SIEM Project

Purpose:

Setup a home SIEM, generate alerts to investigate, and learn how to troubleshoot

Tasks:

Set up ELK to collect,analyze and visualize logs from endpoints

Create public SSH and RDP servers and use Brute Force attacks on those servers

Create alerts and dashboards to visualize the data

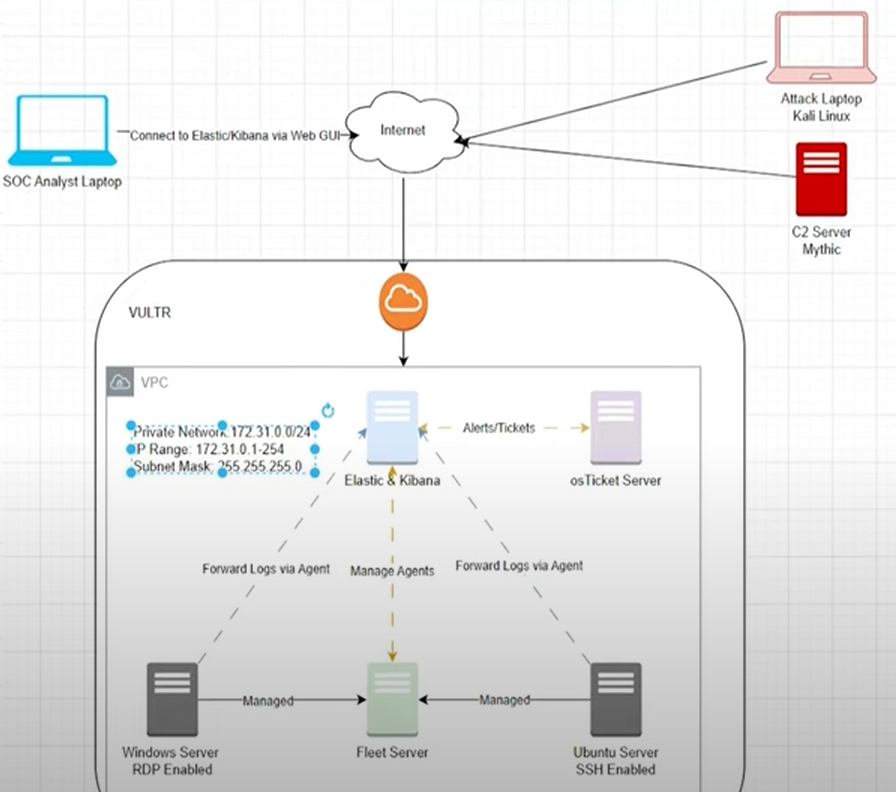
Set up a C2 server using Mythic

Set up and integrating a ticketing system and conducting investigations

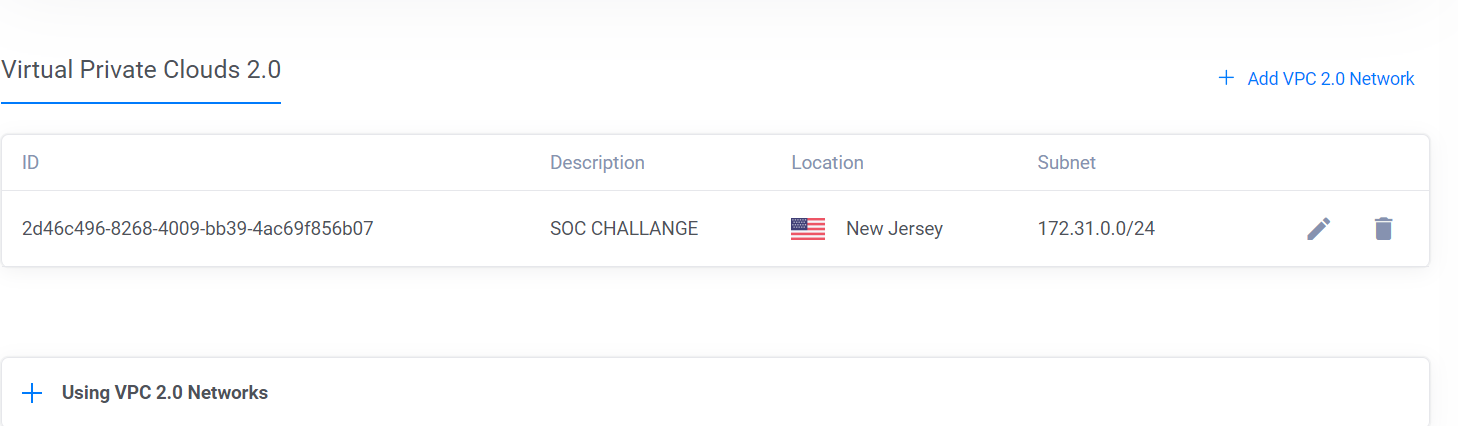
Tools and technology:

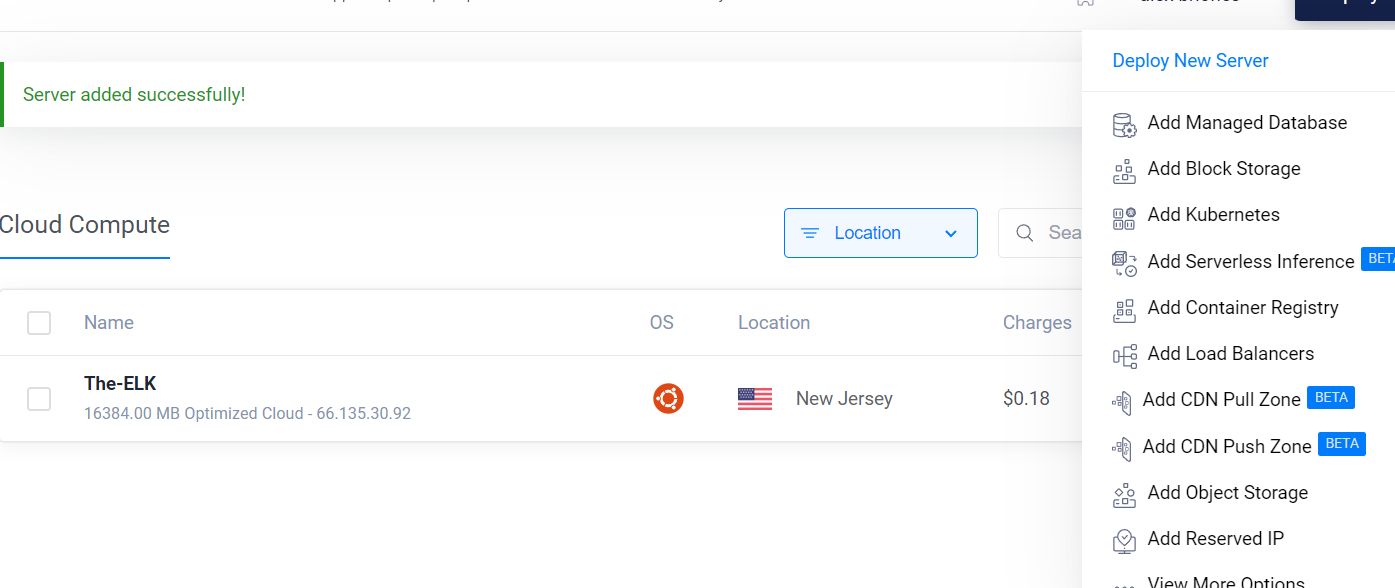
Virtual box, Elastic, osTicket, Mythic, Kali Linux, Powershell, Vultr, Kibana, Sysmon

