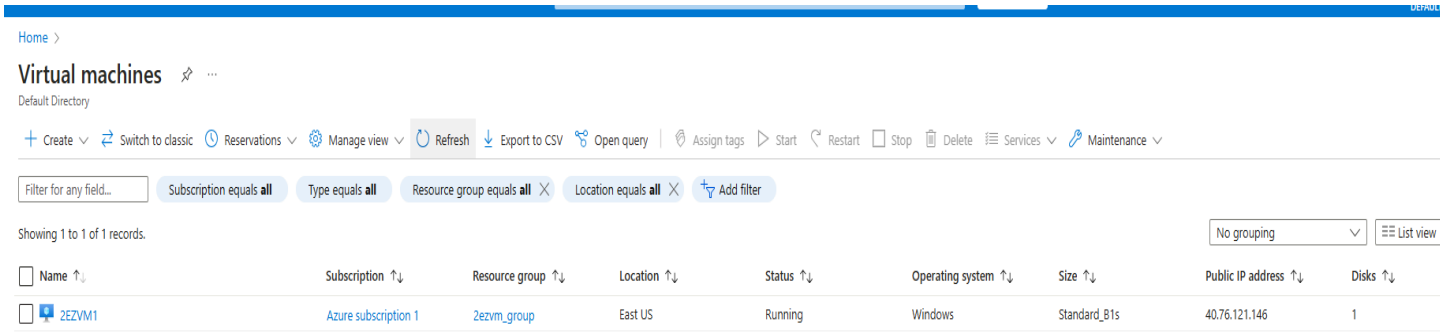
Deploying My Own SIEM

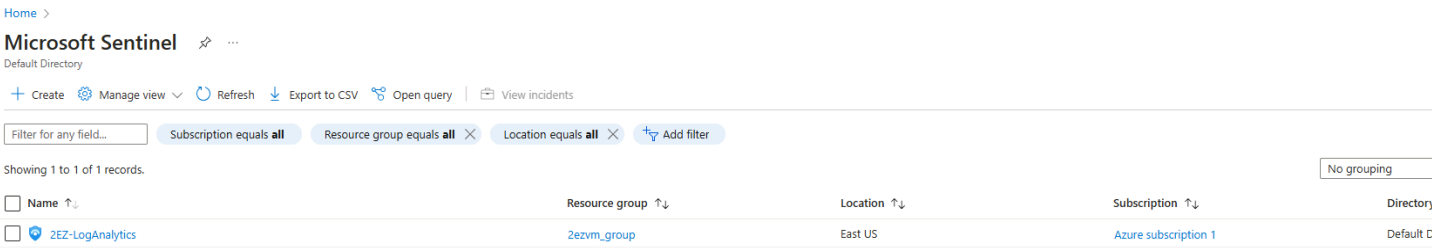
In this project I used Microsoft Azure to create my own SIEM. I used Azure because they give you 200 free credits (Which will usually not get you far) but it was plenty for this project.

After I signed in and gave them all my personal information, I began to set up my first virtual machine. I chose to use the windows 10 pro version, named it 2EZVM1, and added it to a Resource Group called 2EZVM_Group. This Resource Group acted as the container for everything in this project.



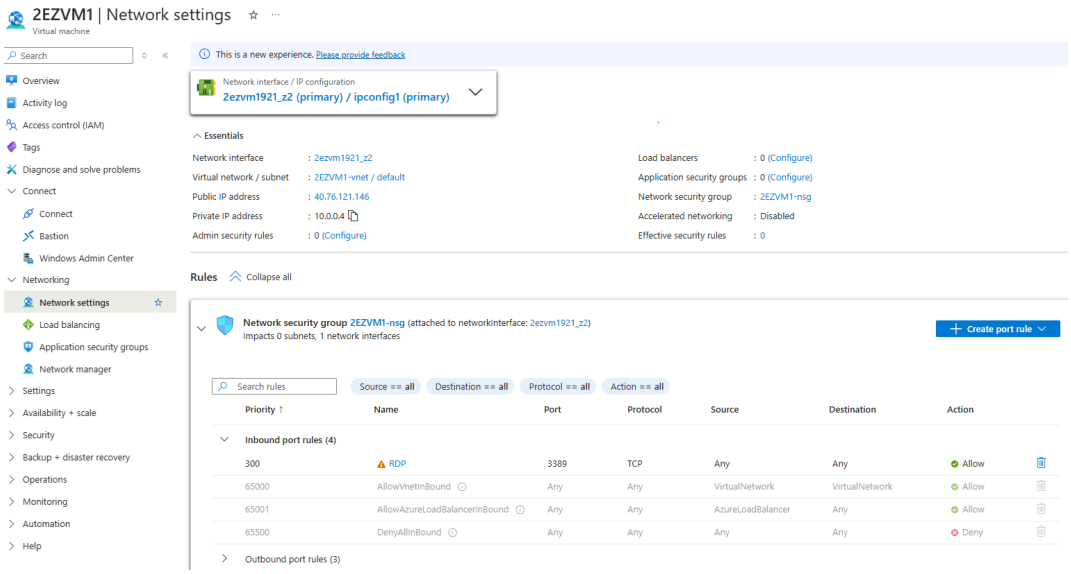
In this project, I allowed the RDP port 3389 to be public because it's very easy to get traffic on this port. This increased the volume of attempted connections which allowed me to detect more security events later in the project.

