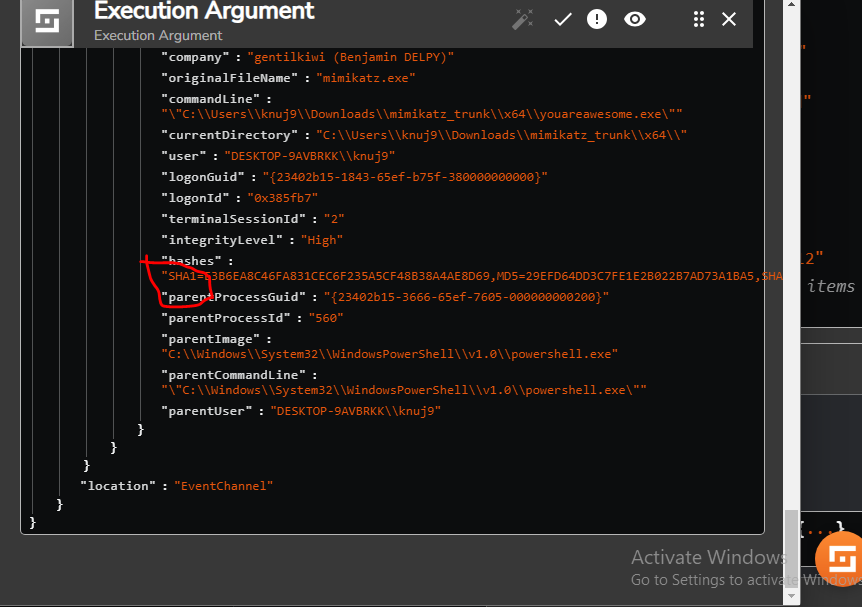
We will have our mimikatz alert be sent over to shuffle, shuffle will then take that and extract the file hash from the file and then check virus total reputation score and then send that over to the hive to create an alert and then email that alert to the SOC analyst.

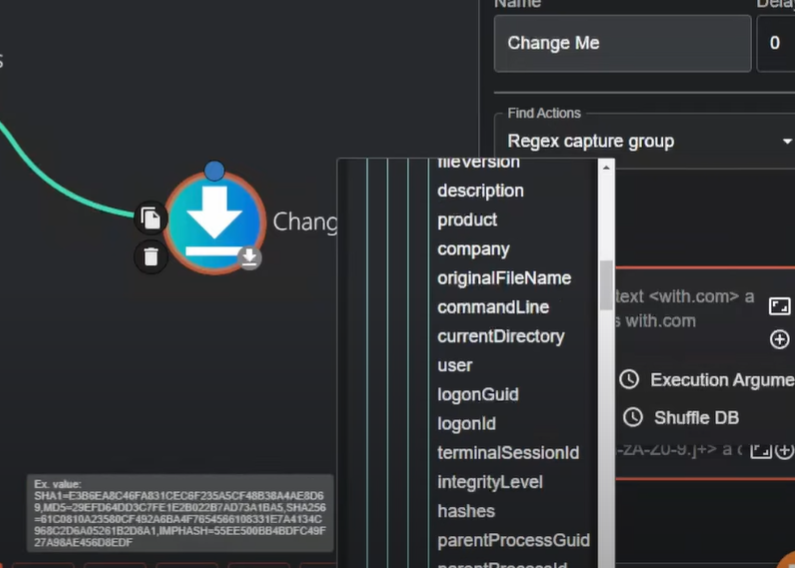
Further investigation when we look at our return values for the hashes, we notice that it is appended by their hash type. In this example SHA1= . If we want to automate this, we will have to parse out the hash type otherwise Virus total will not be able to evaluate the hash value.



Exit that and select our Change Me.