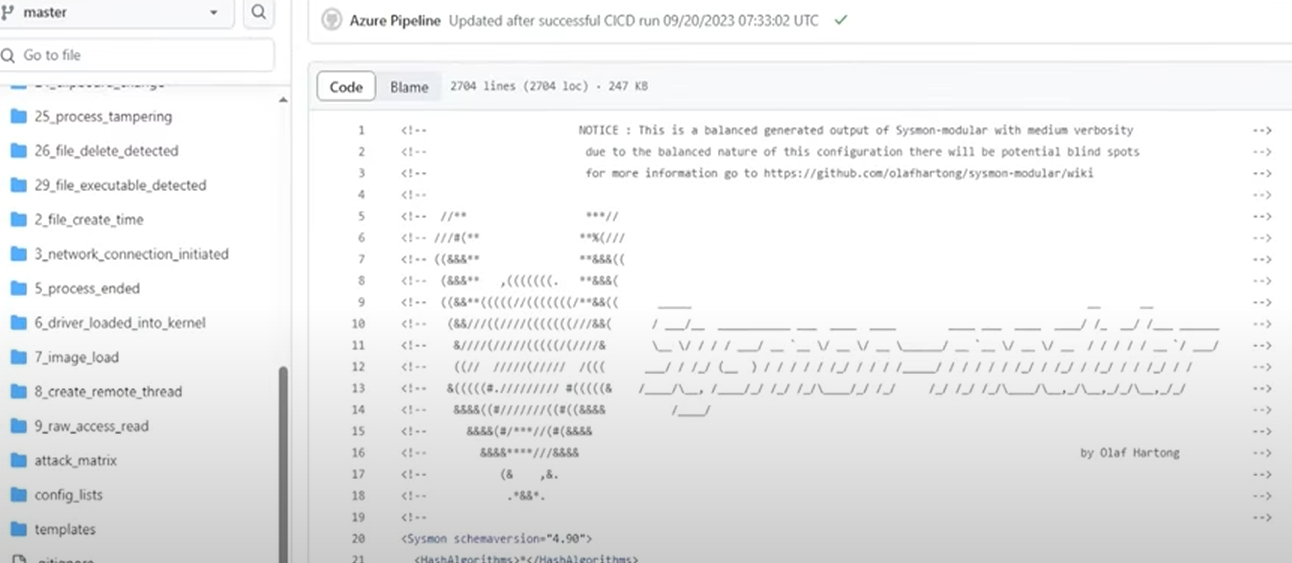
Creating a logical diagram to visualize the project

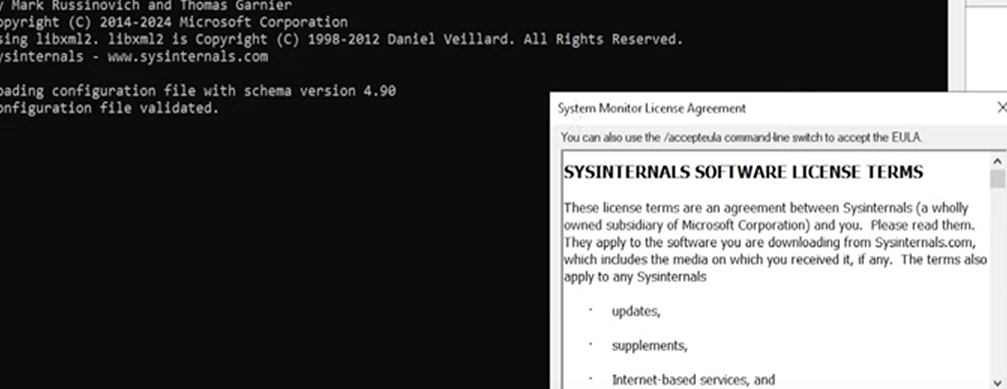


Creating the Fleet, Windows servers and elastic agents to initiate the project





Setting up Sysmon was very simple and straightforward. I did have an issue with pasting the directory on powershell. I then realized that i didn't extract the sysmon file which then allowed me to continue with the next steps to download sysmon. It was very interesting that the website for the sysmon download had the event 

