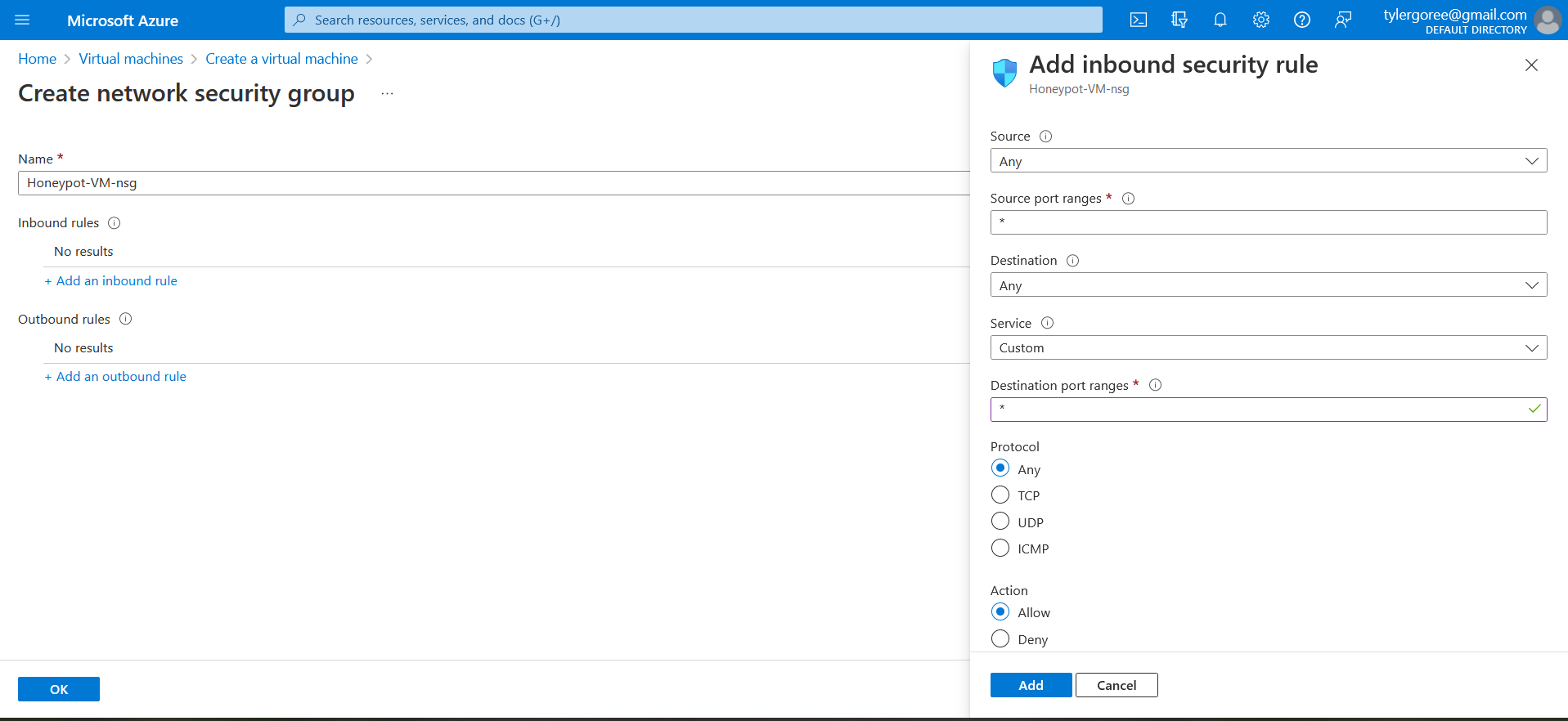
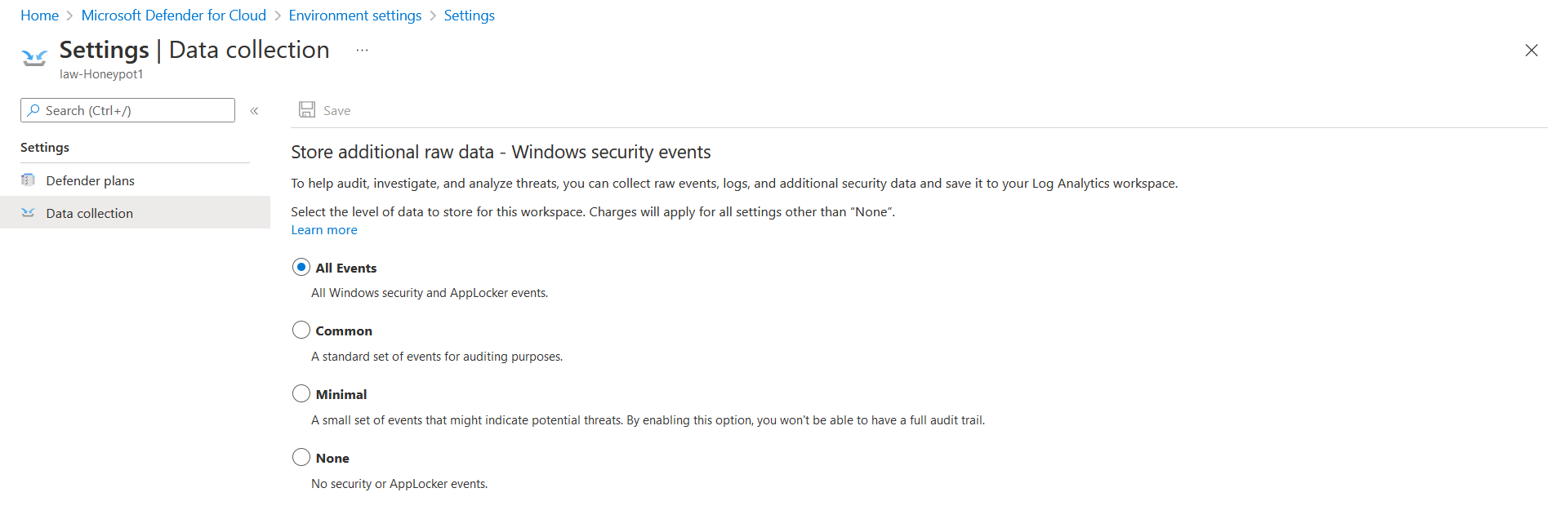
Azure Sentinel Viewing live cyber-attacks Lab

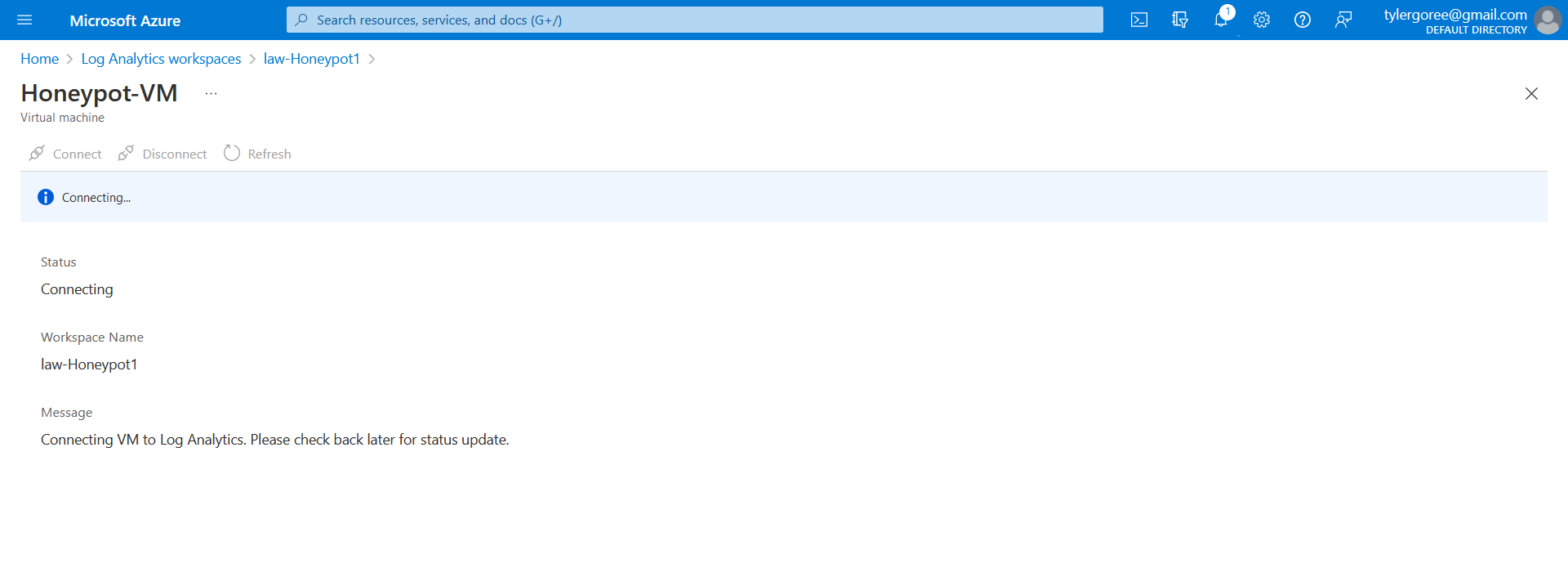
* Azure Sentinel is a cloud based SIEM/SOAR (Security Information Event Manager) Delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.
* To begin, I had to make an Azure account by going to portal.azure.com. Once account is made, I had to create a Virtual Machine and Resource Group that will be used through the duration of the lab, VM = Honeypot-VM Resource Group Law-HoneyPot1. (The resource group houses all your services related to your project)
* Note: Once Project is completed make sure you go back and delete the resource group so you’re not wasting your credits or racking up charges if your using pay as you go option.



