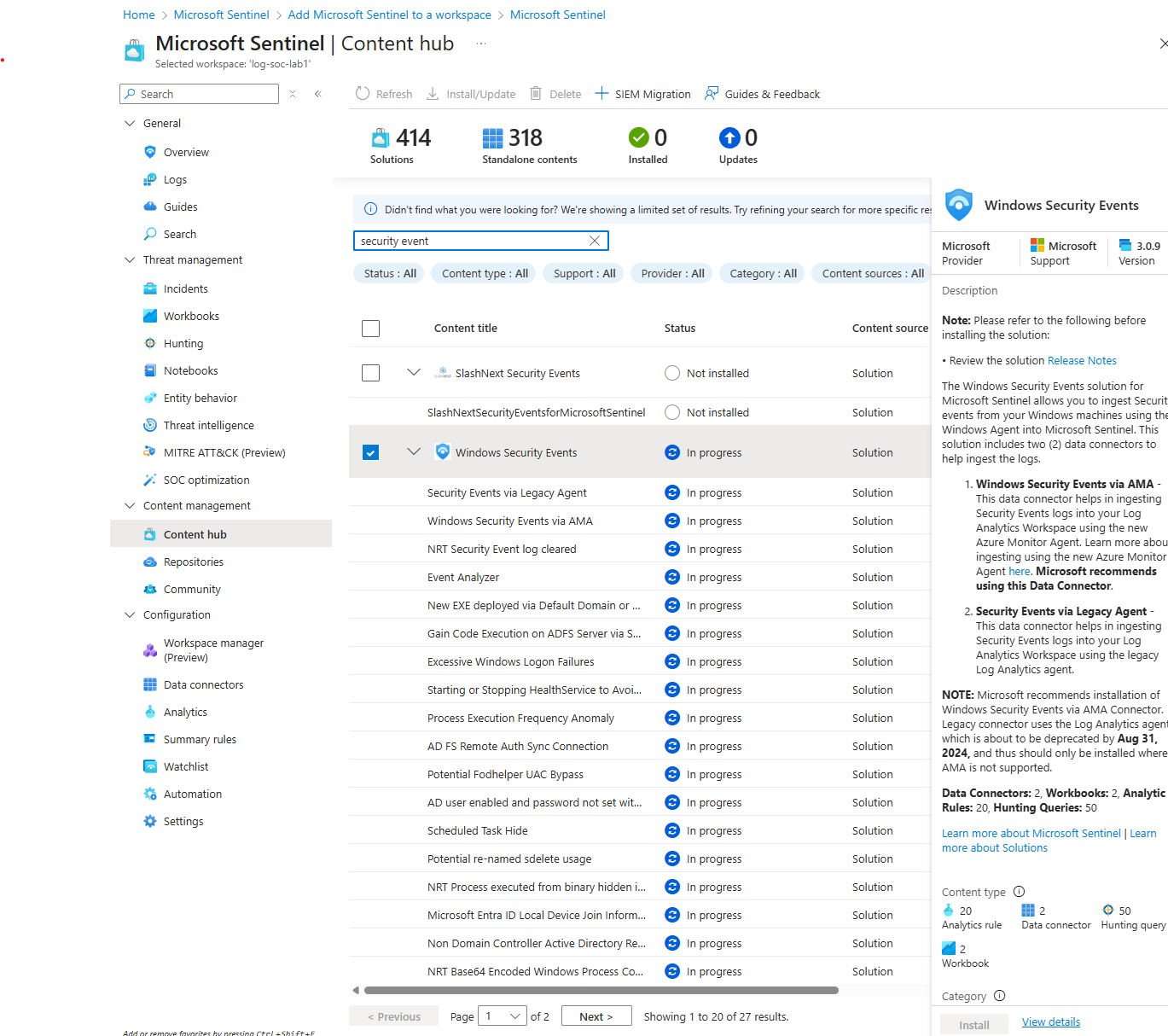
1. Go to Azure create log analytics workspace.