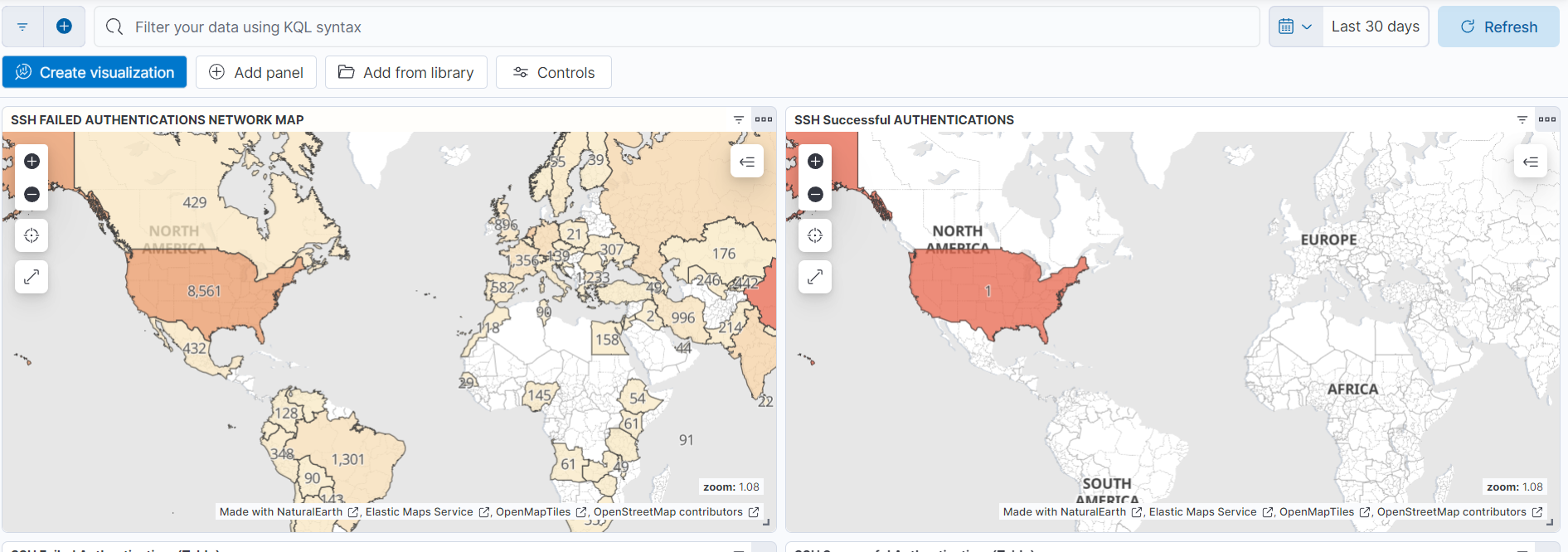


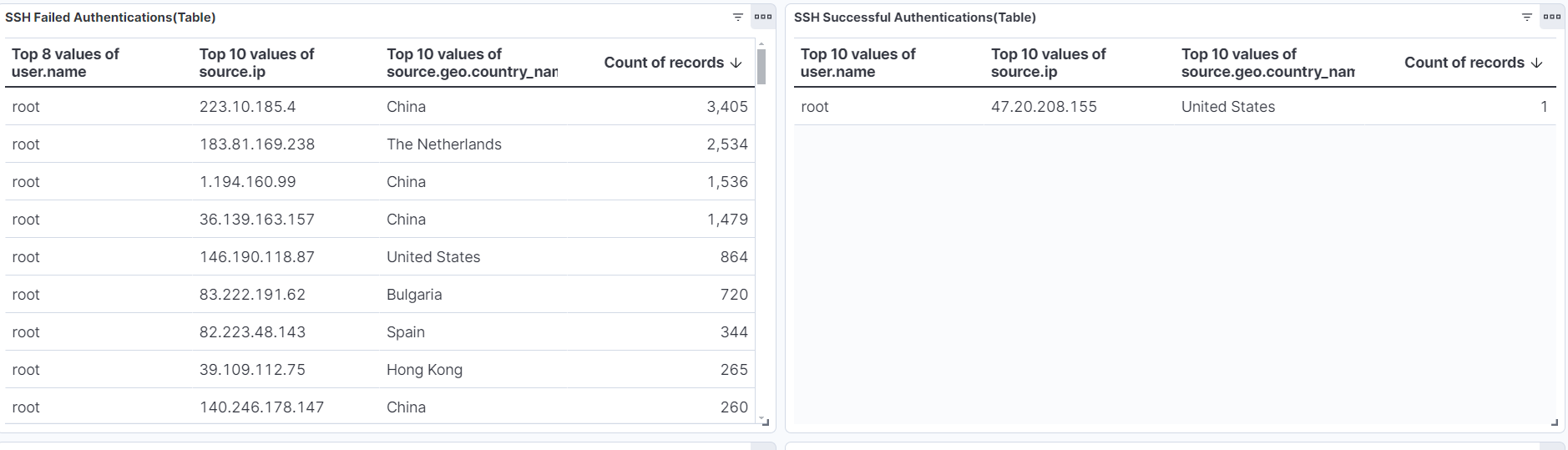
Observe authentication logs from the windows server and created an alert

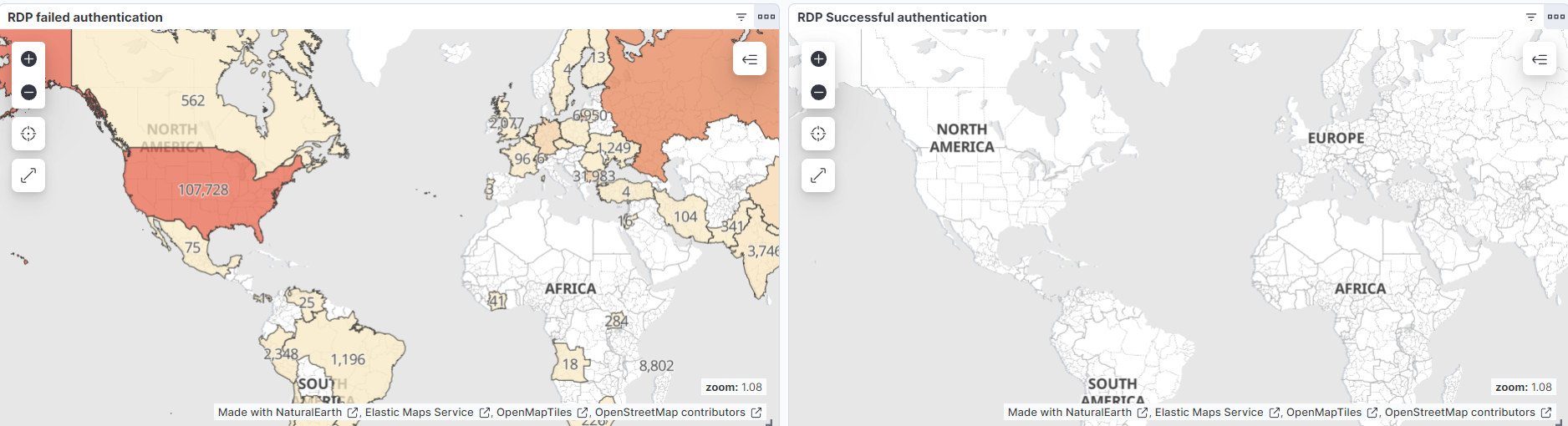


Most of the failed logins used “admin” or “user” for the username,

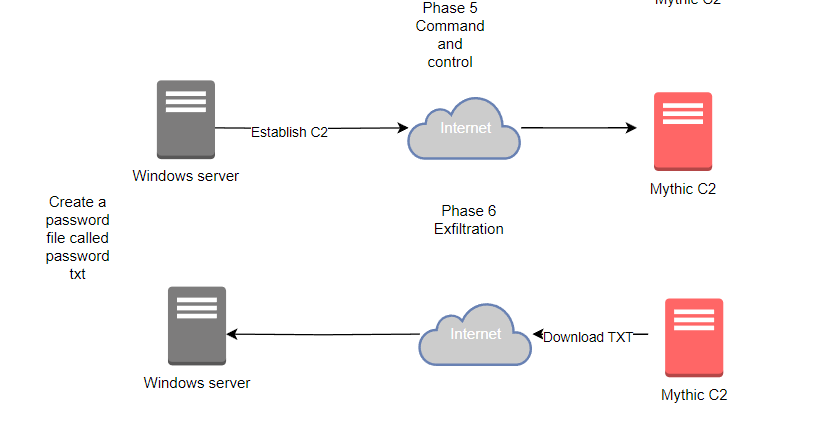
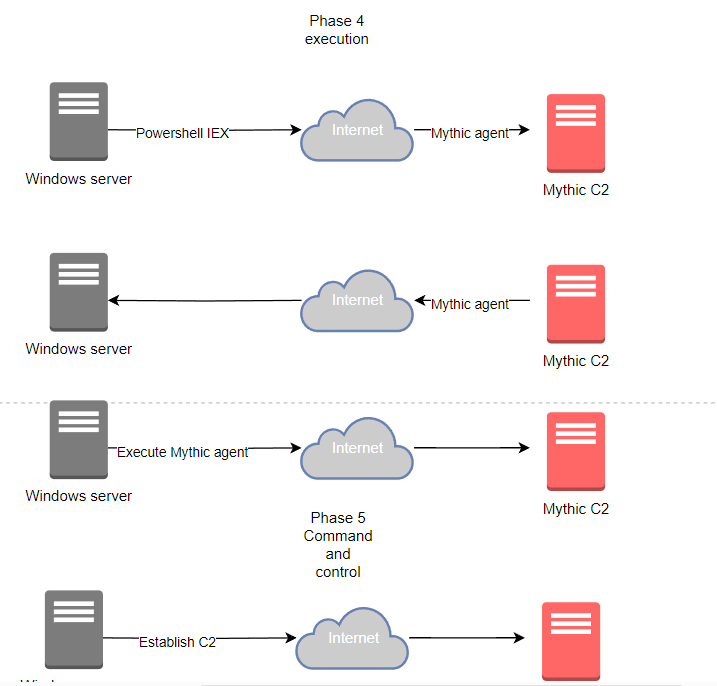
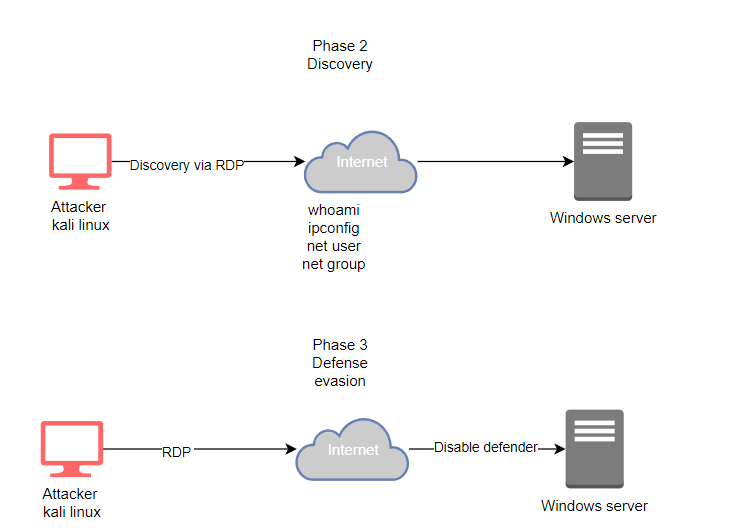
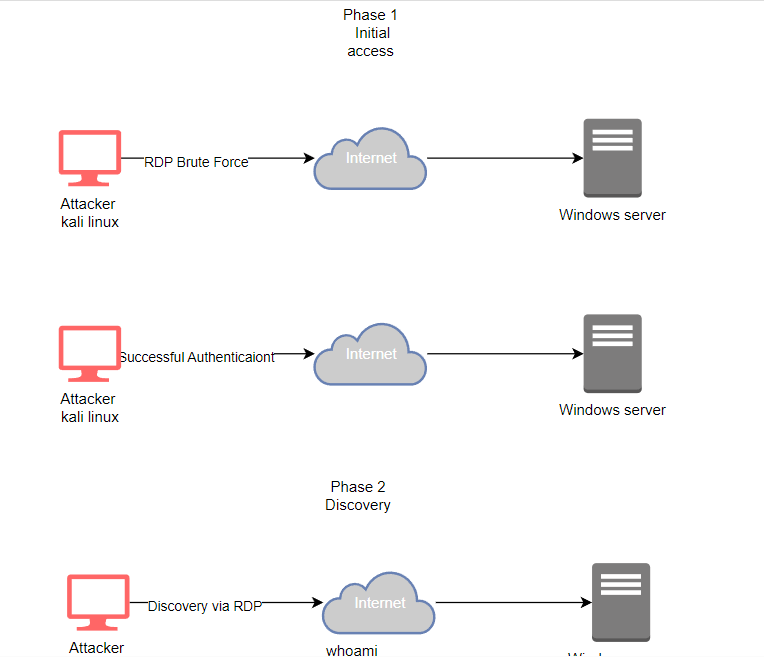
Created a dashboard/alerts for RDP activity