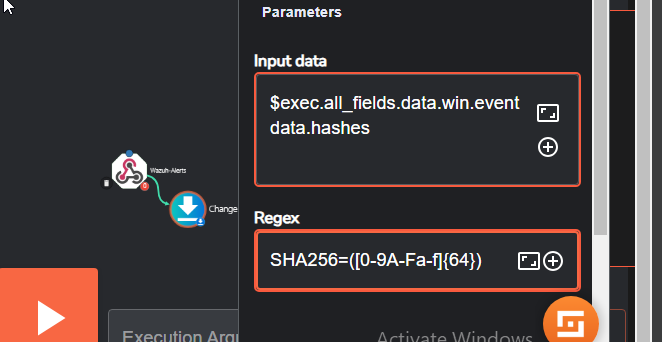
Change Find Actions to Regex Capture Group

Add Execuation Arguement and hover over the options and itll show you the values like our hash here

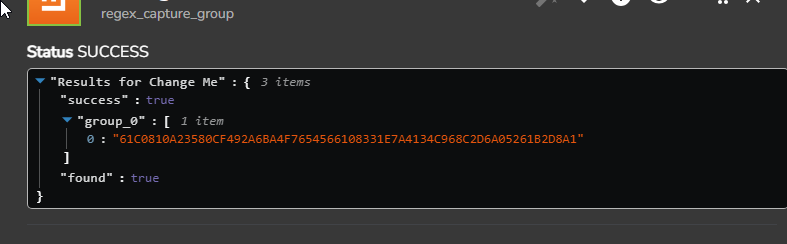


Select hashes and it will populate the input data.

Then create a regular expression that will parse the SHA1 out of the hash. Regex is not my favorite

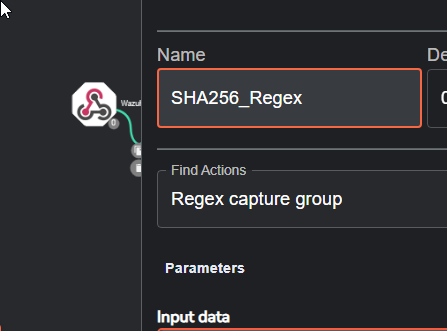


Save and check out the change me log and you can see the hash was successfully parsed

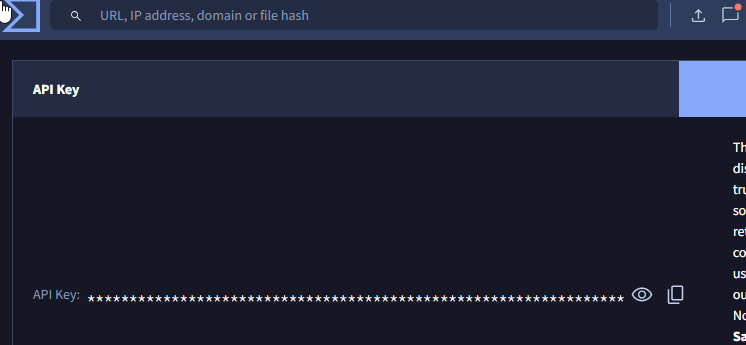


Now we can set this up to automatically send this to VirusTotal and check the reputation score.