Next I began to set up a log analytics workspace called 2EZ-LogAnalytics.

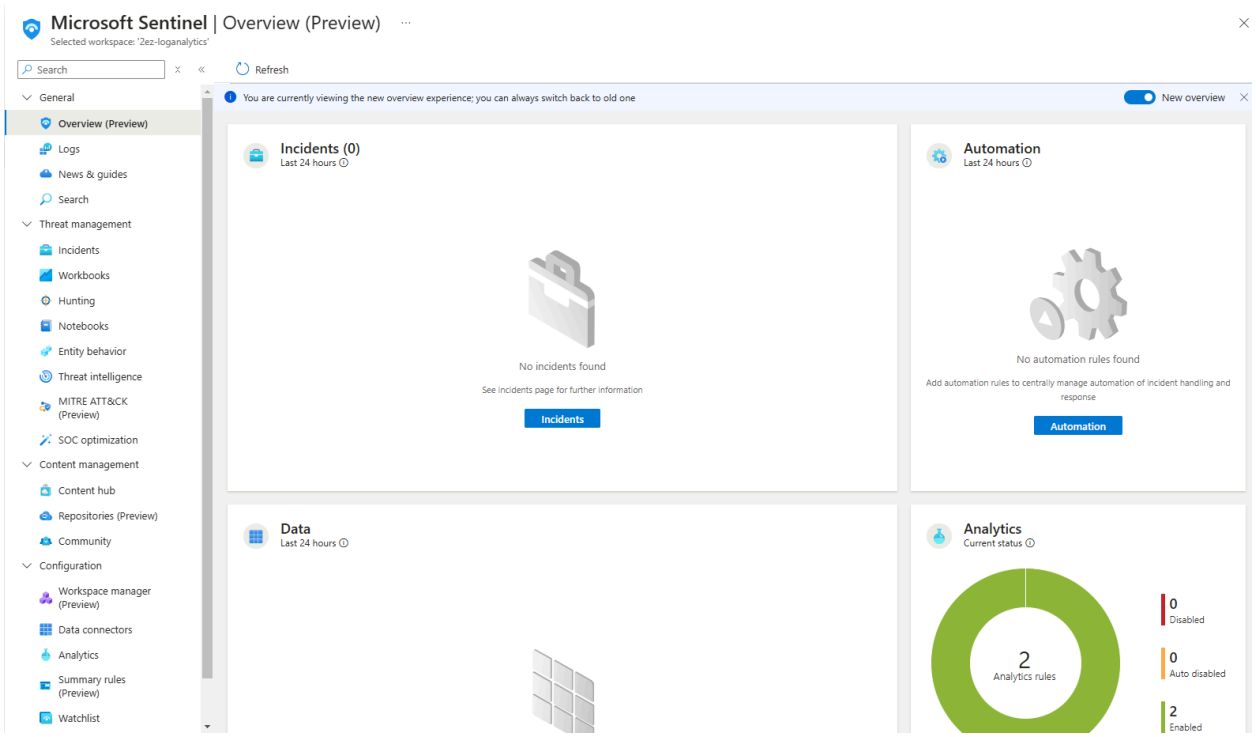


I added 2EZ-LogAnalytics to the resource group that 2EZVM1 was placed in. (2EZVM_Group)

Next, I went back to the VM workspace and navigated to the network settings panel to see if the VM was public facing and receiving traffic. And BOOM! I was already receiving hits on the RDP port.