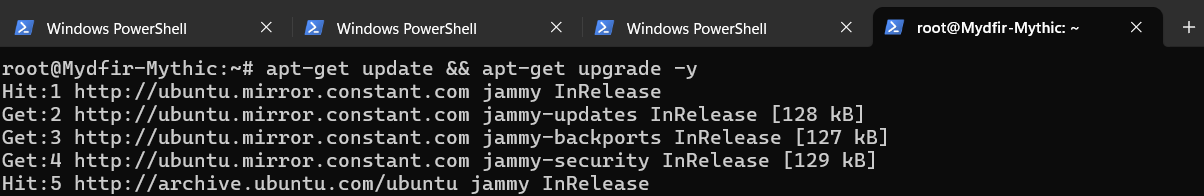


Created a Brute ForceAttack diagram

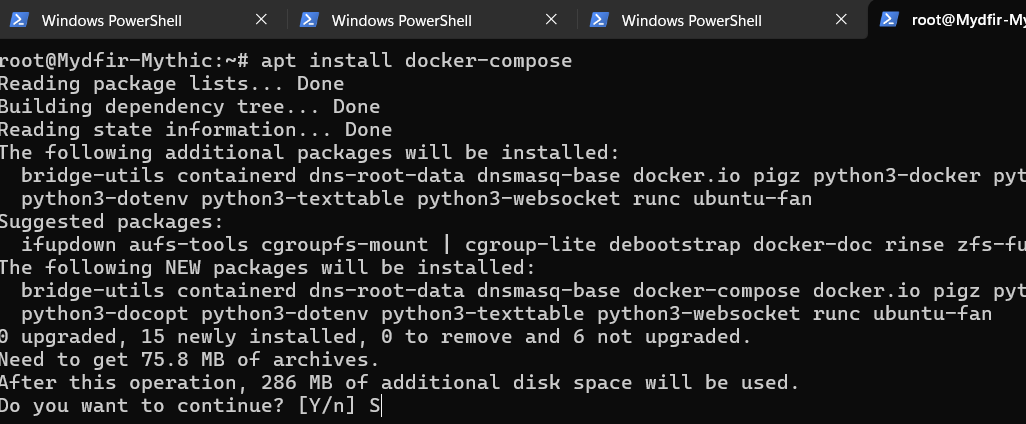


Setup mythic C2 server and learned about mythic

Created a mythic server and updated it through powershell



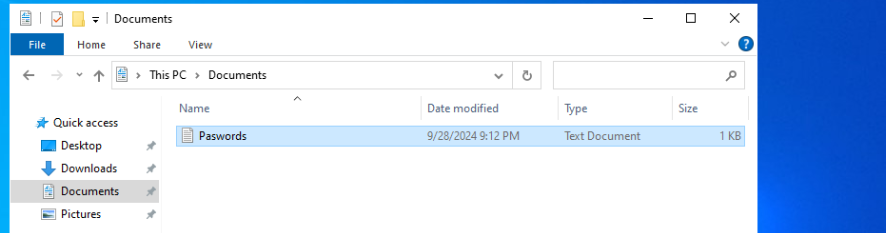
Installing docker compose

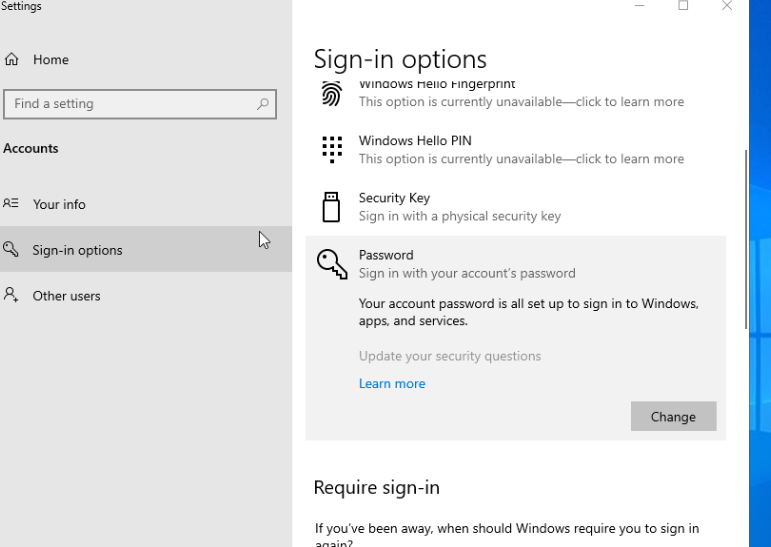


Perform a brute force attack, generate a Mythic agent(APOLLO) and establish a C2

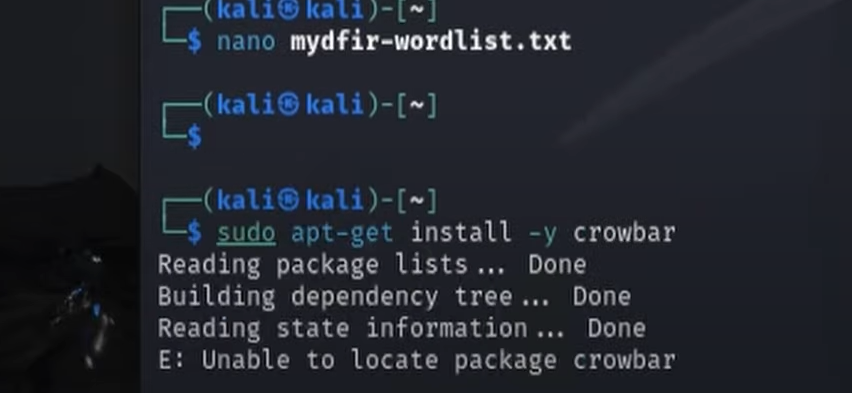
Created a password file inside of the windows server