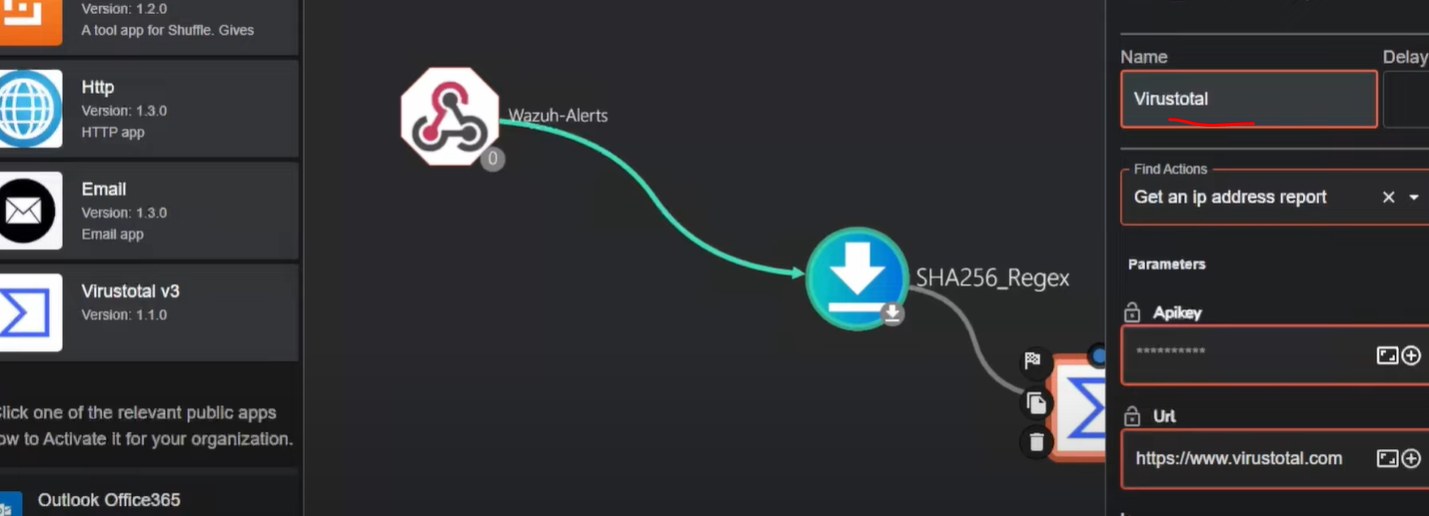
Im going to change “Change Me” to “SHA256\_Regex”



Need to head over to VirusTotal and create an account in order to utilize their API

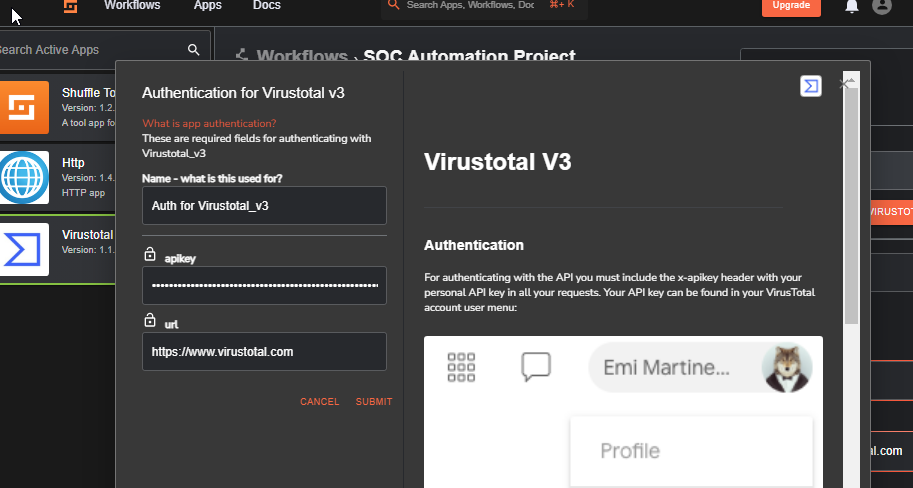


Go back to shuffle and select apps. Find Virus total and drag it into your workflow. I will rename it VirusTotal

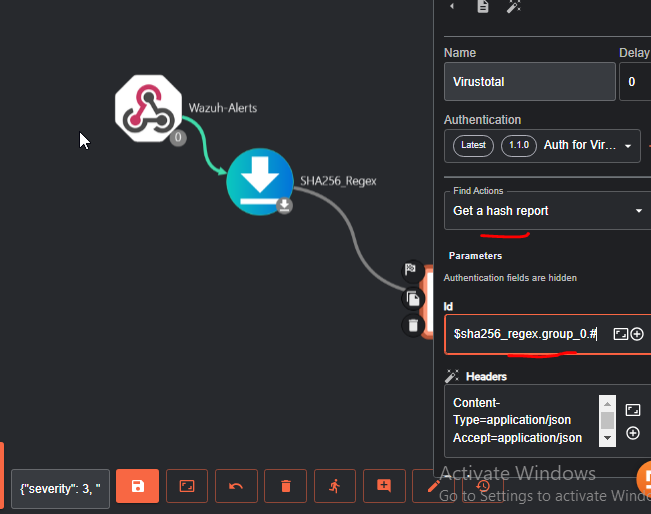


I am going to authenticate with Virus total and add my API in there. And submit.