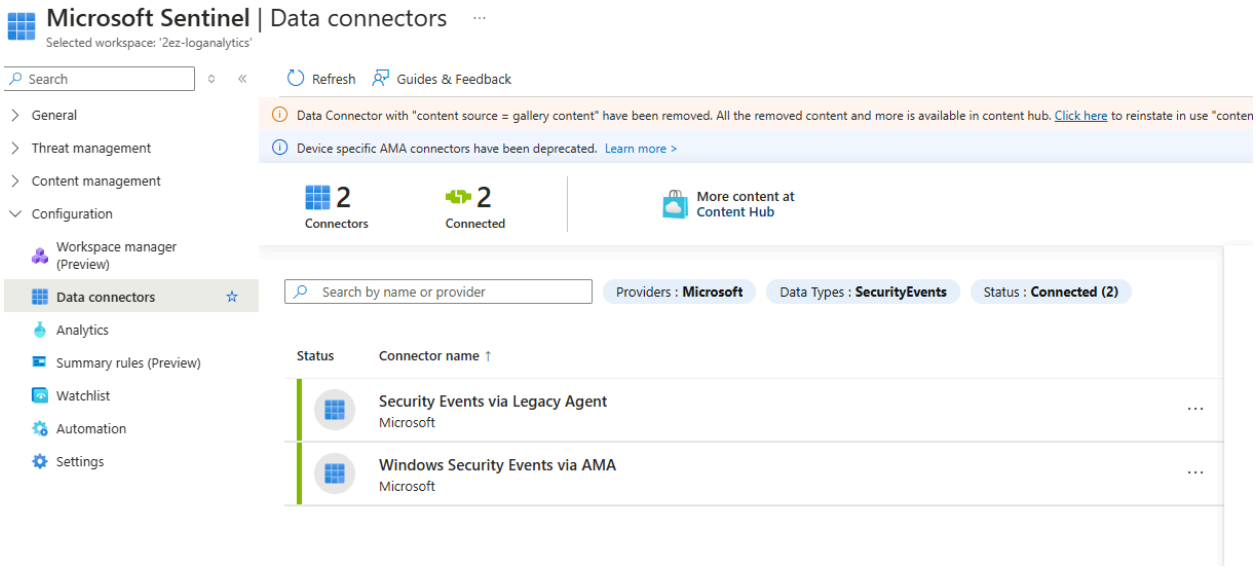
After checking this, I added Microsoft sentinel to my LogAnalytics workspace.



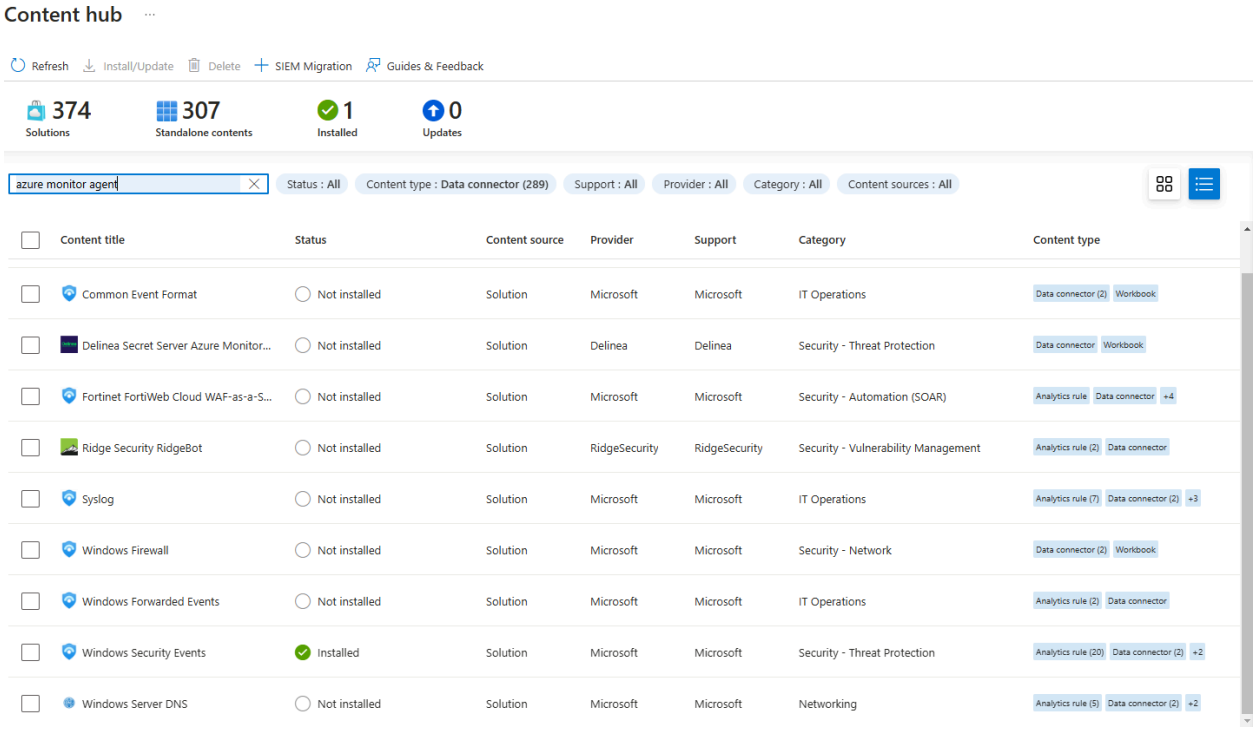
Next, I headed back to the LogAnalytics workspace (2EZ-LogAnalytics) to add the VM's event logs and send them to the Sentinel instance.