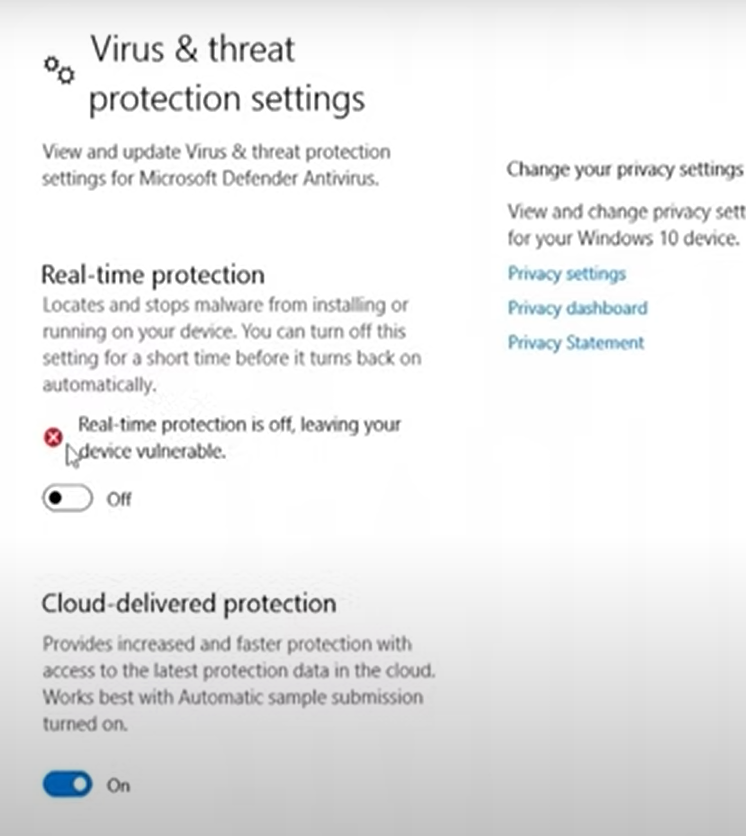
Changed the password of the server to what is in the password file





Using Kali Linux, crowbar is installed to perform an RDP brute force attack to windows server machines and gain access.



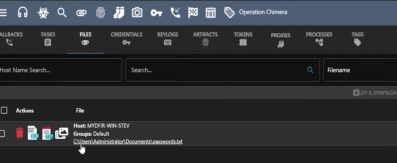
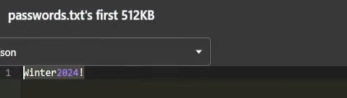
Then disabled all protection on the machine

Install APOLLO from the github repository onto the mythic machine



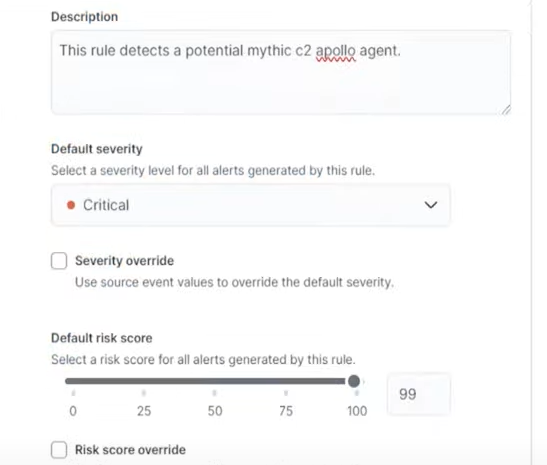
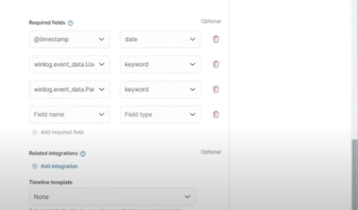
Added the C2 onto the web gui



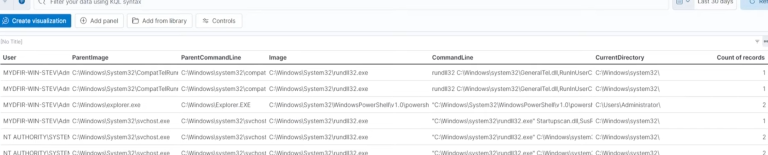
Able to view the password file from the GUI

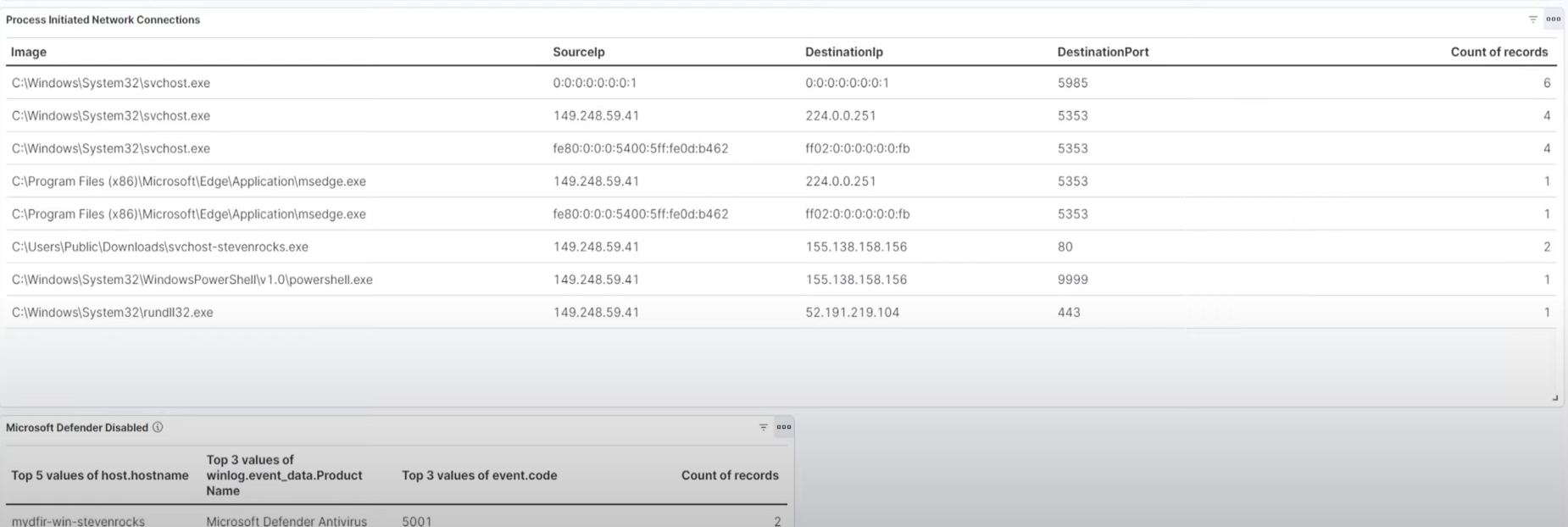
Created an alert and dashboard based on the activity generated by Mythic