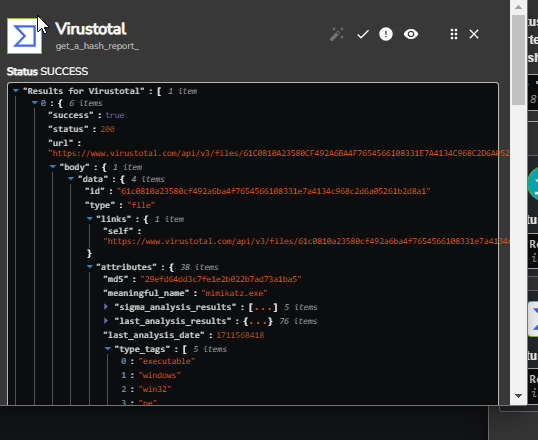
After that I was to go to Find Actions and Select Hash report

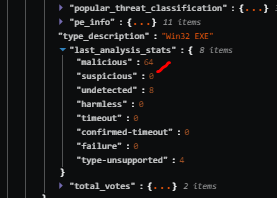


Next I will set the ID to point to the Regex list we made



Save Select the middle workflow and rerun workflow

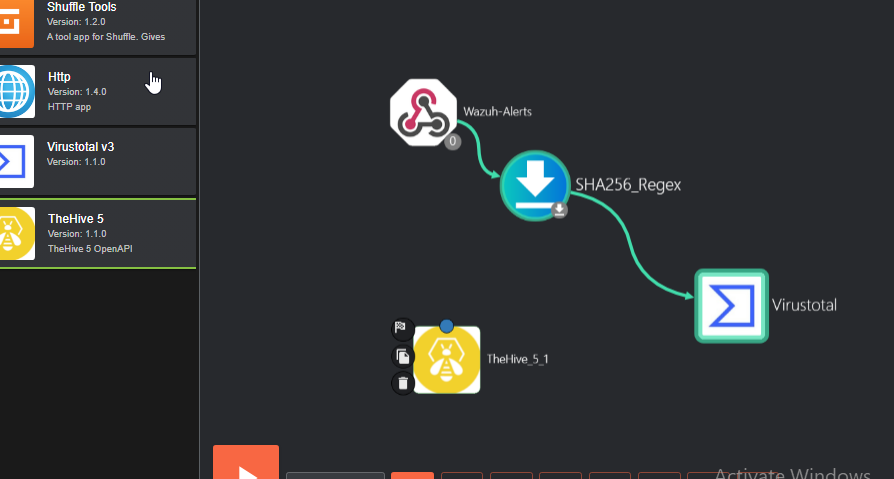




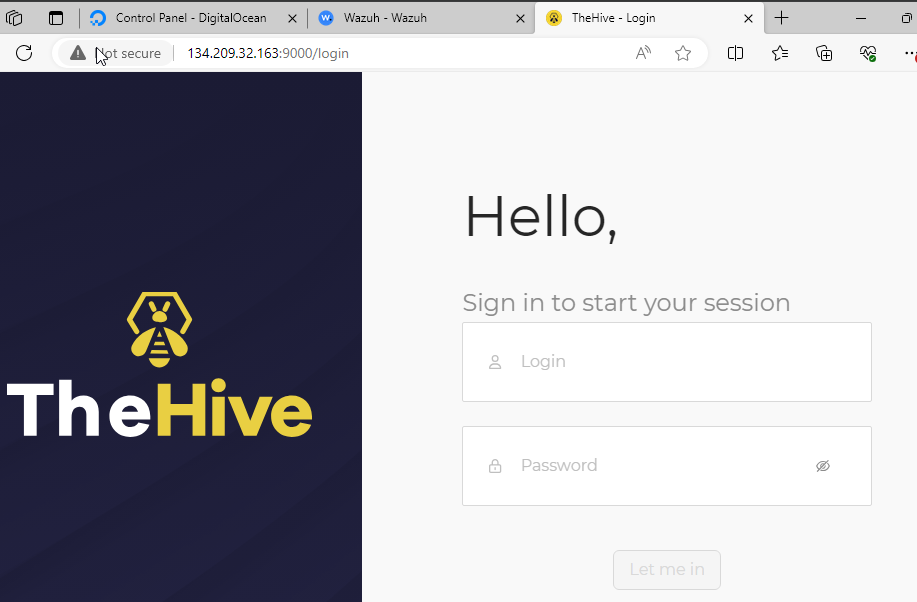
We can see the hash had 64 scanners record it as Malicious .