To do this I went to the Data connectors tab. In the image below I have already installed the *Windows security events via AMA* and *Security Events via legacy agent*. I used *Windows*

security events AMA because the other option is being phased out.

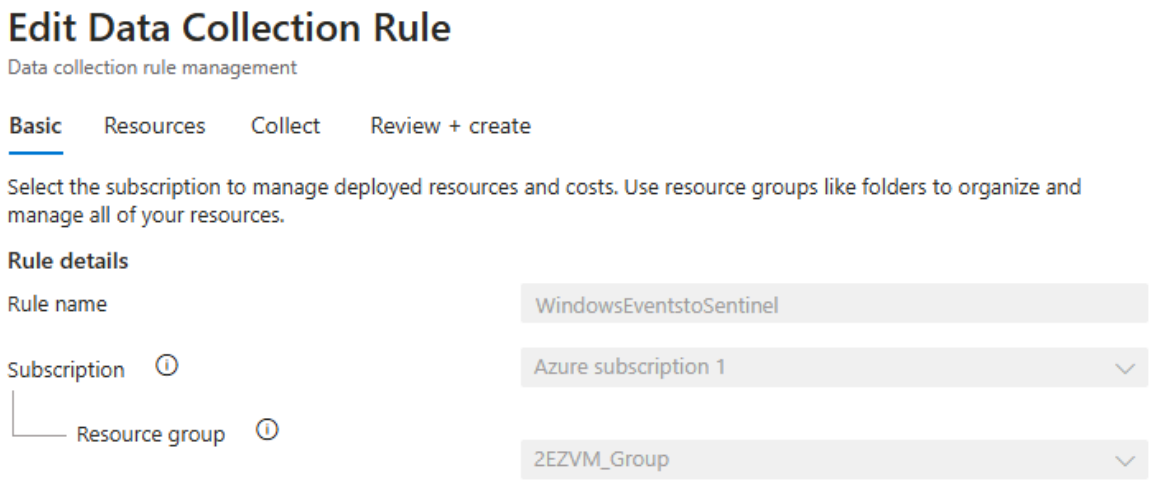


The image below shows the UI after you click into the content hub to find the tool you're looking to install.



After this was installed, I created a new data collection rule seen below within *Windows security events AMA.* I then added a rule name and the resource group for the data collection rule. In the resources tab I selected the 2EZVM which also selected the group and subscription for me.