On elastic creating a new rule for alerts

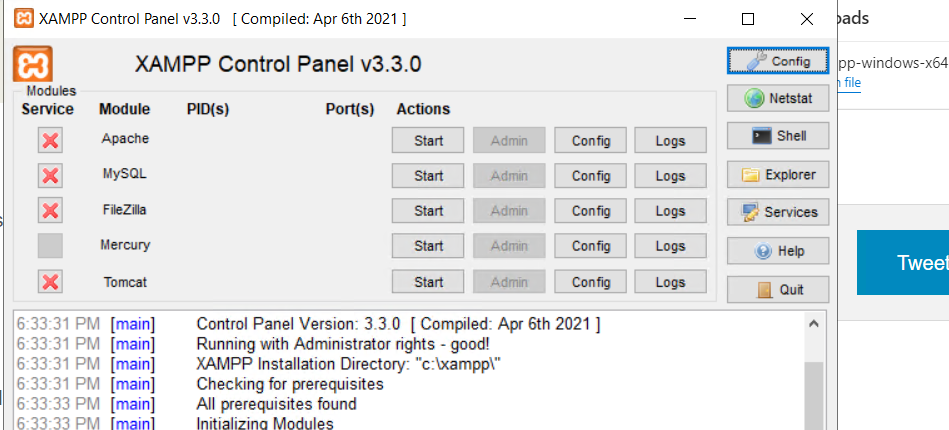
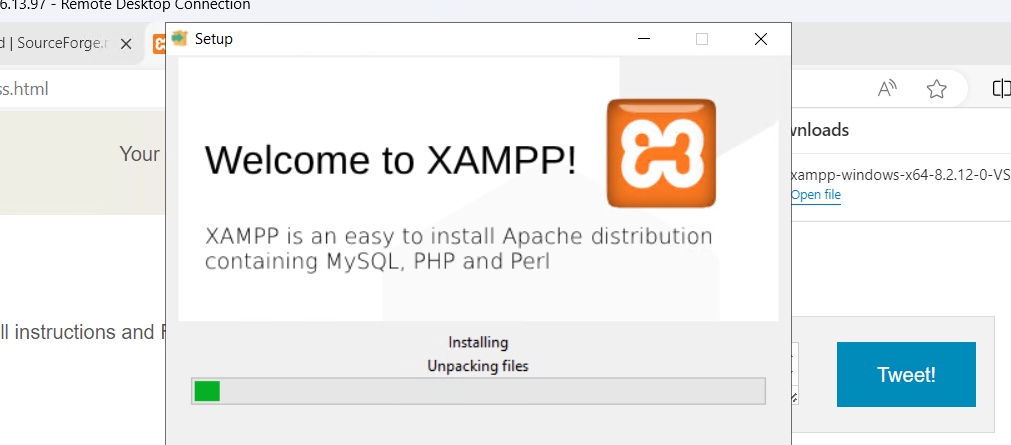