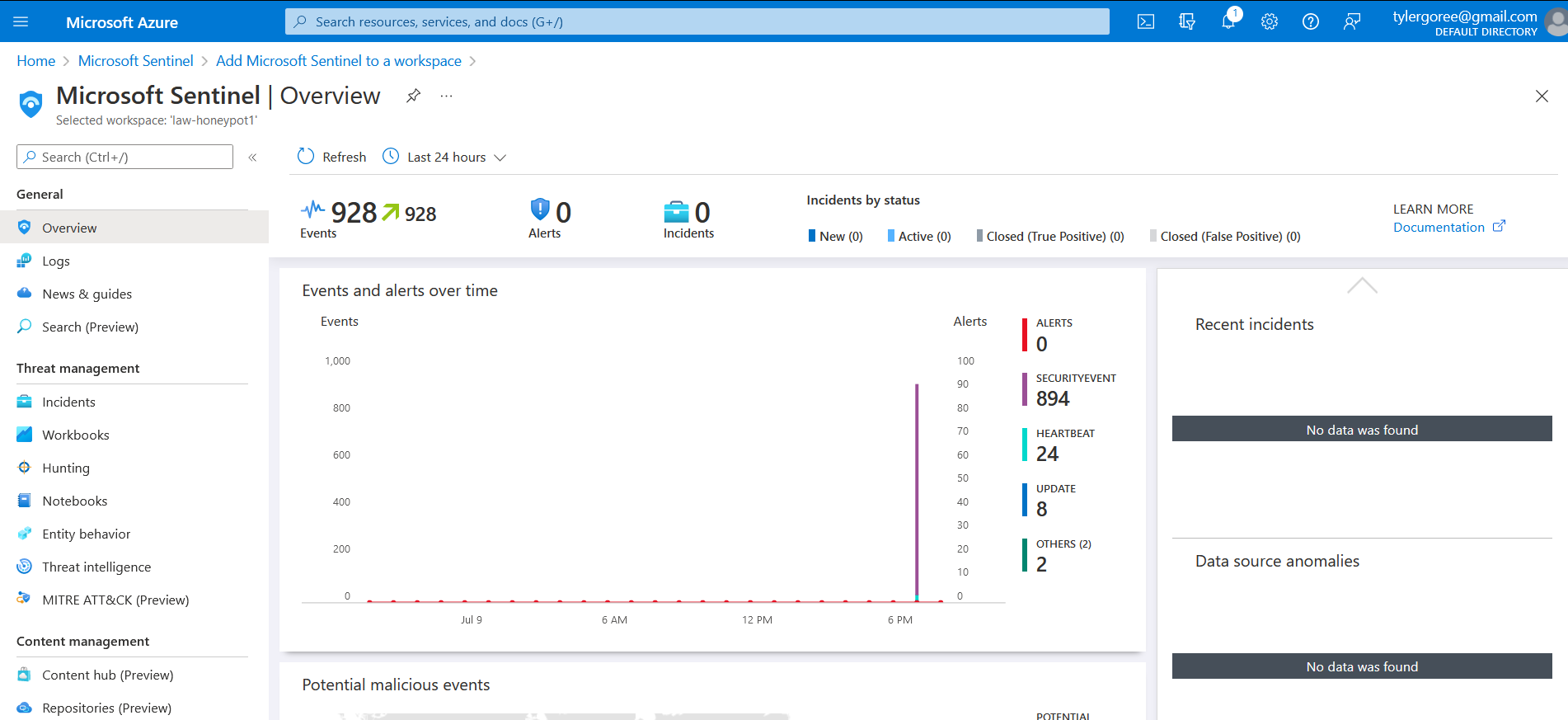
* Creating an NSG (Network Security Group), (Operates like Stateful FW Filtering Traffic and inspecting Inbound traffic, creating a table containing information such as: Source/Destination IP, Protocol, Port, Direction and Priority) that is used checked against returning traffic. The NSG we created should not be used in a production setting as this would be dangerous to you or your organization if applied, but for this lab purpose it works as the goal is to lure attackers into issuing brute force attacks so we can generate data of top countries carrying out malicious cyber activities.