Next we will send the details to TheHive so TheHive can create an alert for case management

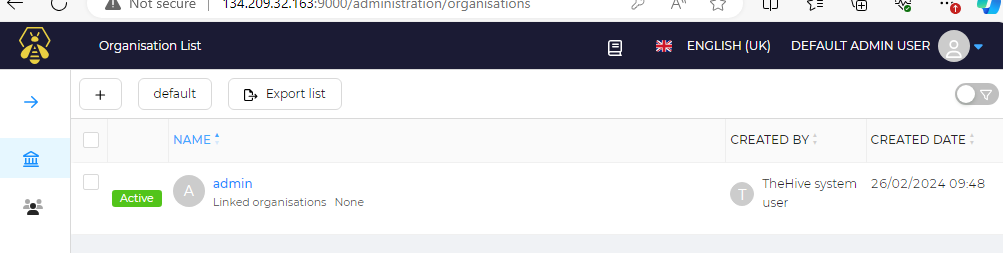
Find thehive app, activate it and drag it into the workflow



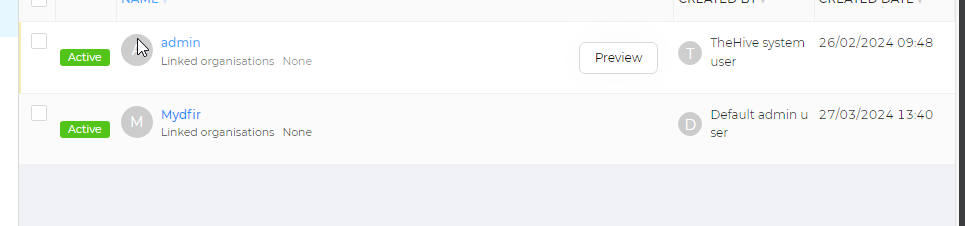
Login to TheHive (remember its the public IP and port 9000)



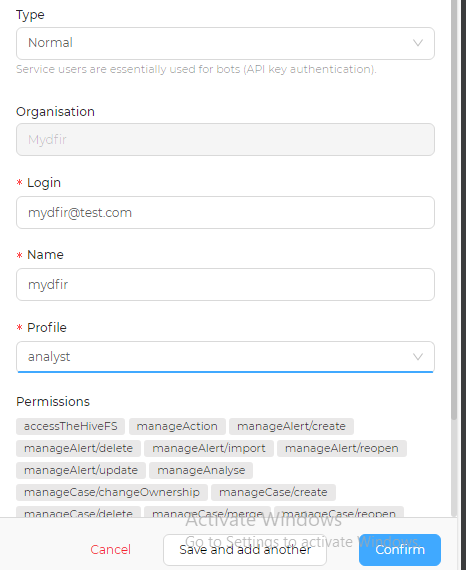
We will then create an organization and a new user for that organization