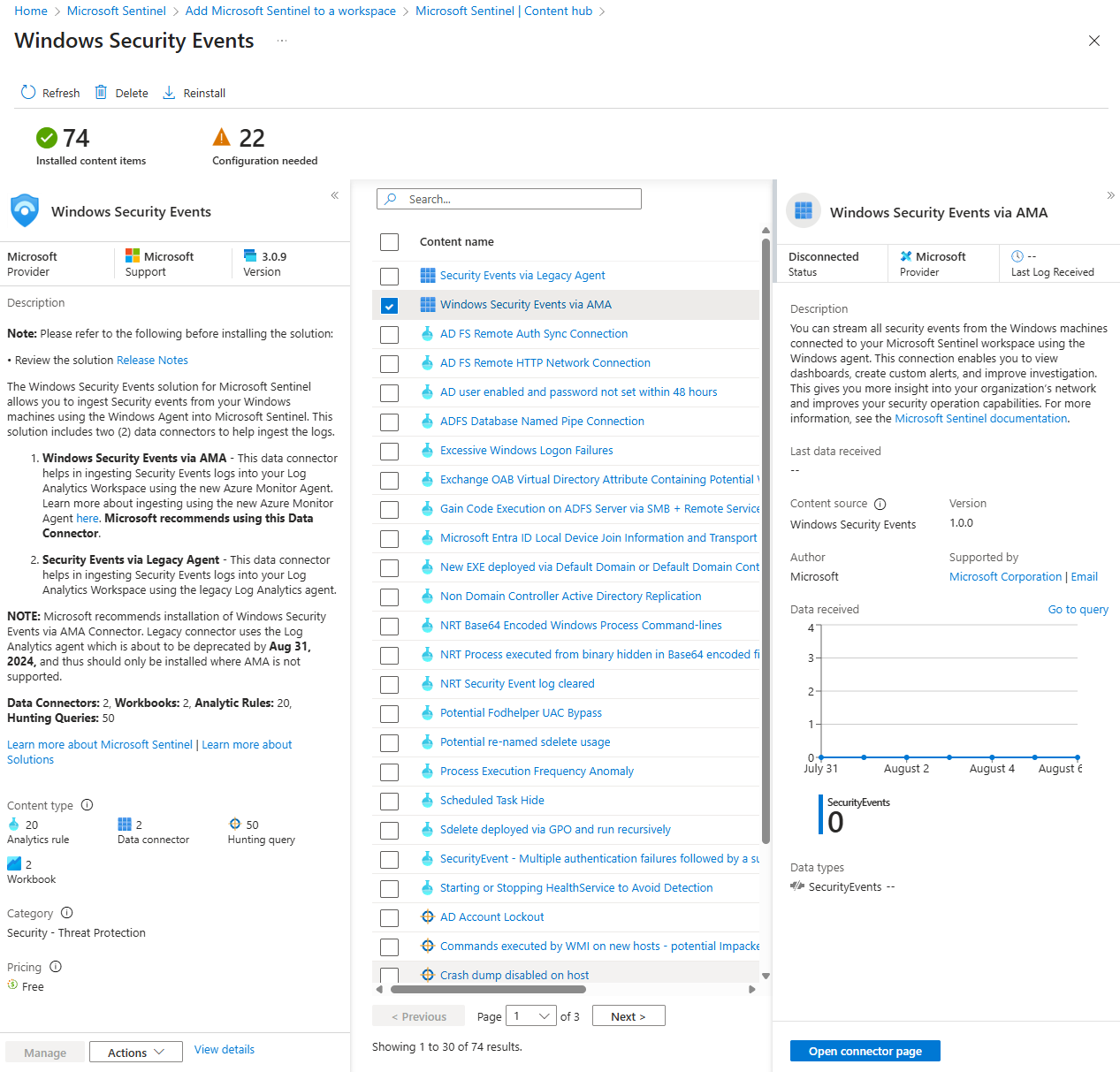
1. Go Azure Microsoft Sentinel add the LOG-SOC-LAB1 for link log analytics workspace to the Azure Microsoft Sentinel (SIEM).