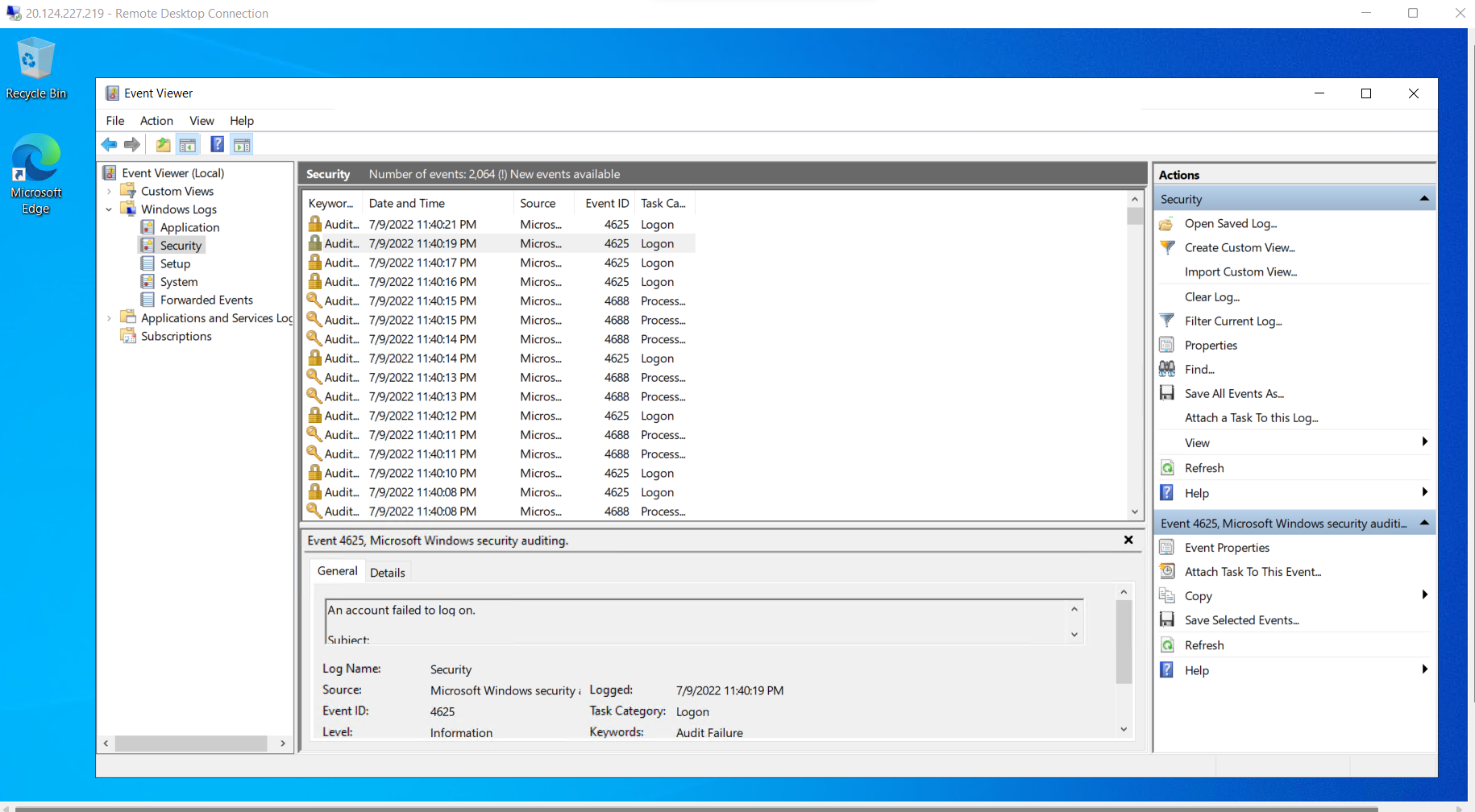
* I had to Link our Log Analytics log to Microsoft Defender/Security center so that it knows where to pull the security event data from
* Note: Log Analytics was created just every other service connecting back to our resource group we created in step 2.



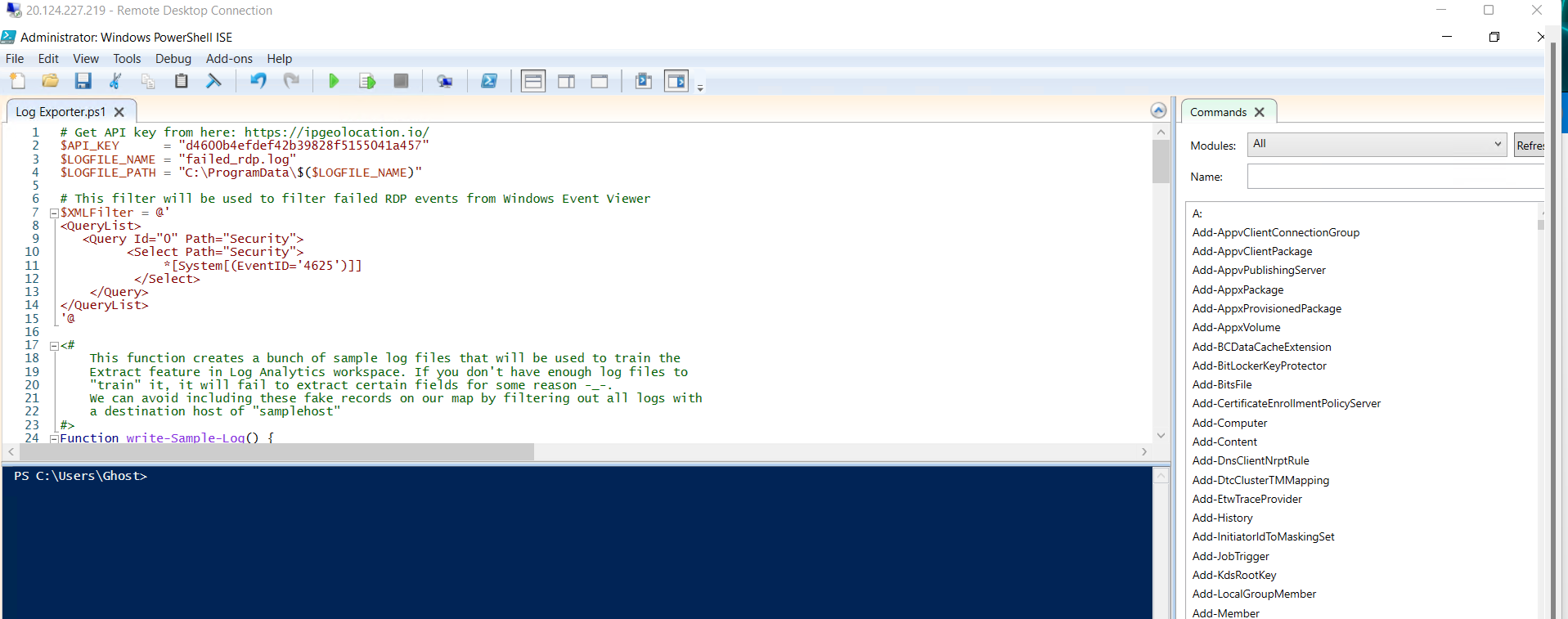
* Next, I had to connect my Virtual Machine to the resource group so that it can pull the logs from all activity occurring on Honeypot-VM. This can take some time to fully configure throughout all connected services.