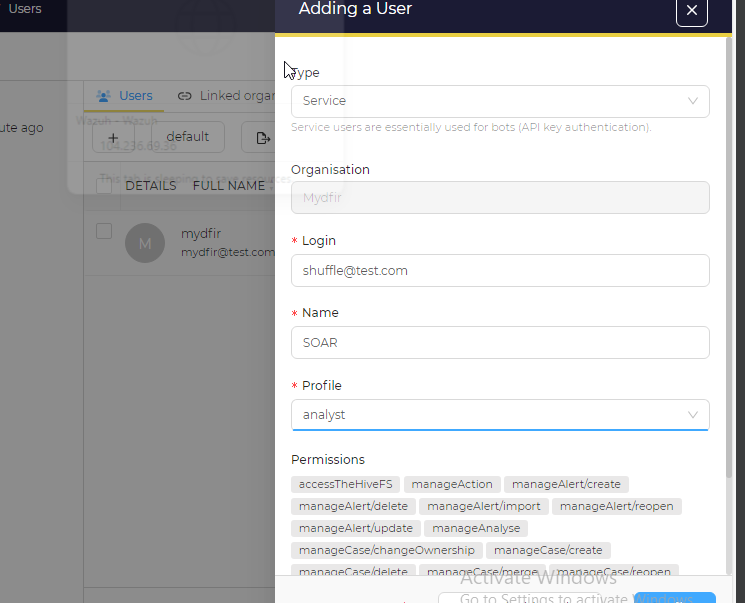


Name of organization is Mydfir



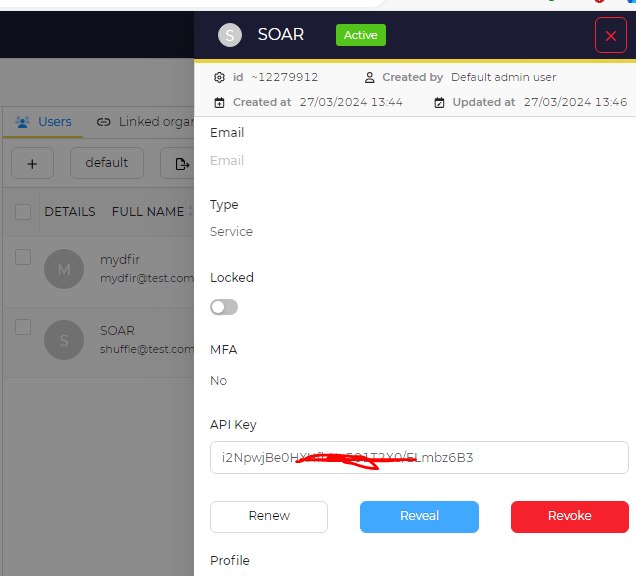
Then we can add 2 users





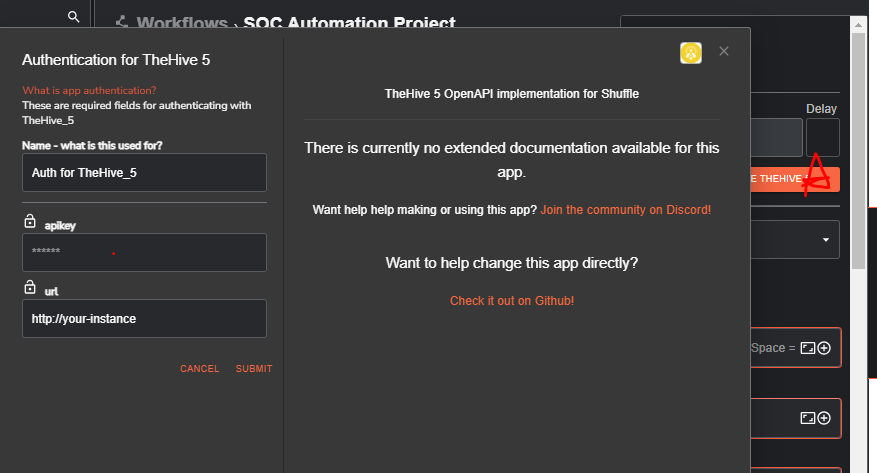
This second user I chose service and keep in mind with any new user please use the Principle of Least Privilege. For this demo I am okay with analyst.

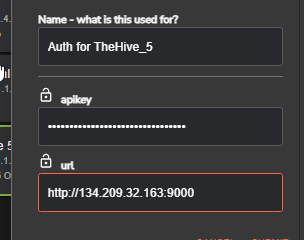
Now we need to make passwords for the user mydfir and an API key for SOAR user



Now I will log out of this admin account and login into my mydfir account and you can see there are no current cases as we just made this account. Les head over to shuffle to configure it to work with TheHive.