Created a dashboard to visualize any executions

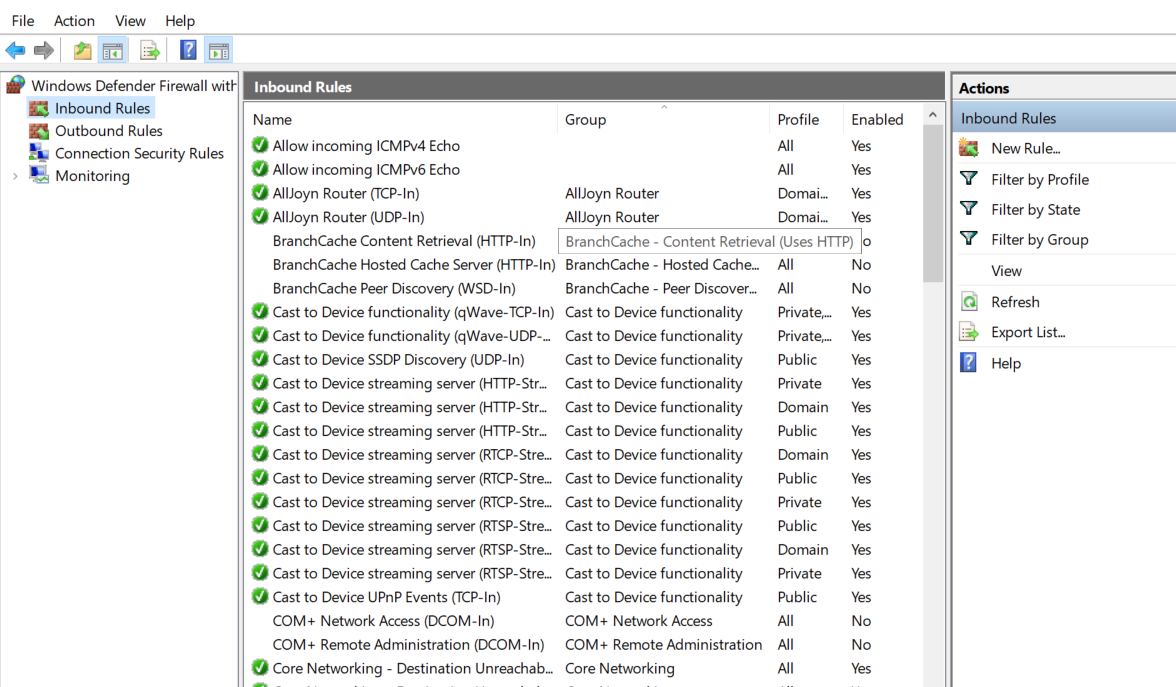


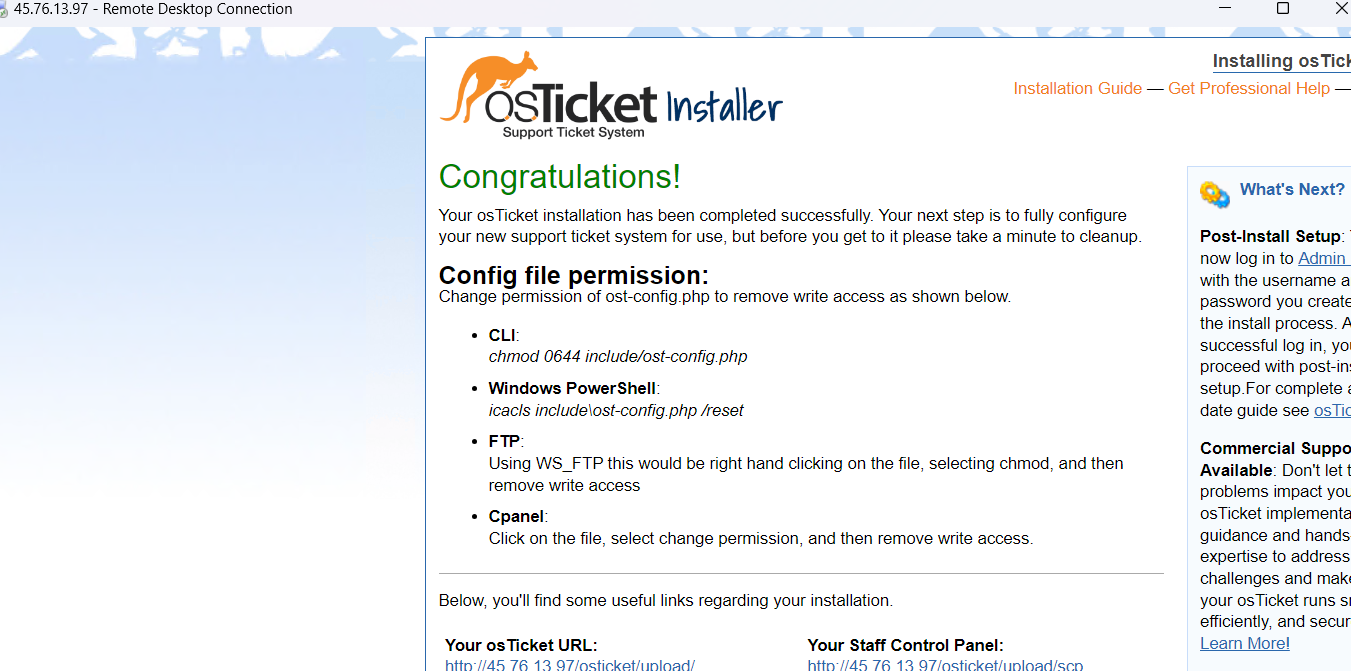


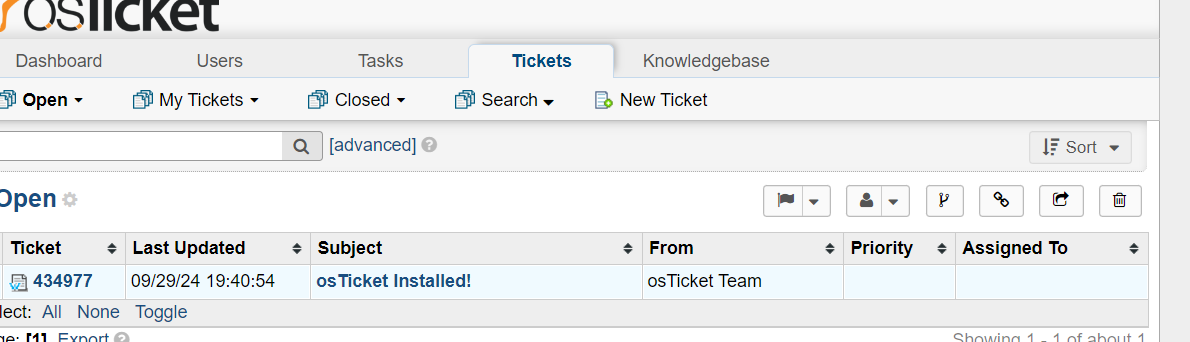
Created an Osticket server within Elastic and RDP’d into it and downloaded a web server that will host the ticketing system

\

Allowing inbound connections to port 443,80 on the servers firewall

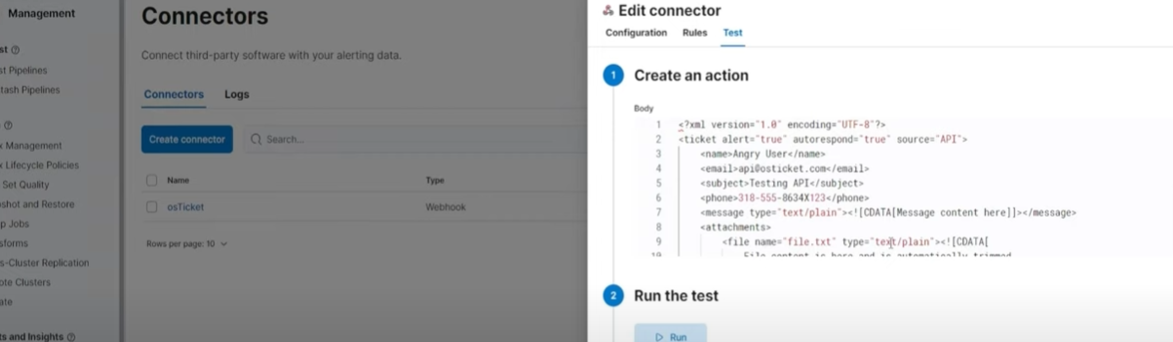
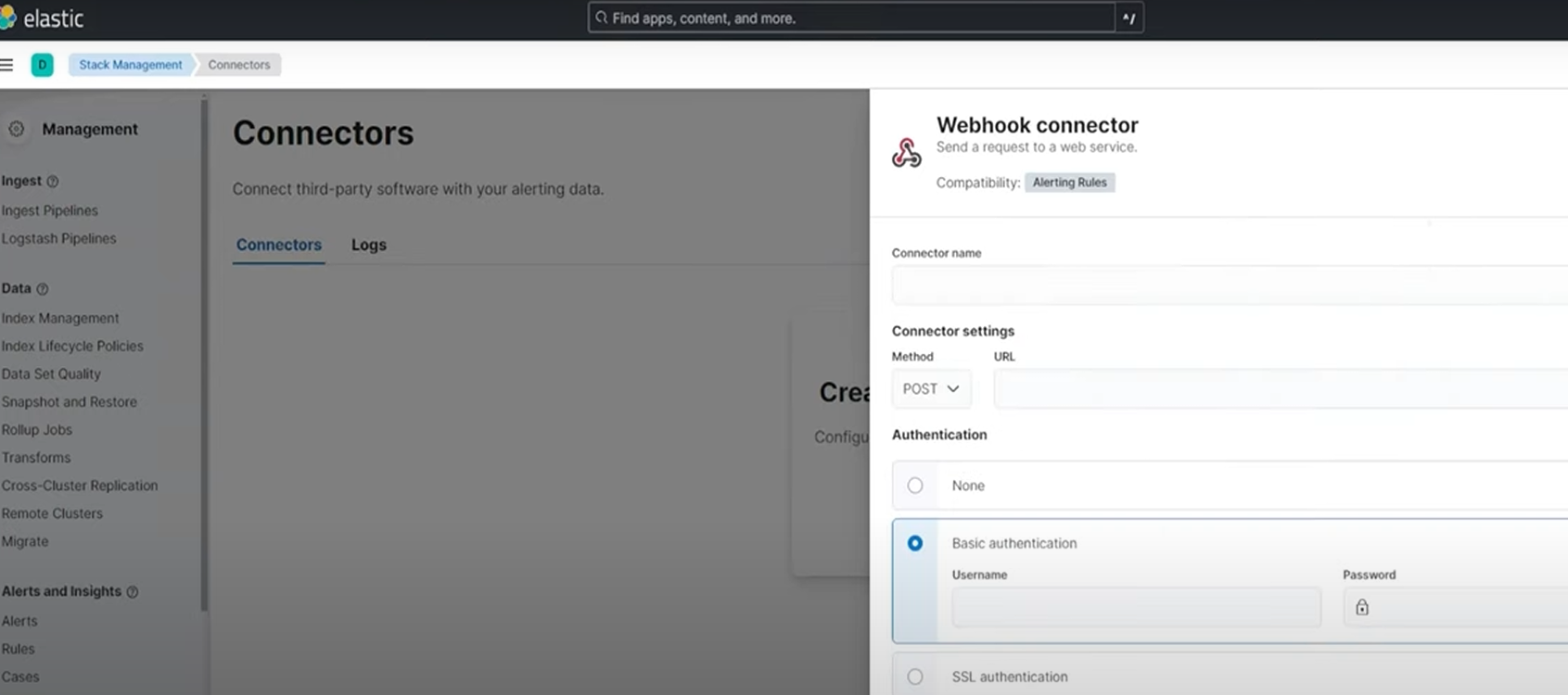


Setting up the osTicket and successfully creating an admin account 



Integrated osTicket with Elk and send a test alert

Setting up Webhook for the alerts using the github payload XML to fill in the create an action area. Once created I was able to create tickets on osTicket from the alerts in Elastic and keep track of alerts.