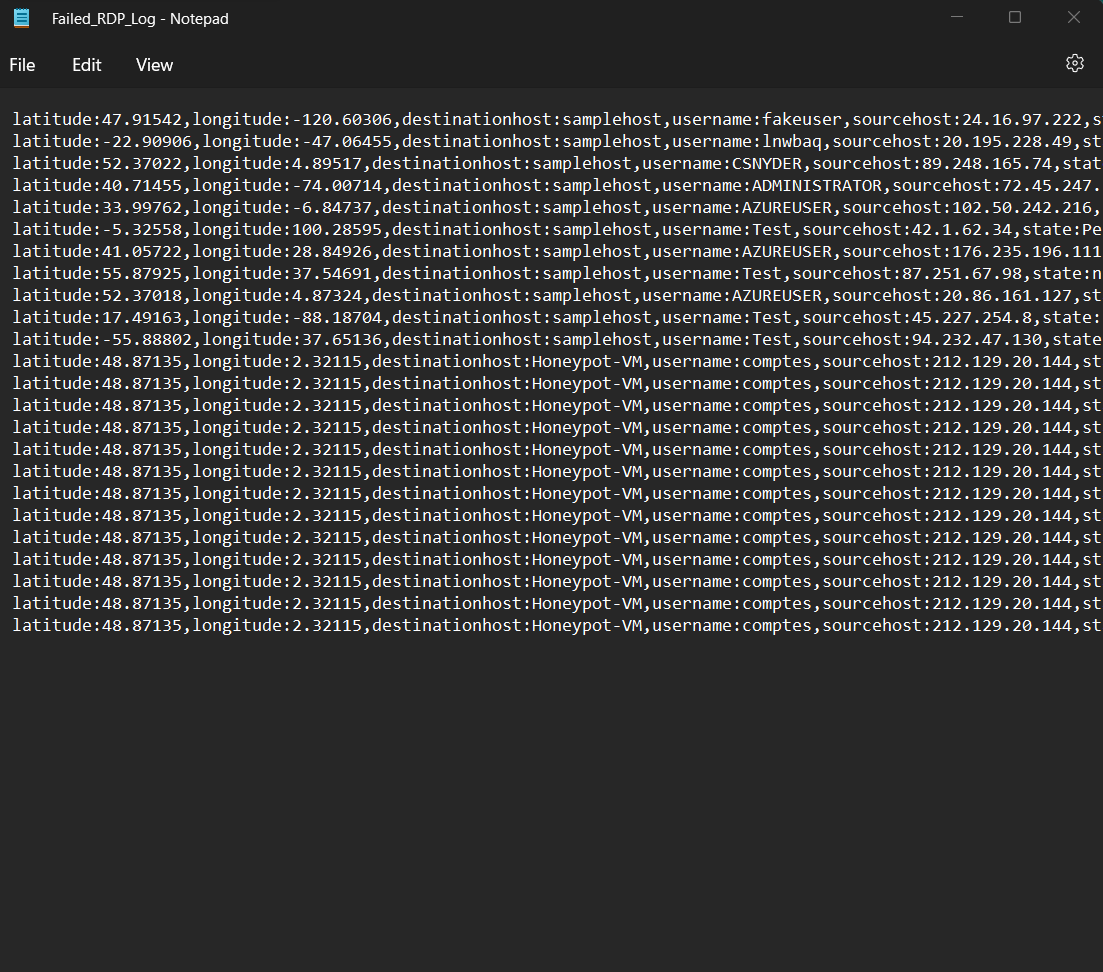
* The above image is the Microsoft Sentinel home display showing some stats pulled from the connected log analytics service. Analyzing just this home page we can conclude that there have been 928 events discovered. Among those 928 894 is security events. You can go deeper looking at the incidents, MITRE ATT&CK map viewing different threats and techniques that occurred during incidents.