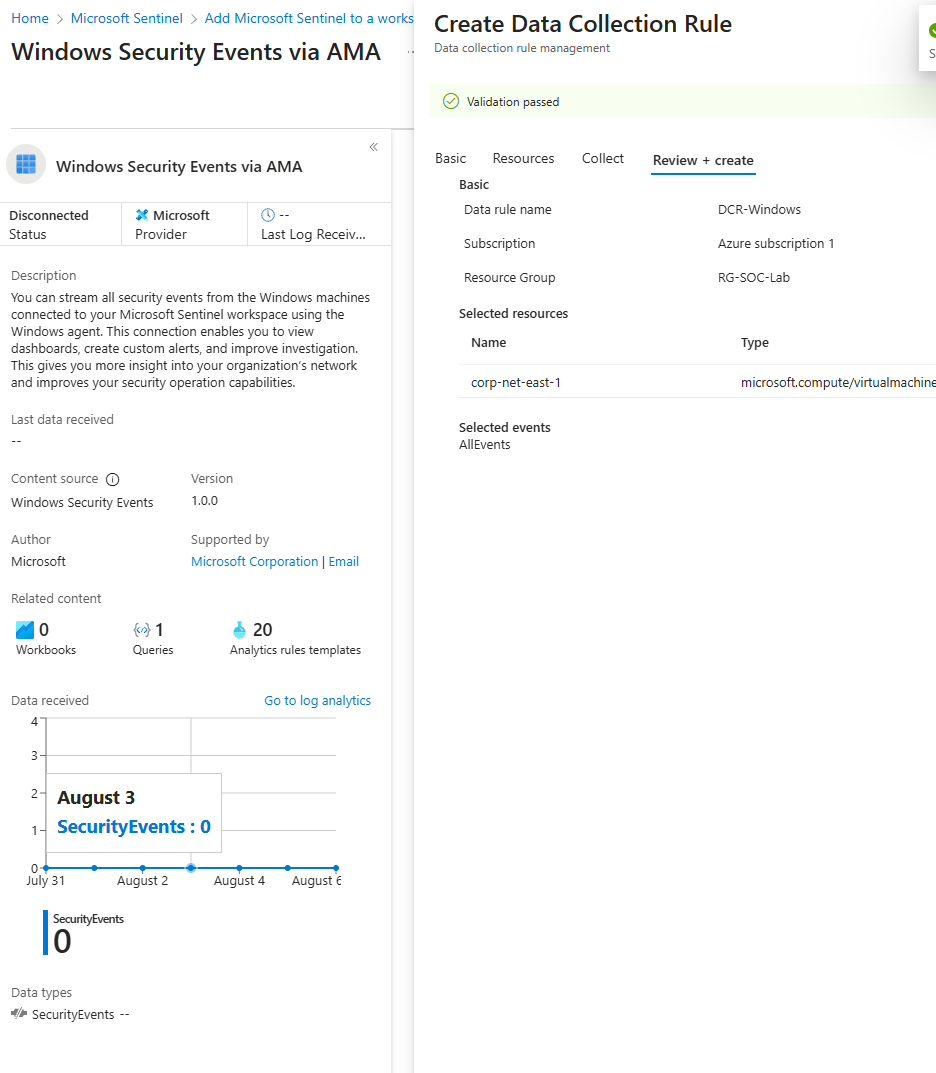
1. Microsoft Sentinel | Content hub - search “ Windows Security Events” and intstall it.



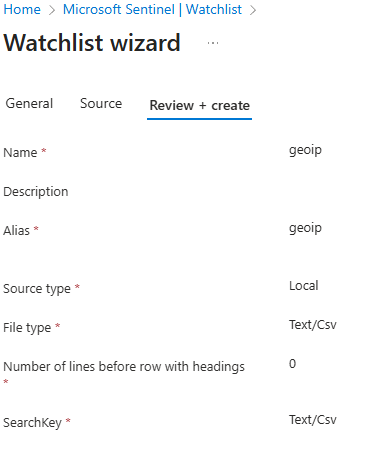
1. After done install go to manage . Select - Windows Security Events via AMA - Open connector page