Select TheHive app and click on the orange authentication button to add the API

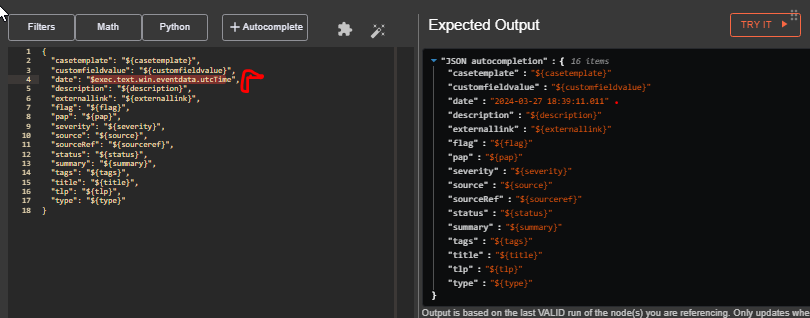




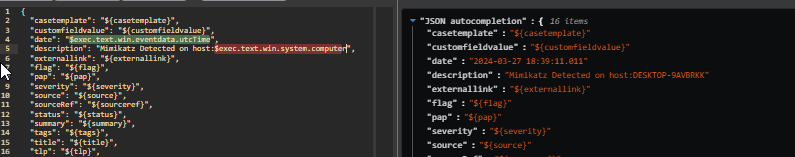
Be sure to add your hive public IP along with the port number.

Next I want to create an alert under find actions.

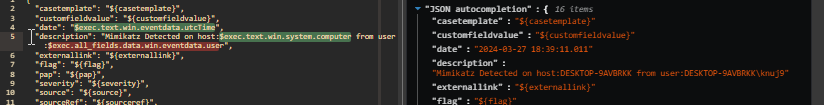
And in the body, I want to add edit the time from virustotal app



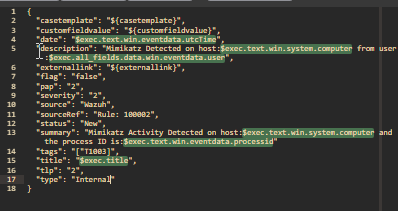
Next we can edit the description to Mimikatz detected on host computer



I lied, lets add the user to that as well as this will be helpful for identification



Next I changed the rest of the tafs



Date:$exec.text.win.eventdata.utcTime

Description: Mimikatz Detected on host:$exec.text.win.system.computer from user:$exec.all\_fields.data.win.eventdata.user

Flag:false

Pap(permissible actions protocol):2 is the default

Severity:2

Source: Wazuh

Source Ref: “Rule: 100002”

Status: New

Summary: Mimikatz activity detected on host:$ and the processId:$ and the command line is:$

(you can add as much as you want to this)

Tag: [“T1003”] for credential dumping

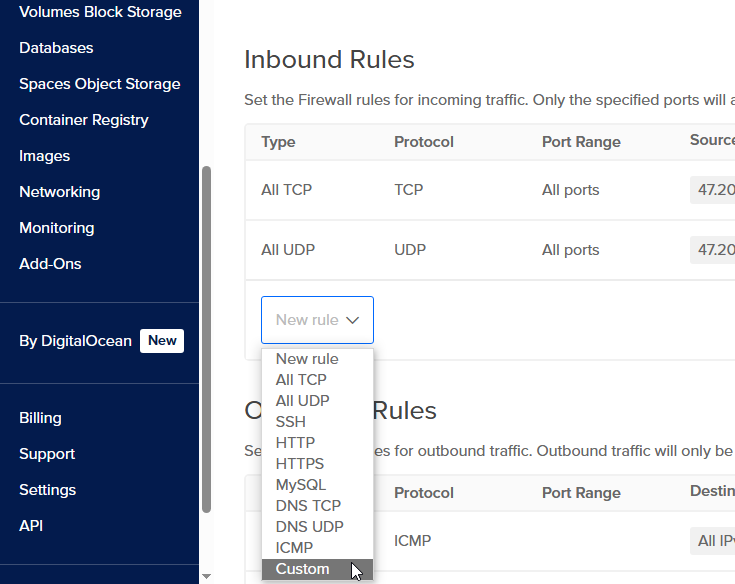
Title: Mimikatz Detected or tie it with the alert itself with $exec.title

tlp(confidentiality): 2

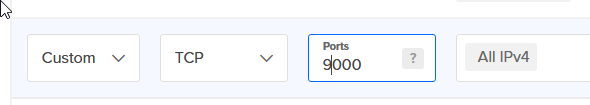
Type: Internal

Save file

Now before we run this we have to modify our firewall to allow all inbound IPs coming from port 9000 as this is where TheHive instance will live. So need to go back to Digital Ocean and make those changes.