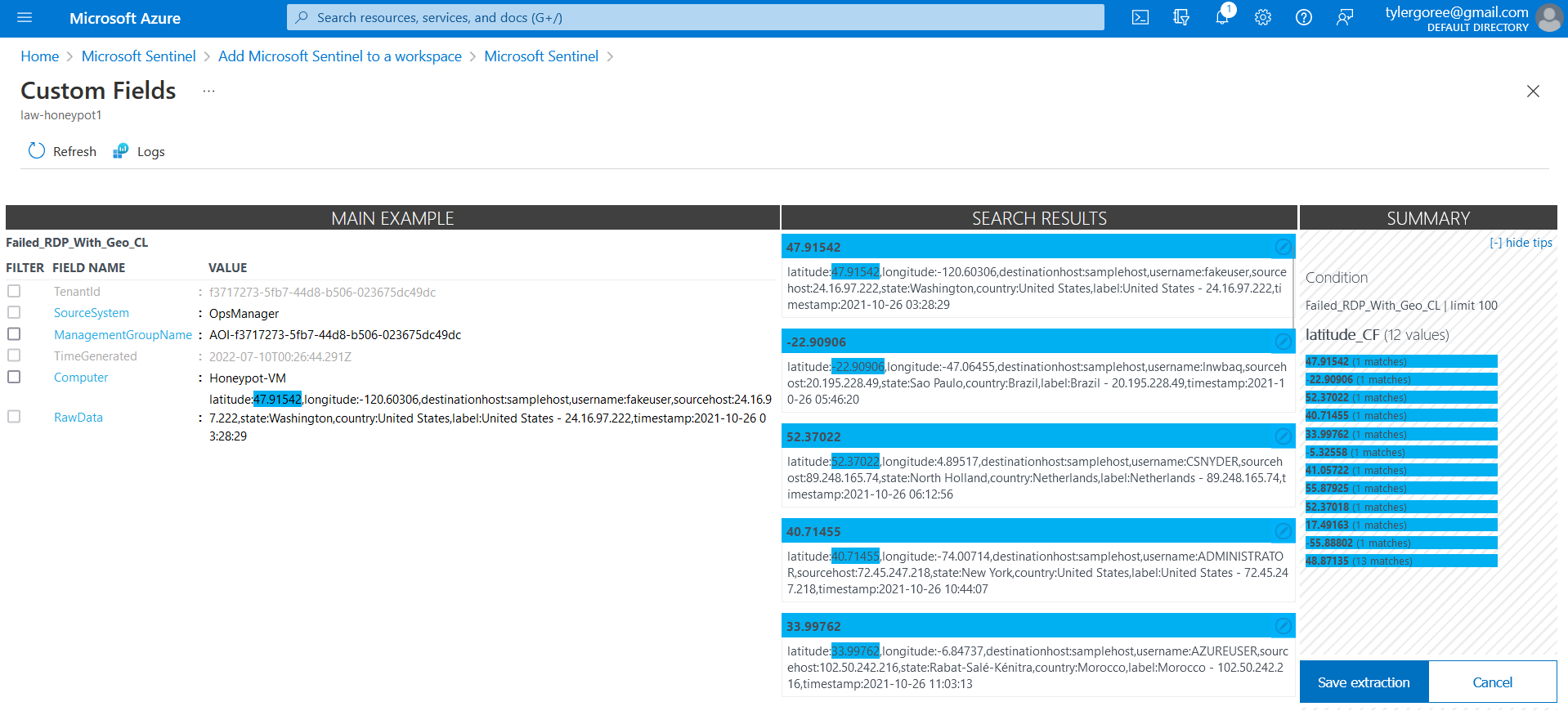
* Using Remote Desktop on my Production Machine in order to login into the Azure Virtual Machine Honeypot-VM (You will use the Public IP and Creds of the VM). I am logging in to view the windows event security logs to see what kind of activity is taking place in order to establish a baseline before I set it live and discoverable.
* Note: If you are unsure on what your VM IP is you can locate it by going to your Virtual Machine on portal.azure.com and looking at the overview page.