Investigate a SSH and RDP brute force alert

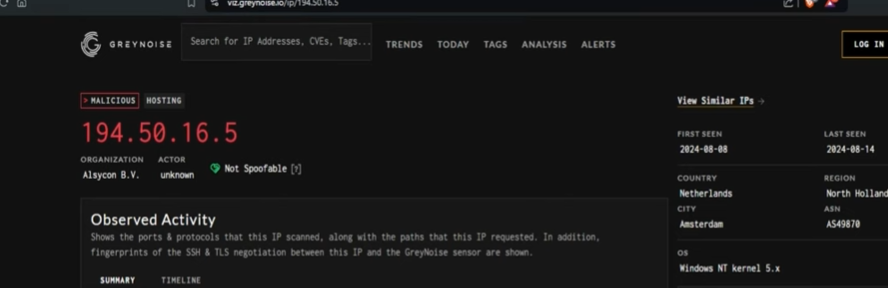
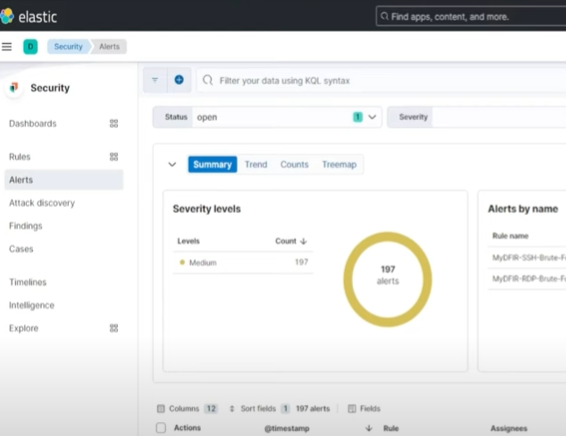
Questions that were used as a guideline when investigating these alerts were

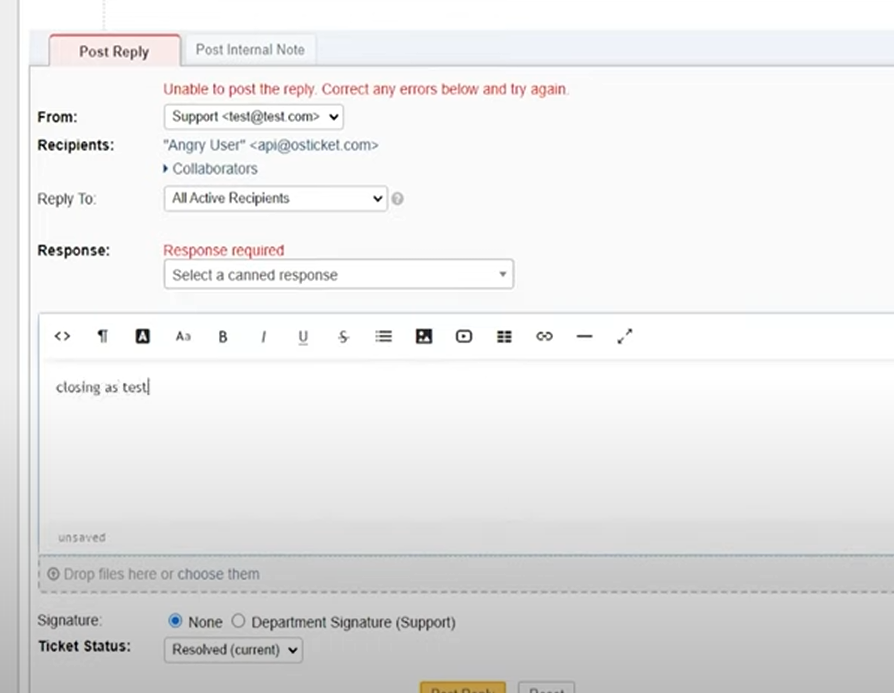
Is this IP known to perform brute force activity?

Any other users affected by this IP?

Were any of them successful?

If so, what was executed after a successful login?

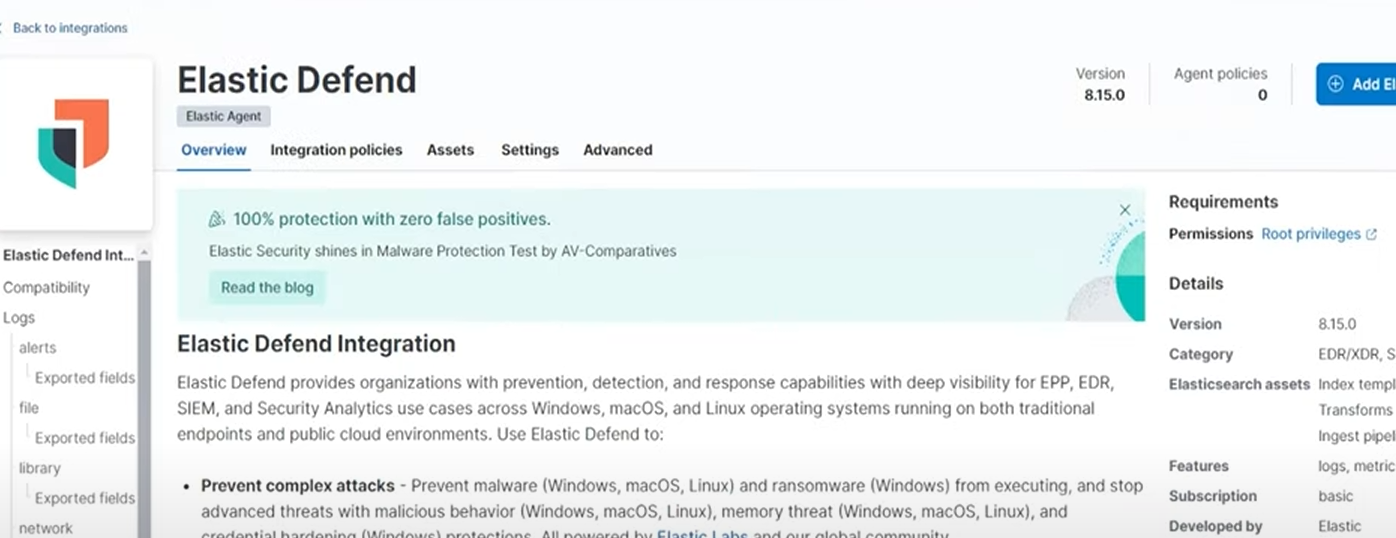
 used greynoise to check if the IP’s that popped up on the alerts were indeed malicious

Using Osticket to simulate investigation on a ticket and updating ticket with findings and finally closing the ticket out



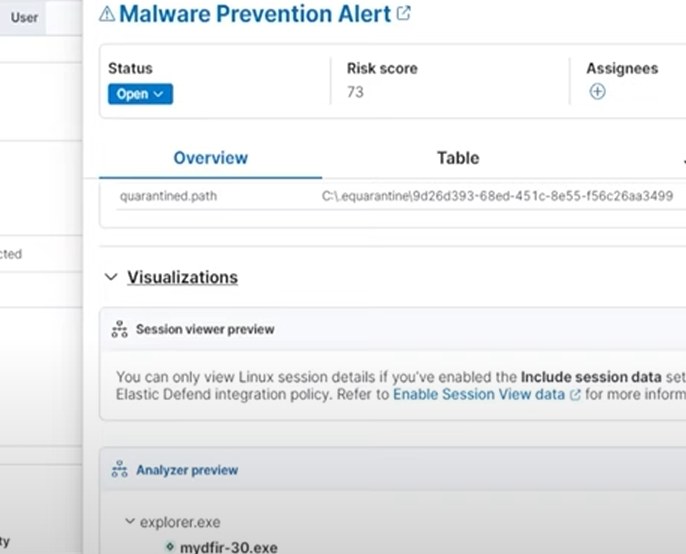
Used Greynoise to help investigate this IP for RDP brute force

Installed Elastic defend

Installing Elastic’s very own EDR

And configured for traditional endpoints like desktops, laptops ro virtual machines. Then connecting it to the windows server

Successfully defended against unwanted software when opening an exe. File

 The alert was created for this for this event and was viewable through the alert dashboard

In Conclusion I was able to start up an ELK instance and two servers(Linux SSH and Windows RDP). I then installed elastic agents to push logs into Elasticsearch while also creating alerts and dashboards for brute force.While able to learn more about a common C2 framework Mythic agents. Then I was able to integrate an osTicket to assign tickets to myself and close them out with my notes on my discoveries.