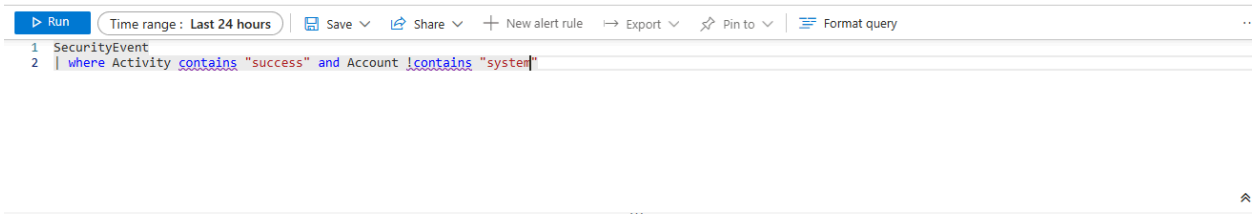
I also



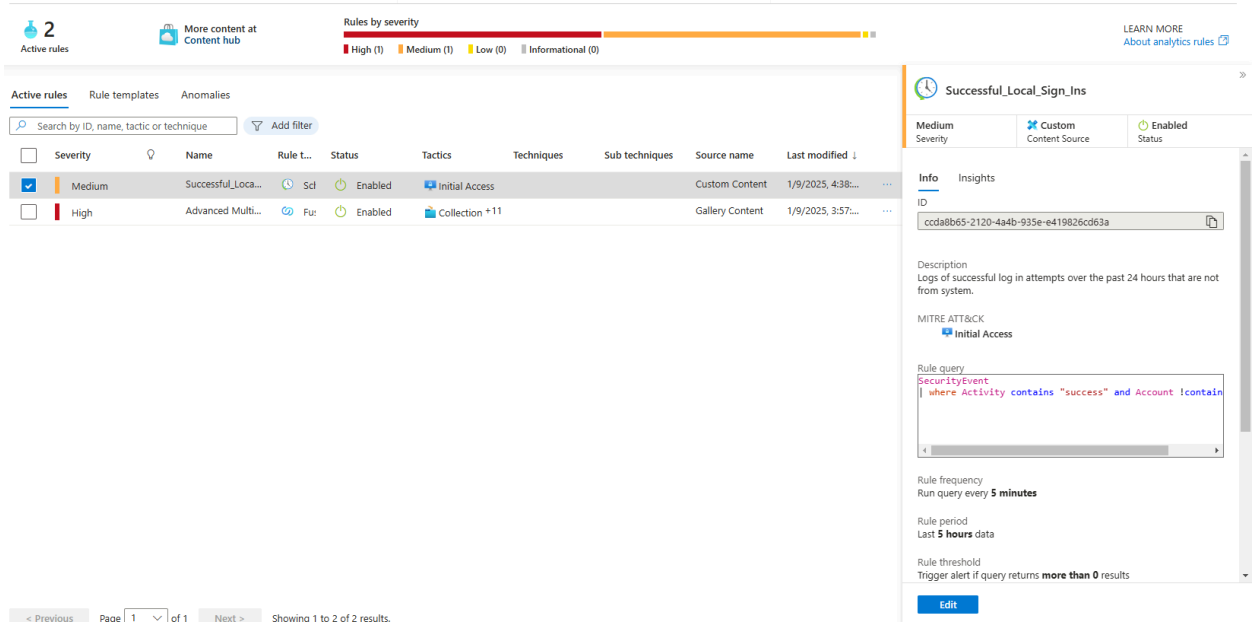
I also created a rule in the collect portion of the data collection rule to return all security events. After this I began receiving logs.

Next I wanted to create a Sentinel rule to detect successful login attempts via RDP from users that we're not a system account.

For this I navigated to the Logs tab in the sentinel workspace and created a new security incident query seen below.