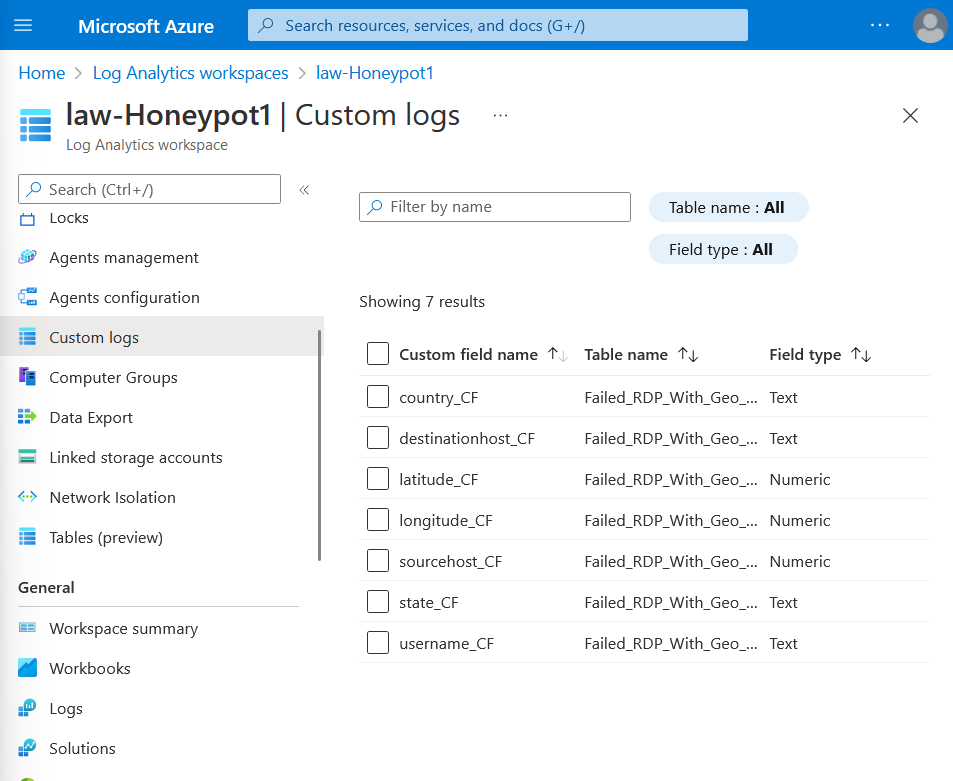
* Downloading pre-configured Power shell script using windows PowerShell ISE to pull geo location data.
* Note: In order for the geo location to work properly I had to get my own API key as using someone’s else may result in security issues and you won’t be able to continue. To get this key I had to go to the following website https://ipgeolocation.io/ to register then I was provided with the necessary working key.



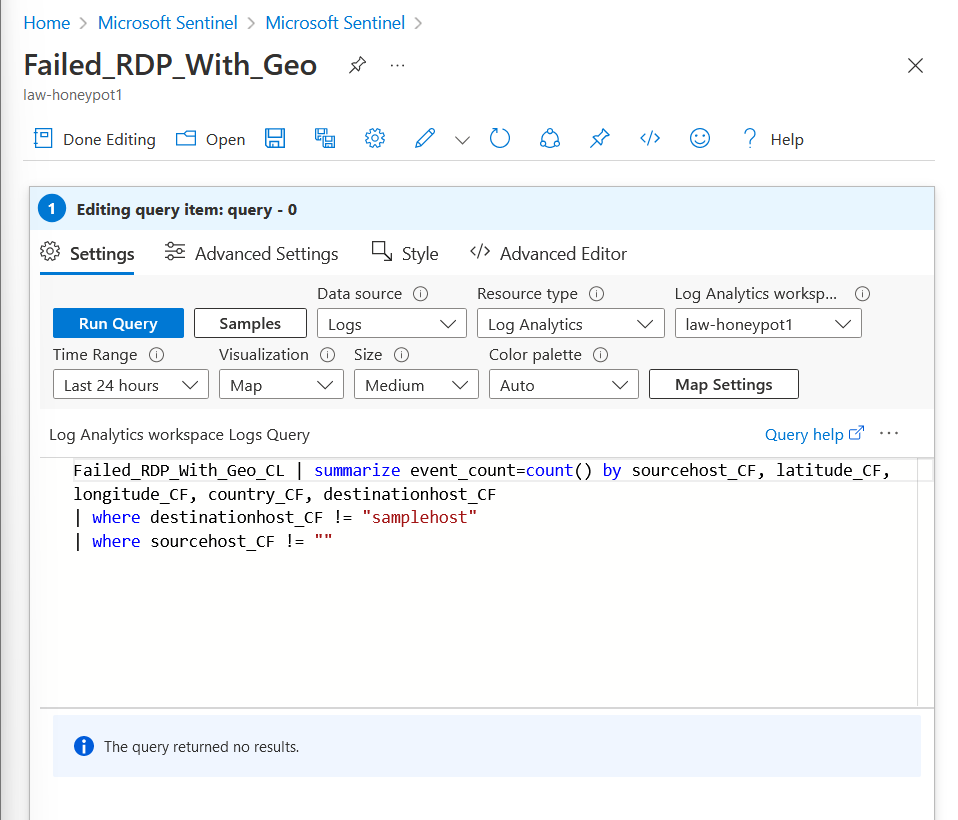
* I used the output above to create a template in Microsoft Sentinel in order to get the application trained/programed to look for and gather the necessary information. Note: The word file must be stored on the machine your configuring Microsoft Sentinel to pull from
* Note: Creating the custom log in Microsoft Sentinel appears to successful right away, but its deceptive in the fact you have to allow it 10-15 minutes to link up with the other services attached to it such as Log Analytics
* After the link is completed across the border and you can then successfully run the script. It should populate log entries that your going to use to generate the field data for the report and geo map if your using one.