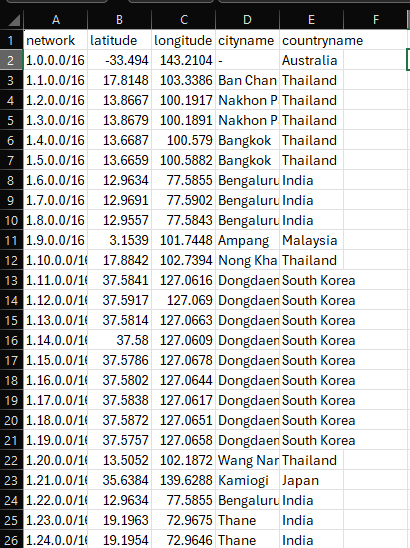


1. Create data collection rule

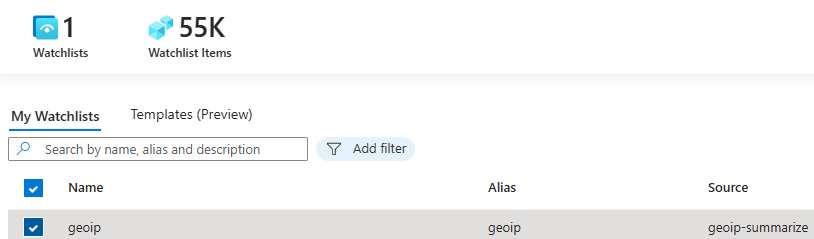


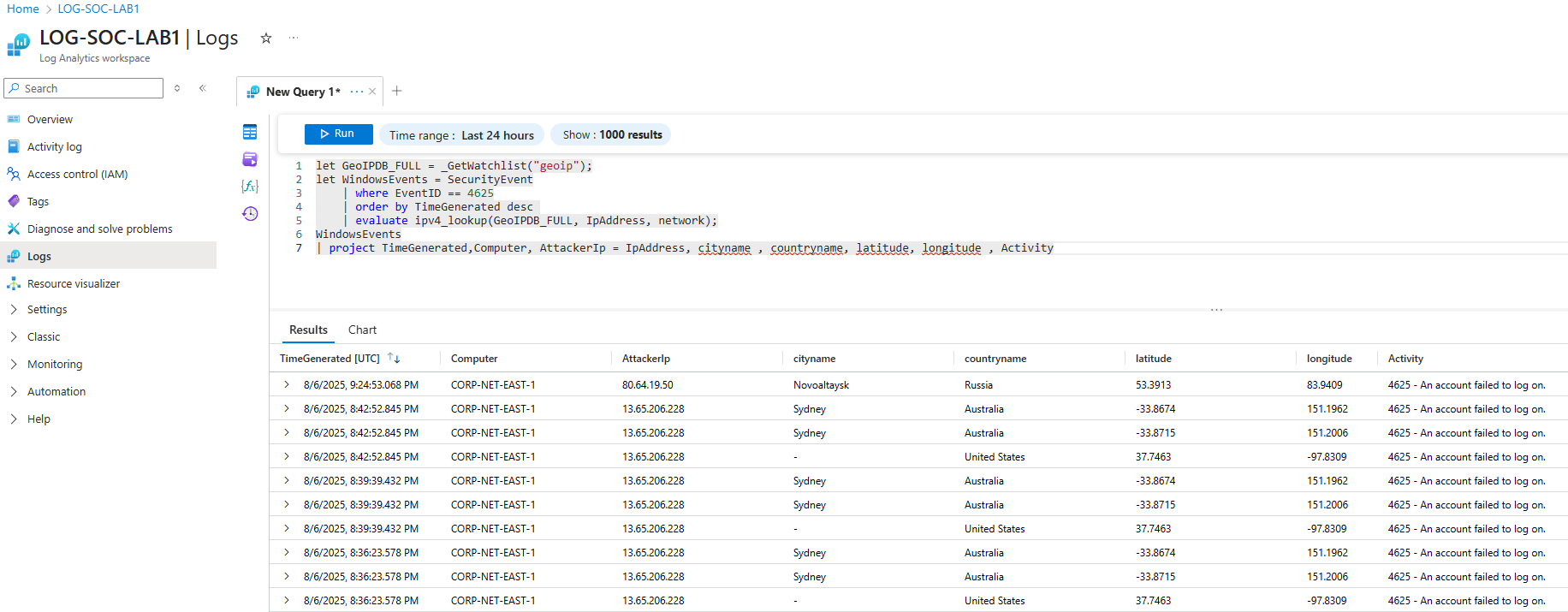
1. Go to Microsoft Sentinel - create a watchlist wizard and upload the geoip-summarised excel file for using the attacker IPaddress detect latitude ,longitude,cityname and countryname.