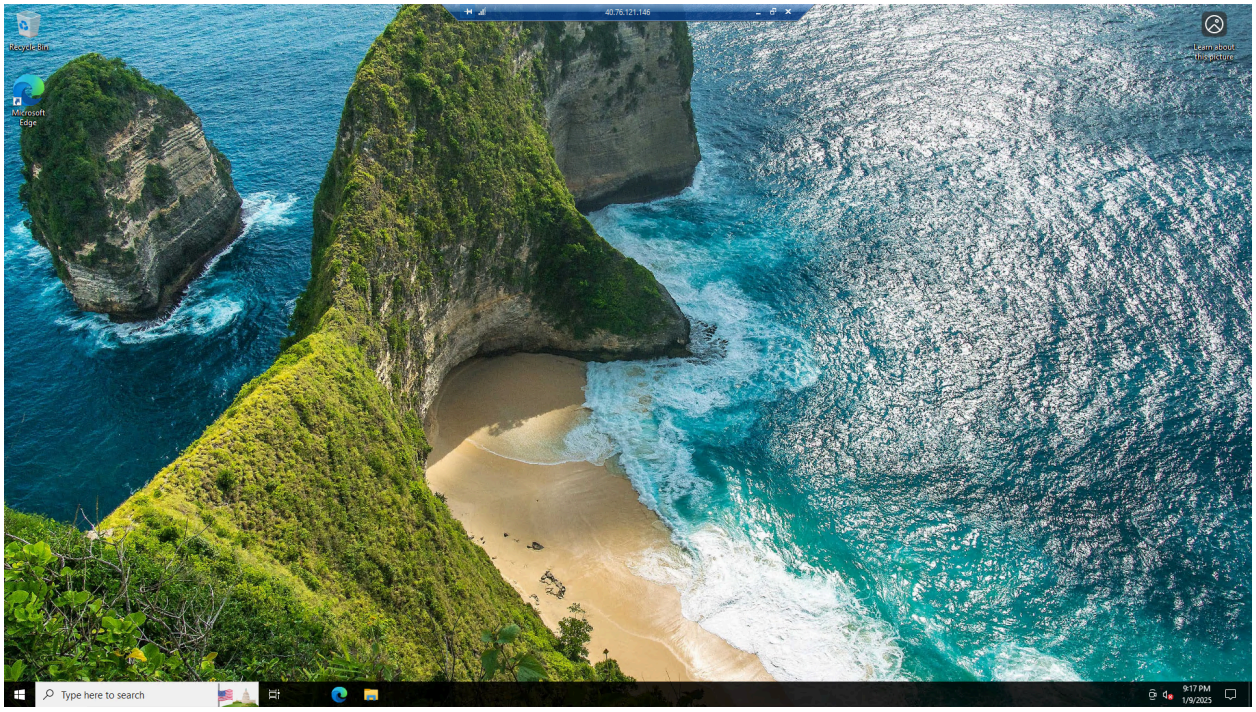


After this, I went to the analytics window to see my new rule. You can see in the image below my rule is the medium level incident.

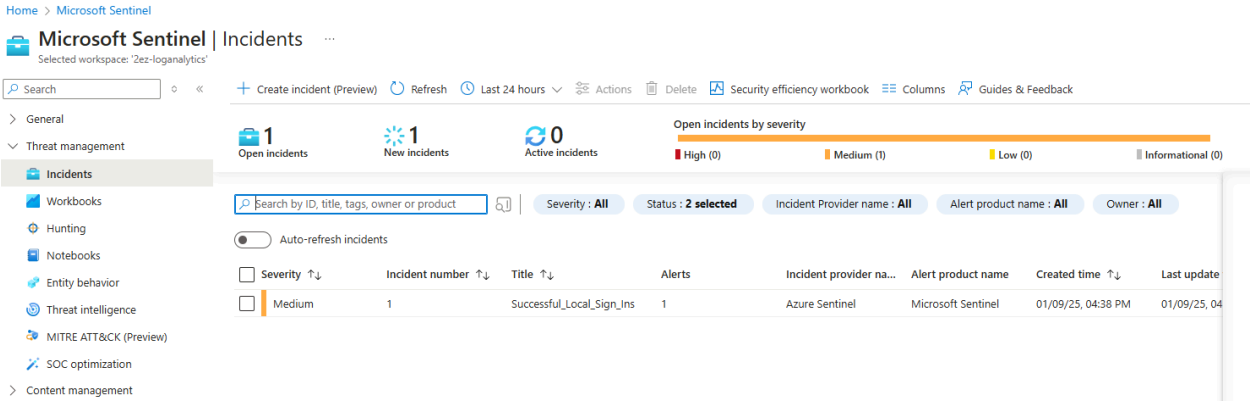


.

This was set to run every 5 minutes so I went to log in myself to test the rule. Below is me logged into the VM successfully.



To check if this triggered an alert for my rule, I then went to the incidents page within sentinel and boom, the alert was there.



This project gave me plenty of insight into how to set up not only a virtual machine, but also how to use the tools within Azure to monitor activity on an endpoint. In the future, I plan to do more projects like this to extend my knowledge of this ecosystem. Unfortunately, this will cost money as my free trial will run out of credits soon. So if you'd like to see more projects like this please hire me!