* Extracting that field data is started by choosing any entry right clicking and selecting extracting data.



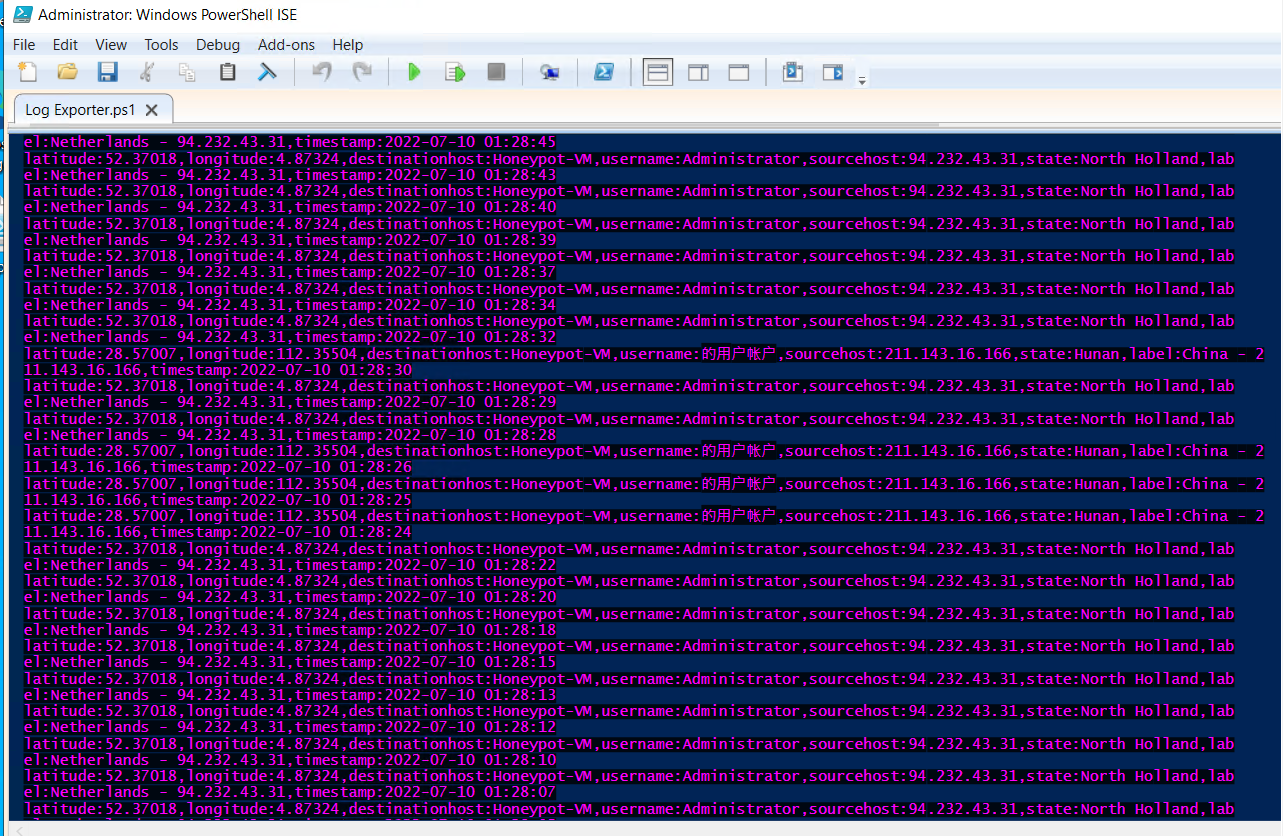
* From this view I had to start collecting my field data, which I found to be a little tedious. This process begins with you selecting the item field data (47.91542) not the field name by highlighting it. A pop window should appear so you can provide the field name and field value.
* Analyzing the search results for success and accuracy to be achieved. If it is, the you just hit Save Extraction and repeat the steps till you collected all the field search material.
* Note: When going through your search results and you see inaccuracy the following manual steps must be achieved: Go to the incorrect field data and highlight it, another pop-up window should appear input the correct field name and value and save extraction and repeat all over.



* When completing the extraction field search data list, you can verify the list by going to custom logs and them choosing custom data. If your results come in with inaccurate information you can delete the field and redo it again.



* Going back into Microsoft Sentinel I am needing to create a new workbook that will use following query. The Query function pulls the selected data and stores it into map or if your having problems with viewing your map or your map won’t display you can always analyze the logs



* In conclusion, I was having problems displaying my geo map, but I was able to analyze the event logs. From the event logs I can conclude that among top suitors for malicious activity/ attempting to brute force my Virtual Machine is coming from China and North Holland.