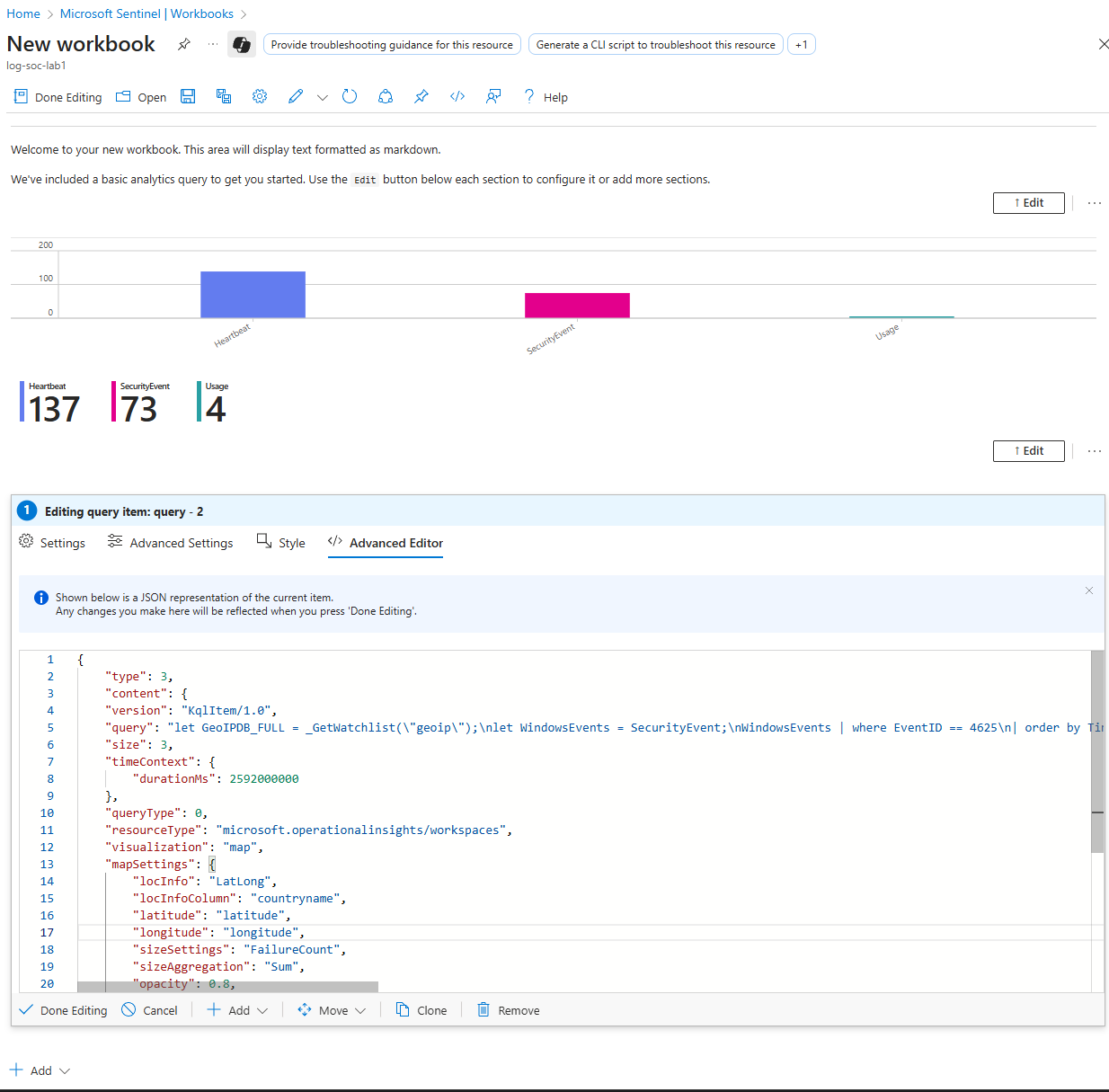




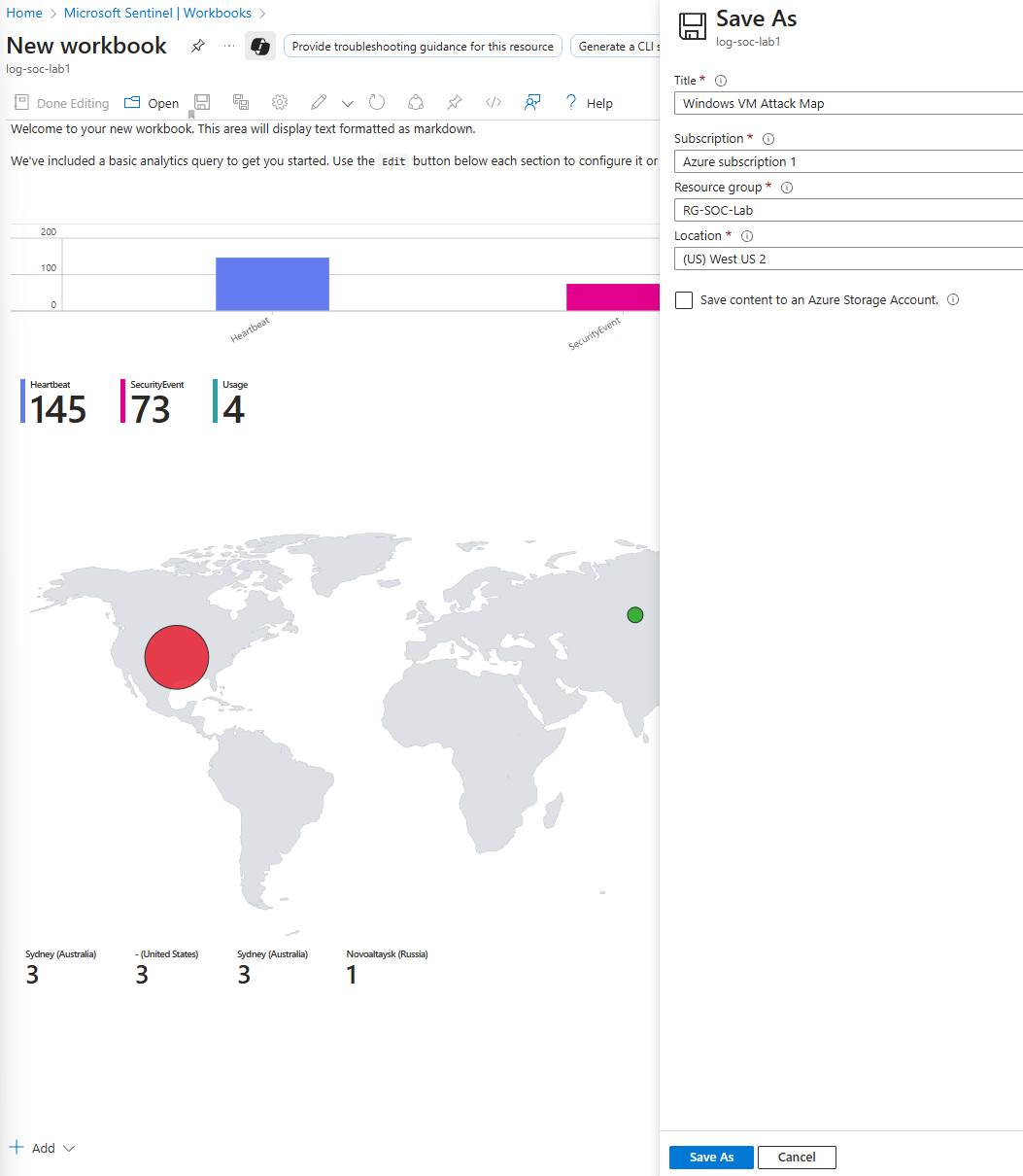
1. After finishing upload, you are able to see 1 watchlists and 55k watchlist items



1. 
2. Go to Microsoft Sentinel | Workbooks > Add Workbook > Edit > Add > Add query > select Advanced Editor > write the query to create a map



1. After Done editing you able to see a map locator Attacker from where. Then configure the title, resource group and save as.



1. This is a report after one day, with a total 6.58k attack to the VM.