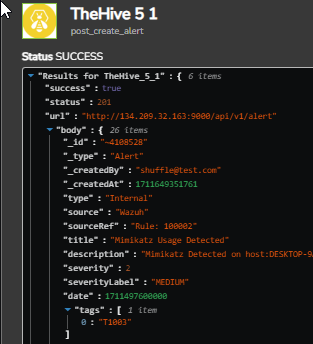
Here we are going to make a custom rule:



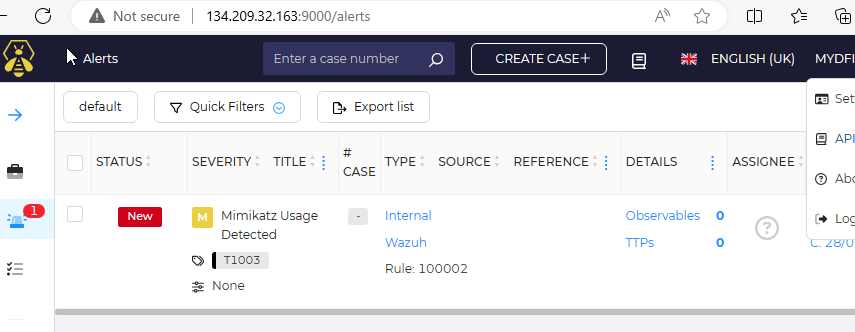
Now I can rerun the workflow

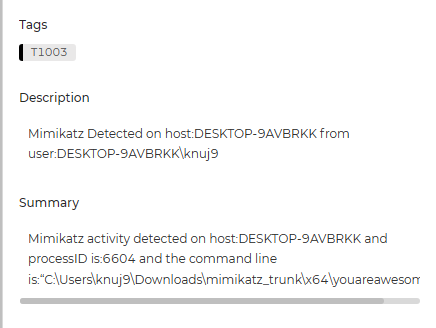
And we see the Hive was successful



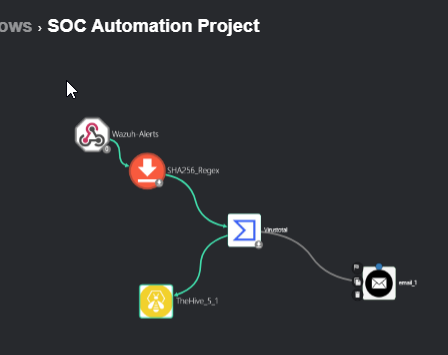


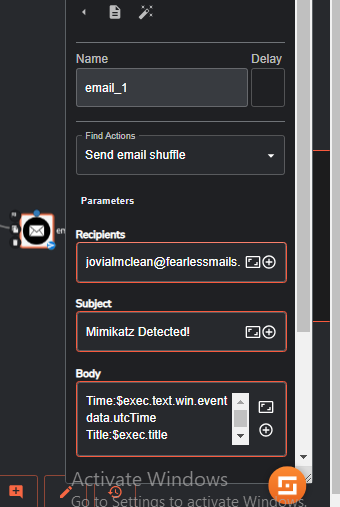
And lets look at what Mydfir user sees on their end in TheHive instance:





Next is to send our analyst an email containing relevant information. To do this we can add an email app to the workflow connected from VirusTotal





And now we can see the alert email came in



With this automation in place we can utilize a vast amount of practical use cases.

We connected Shuffle(SOAR), sent alerts to TheHive, and sent to SOC analysts via Email.

Next will be setting up Ubuntu for a similar example while demonstrating how to automate the response side.